# Dell SonicWALL

## Sales Playbook

May 7, 2012

DELL CONFIDENTIAL
*Do not distribute or share with*
*non-employees for any reason.*

## Table of Contents

## Purpose

The objective of this playbook is to provide sales teams with information about the SonicWALL acquisition in order to facilitate a fast ramp on SonicWALL products, as well as ensure a smooth transition experience for Dell customers. This document includes a description of the deal, an overview of the strategic fit for Dell, product summaries, competitive assessments, and Dell sales engagement information for both Direct and Channel Sales organizations.

**For more information on SonicWALL, please see the Dell SonicWALL Dashboard here**

## Legal Guidelines

This sales playbook is a confidential document intended solely for internal use by Dell sales teams. It is intended to support the Dell SonicWALL acquisition announcement and subsequent go-to-market activities with the goal of ensuring that our customers have a consistent and positive experience.

You may explain the benefits of Dell SonicWALL products as follows:

- SonicWALL extends Dell's security capabilities already in place with the Dell SecureWorks security services, cloud security solutions, data encryption solutions, mobile device management and Dell KACE vulnerability and patch management.
- SonicWALL provides Dell an opportunity to offer comprehensive and integrated Unified Threat Management to SMBs and Next Generation Firewall to Large Enterprise and Public customers.
- SonicWALL to become Dell's center of excellence for security appliance solutions.
- Dell's brand and global distribution accelerates SonicWALL's current go-to-market capabilities.
- SonicWALL's dynamic network security protection solutions complement Dell SecureWorks' industry-leading IT security services, enabling Dell to offer comprehensive Unified Threat Management, Next Generation Firewall as well as security services to organizations of all sizes.
- Dell remains committed to delivering complete security solutions utilizing the most effective technologies and services from both within Dell and from leading providers.

You will be able to provide customers with Dell SonicWALL products immediately through existing SonicWALL sales channels, as well as through Dell S&P.

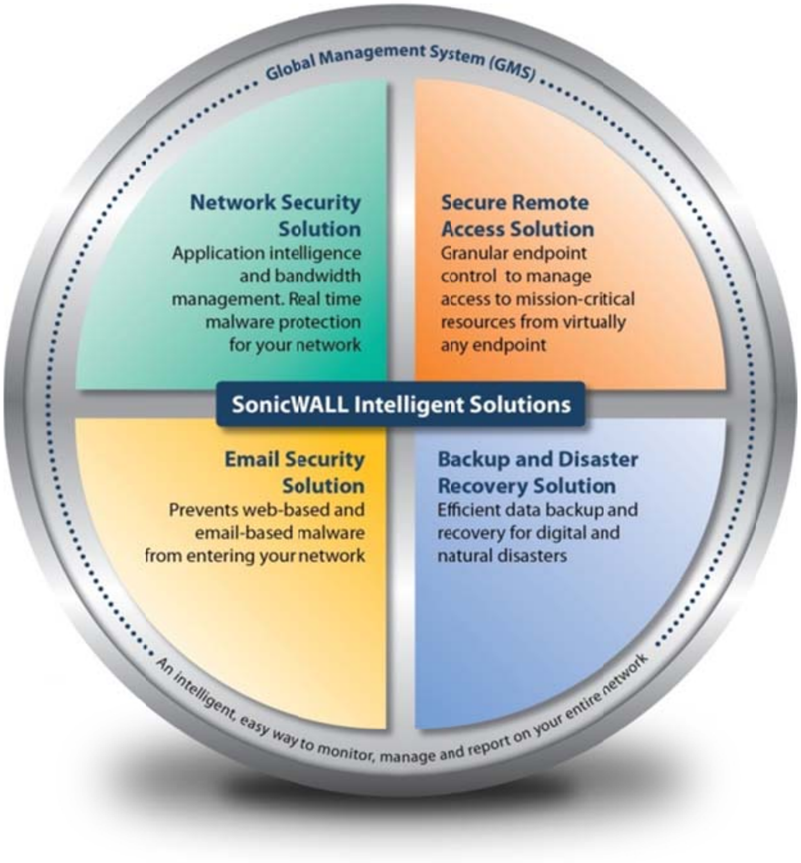
This sales playbook is a highly confidential document intended solely for internal use on and after the acquisition announcement.

## Dell's Software Solutions Strategy

- Software plays an increasingly important role in Dell's future as an end-to-end IT solutions provider.
- Dell already has strong software capabilities in fast-growing areas, including systems management (KACE), cloud integration (Boomi), and infrastructure virtualization and workload orchestration (Scalent), as well as more recently next-generation unified backup, archive and replication (AppAssure).
- In addition to these capabilities, Dell has world-class software expertise in servers, storage, networking, and mobility solutions.

## General Dell SonicWALL Solution Overview, Vision, Product Portfolio Overview

Dell® SonicWALL® provides intelligent network security and data protection solutions that enable customers and partners to dynamically secure, control, and scale their global networks. Using input from millions of shared touch points in the Dell SonicWALL Global Response Intelligent Defense (GRID) Network, the Dell SonicWALL Threat Center provides continuous communication, feedback, and analysis on the nature and changing behavior of threats. Dell SonicWALL's Research Lab continuously processes this information, proactively delivering countermeasures and dynamic updates that defeat the latest threats. Patented* Reassembly-Free Deep Packet Inspection® technology, combined with multi-core parallel architecture, enables simultaneous multi-threat scanning and analysis at wire speed and provides the technical framework that allows the entire solution to scale for deployment in high bandwidth networks. Dell SonicWALL network security and data protection solutions, available for the SMB through the Enterprise, are deployed in large campus environments, distributed enterprise settings, government, retail point-of-sale and healthcare segments, as well as through service providers.  Dell SonicWALL offers a comprehensive lineup of industry-leading network security and data protection solutions, including firewall, secure remote access/ SSL VPN, anti-spam/email security, and continuous backup and recovery, plus centralized management and reporting.


Global Management System (GMS)
Network Security Solution
Application intelligence and bandwidth management. Real time malware protection for your network
Secure Remote Access Solution
Granular endpoint control to manage access to mission-critical resources from virtually any endpoint
SonicWALL Intelligent Solutions
Email Security Solution
Prevents web-based and email-based malware from entering your network
Backup and Disaster Recovery Solution
Efficient data backup and recovery for digital and natural disasters
An intelligent, easy way to monitor, manage and report on your entire network

### Network Security

Essential to an intelligent and highly adaptive security system, Dell SonicWALL Next-Generation Firewalls offer superior protection and control for both wired and wireless networks and, unlike competitive offerings, scan all network traffic with high performance and low latency and massively scale to extend state-of-the-art security to growing and distributed enterprise networks.

### Email Security

Many anti-spam and email protection solutions are cumbersome to manage and inflexible to use, resulting in frustrated users and a higher-than-expected cost of ownership. Dell SonicWALL® Email Security solutions are different, as they employ a variety of proven and patented technologies designed to block spam and other threats effectively, easily and economically.

### Secure Remote Access

Dell SonicWALL® Secure Remote Access (SRA) Series offers SSL VPN access to mission-critical resources from virtually any endpoint—including desktops, laptops, tablets and smartphones. There's a scalable remote access solution for every organization—from the smallest business to the largest global enterprise.

### Backup and Disaster Recovery

Dell SonicWALL® Continuous Data Protection (CDP) Series enables your business to preserve, replicate, archive, govern and restore data with ease. New and advanced features streamline backup operations and manage information assets efficiently and intelligently.

### Global Management System

Dell SonicWALL's management and reporting solutions provide the ability to create and manage security policies, provide real-time monitoring and traffic analysis and deliver intuitive reports for all of the Dell SonicWALL security solutions.

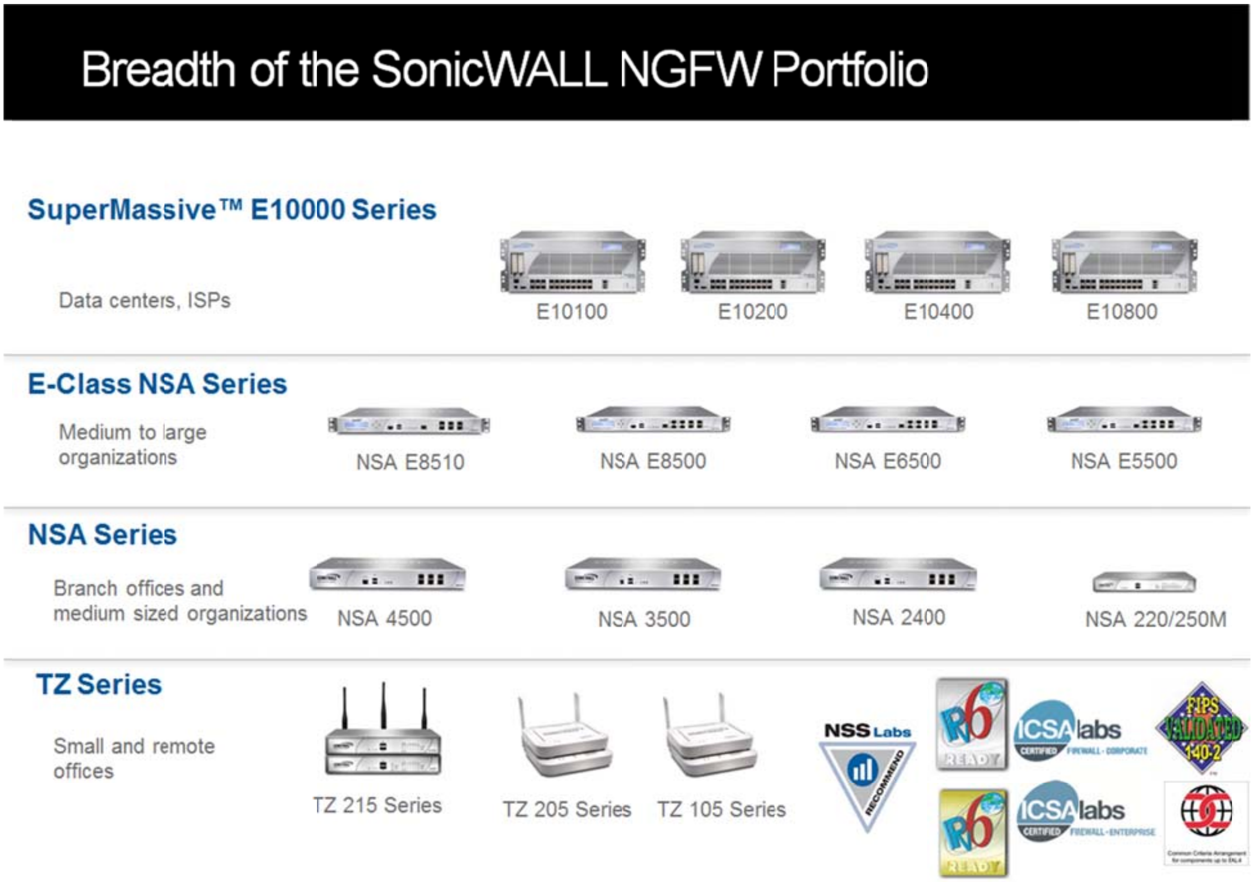
## Dell SonicWALL Network Security Portfolio Overview

The Dell SonicWALL Network Security product line is comprised of four primary lines of firewalls aimed at networks of all sizes, ranging from large enterprise, carrier and datacenter deployments to SMB/Distributed Enterprise to Small Office/Home Office (SOHO). The four classes of firewalls are:

- **SuperMassive E10000 Series** (Carrier, Large Enterprise, Data Center, Campus)
- **E-Class Series** (Small/Medium Enterprise, Campus, Data Center)
- **NSA Series** (Small/Medium Business, Distributed Enterprise)
- **TZ Series** (SOHO, Retail, SMB, Distributed Enterprise)

All Dell SonicWALL firewalls run on the proprietary SonicOS operating system and are powered by patented Reassembly-Free Deep Packet Inspection™ technology to scan all network traffic and provide application intelligence, control and visualization, real-time intrusion prevention, anti-malware, SSL decryption, high-speed virtual private networking (VPN) technology and other robust security capabilities. This approach allows networks with Dell SonicWALL firewalls to eliminate the majority of threats at the gateway, before they make their way into or out of the network. Dell SonicWALL's firewalls are built around a massively multi-core architecture to take advantage of massive parallelism to deliver high performance wire-speed, low-latency Deep Packet Inspection level of security. The user interface in SonicOS has grown in sophistication alongside with the products, but retains its intuitive and easy-to-use nature rooted in the experience expected by SMB customers.

The power and effectiveness of the Dell SonicWALL Network Security portfolio has been demonstrated in the comprehensive 3rd party testing by NSS Labs and its 2012 Next-Generation Firewall Security Value Map™ report. This test not only granted the SuperMassive E10800 running SonicOS a highly coveted NSS Recommended rating, but also demonstrated it as the NSS Labs recommended Next-Generation Firewall (NGFW) with the highest overall protection and the highest throughput at 18.9 Gbps (~5.5x the next closest rival). Of note, the proven SonicOS architecture is at the core of every Dell SonicWALL® firewall from the SuperMassive™ E10800 to the TZ105.



## Breadth of the SonicWALL NGFW Portfolio

**SuperMassive™ E10000 Series**

Data centers, ISPs

E10100 E10200 E10400 E10800

**E-Class NSA Series**

Medium to large organizations

NSA E8510 NSA E8500 NSA E6500 NSA E5500

**NSA Series**

Branch offices and medium sized organizations

NSA 4500 NSA 3500 NSA 2400 NSA 220/250M

**TZ Series**

Small and remote offices

TZ 215 Series TZ 205 Series TZ 105 Series

NSS Labs
RECOMMEND
READY
ICSA labs CERTIFIED FIREWALL - CORPORATE
FIPS VALIDATED 140-2
READY
ICSA labs CERTIFIED FIREWALL - ENTERPRISE

### Customer Pain Points

## Small and Medium Business Customers

- **Ease of Use and Deployment** – SMBs generally do not have dedicated network security IT staff experienced with deploying networking solution, therefore making ease of use and deployment a valuable aspect of any IT solution that they deploy.
- **Simple, yet powerful comprehensive security –** Firewalls are purchased for security, and they must deliver security in an unobtrusive and effective manner. Security means different things to different people, but to Dell SonicWALL it means full DPI protection with Intrusion Prevention and Gateway Anti-Malware, both of which update automatically in the background without user intervention.
- **Reliability, Availability and Redundancy –** Ability to resist downtime, especially in Retail/POS environments through multiple-WAN failover, Multiple-firewall failover, Failover to 3G/4G.
- **Easy to Use Remote Access (IPSec VPN & SSL VPN) –**Remote access is crucial for connecting offices together, allowing people to work from home or when on the road.
- **Secure Wireless Connectivity –** With laptop sales eclipsing sales of desktops several years ago, and tablets now surpassing laptop sales, wireless connectivity is almost a mandatory component of any network.
- **Equipment consolidation –** SMBs want to eliminate costs and reduce management overhead. By consolidating multiple pieces of equipment into a single device, Dell SonicWALL firewalls help to eliminate:
  - Dedicated wireless controllers
  - Routers dedicated for T1/E1 termination (NSA 250M only)
  - IPS or content filtering systems separate from firewalls
  - Dedicated Remote access (SSL VPN or IPsec VPN) appliances

## Retail & POS Customers

All retail locations concern themselves with security and reliability.  A security breach can open the retailer to fines, lawsuits and lost business.   Downtime can result in direct loss of sales revenue, and is therefore equally catastrophic.  Retail deployments look for firewalls that Provide:

- **Security features that help to comply with the PCI-DSS standard** – Dell SonicWALL IPS, VPN, network segmentation, wireless segmentation and wireless rogue access point detection features help to comply with the PCI-DSS standard.
- **Reliability, Availability and Redundancy** – Downtime in POS environments is measurable in revenue. Ability to resist downtime, through multiple-WAN failover, Multiple-firewall stateful failover and failover to 3G/4G is crucial in this sector.
- **Centralized Management & Reporting –** eliminates the need for a dedicated IT person at every retail location and helps to enforce a consistent security stance across the retail enterprise.  Also needs to eliminate truck rolls for a reduced TCO (achieved with Dell SonicWALL Global Management System).
- **Wireless Guest Services** – that do not compromise security while allowing patrons to access the internet, subject to a login or an acceptable user policy.

## Distributed Enterprise Customers

Dell SonicWALL has traditionally had a lot of success deploying firewalls to companies that have multiple remote locations that connect to a central office, forming a distributed network and requiring centralized management and VPN connectivity.

- **Distributed Network Security** – The ability to provide a consistent network security policy across the entire enterprise, including wireless configuration, while knowing that the periphery of the network has the same level of security as the core.
- **Application Control and Network Productivity** – Identify, control and eliminate problematic traffic on the distributed network while prioritizing core business traffic.
- **Reliability, Availability and Redundancy** – Ability to resist downtime for branch offices. In addition to multiple-WAN failover, Multiple-firewall failover and Failover to 3G/4G that may be deployed in SMB and Retail, distributed enterprises may look for more advanced reliability features for their branch offices such as Stateful High Availability.
- **Scalable Centralized Management** – Centralized management that can scale to thousands of end points, prevents truck rolls and reduces the TCO is crucial in distributed enterprise (achieved with Dell SonicWALL Global Management System).
- **Equipment consolidation –** Distributed Enterprises want to eliminate costs and reduce management overhead.  By consolidating multiple pieces of equipment into a single device, Dell SonicWALL firewalls help to eliminate:
  - Dedicated wireless controllers & separate wireless infrastructure
  - Routers dedicated for T1/E1 termination (NSA 250M only)
  - IPS or content filtering systems separate from firewalls

## Enterprise & Datacenter

- **Security (Intrusion Prevention, Stateful Packet Inspection)** – The primary purpose of the firewall is to establish a secure perimeter or to protect a server farm.  The firewall must be able to stand up to a large number of attacks at different network layers.  As the malware economy continues to grow, it becomes increasingly costly, sometimes with legal consequences, for companies to become victims of hacking attacks.

- **Performance, Low Latency & Scalability** – The firewall cannot slow down the network while defending the network from attacks, since such a slowdown will reduce the company/datacenter productivity. Real world evidence shows that performance is often preferred over security, i.e. if security slows down performance to unacceptable levels, security is turned down. **Application Visualization and Control –** This is a fairly recent development in that enterprises came to a realization that the secure perimeter that they relied upon in the past has **eroded** with Web 2.0 technologies and protocols tunneling over HTTP/HTTPS. To re-establish this secure network perimeter, enterprises have turned to application control technologies which peer into the tunneling traffic and regain visibility and control. **VPN & Connectivity –** Large firewalls are often deployed as VPN concentrators for distributed branch office traffic, and thus must have a proven high performance VPN technology that can be easily managed and deployed

## Competitive position in the marketplace

Dell SonicWALL is considered the incumbent in the SMB space due to its brand recognition, reputation and market share. It is an emerging player in the Enterprise firewall space and has recently challenged with the results of the latest 3rd party reports and customer wins. While traditionally Dell SonicWALL competed in the Unified Threat Management (UTM) space, its Application Control capabilities introduced in 2007, and further enhanced in 2010, made the SonicOS feature set and architecture perfectly aligned to participate in the growing NGFW market. Gartner considers Dell SonicWALL's E-Class NSA and SuperMassive E10000 Series firewalls suitable for Enterprise deployments and as NGFWs, while positioning the rest of the NSA and the TZ product line as UTM/SMB products. However, in reality, all firewalls in the NSA, E-Class NSA and the SuperMassive lines qualify as Next Generation Firewalls based on the strict definition of the category.

**Dell SonicWALL primary competitive advantage is its ability to deliver extremely high levels of security effectiveness along with *extremely* high levels of Deep Packet Inspection performance… This level of security and performance, combined with a low TCO, robust centralized management and an easy to use interface help Dell SonicWALL win a large share of competitive deals.**

## Juniper Networks

Juniper Networks competes in the network security space with their SRX line of firewalls, which in 2009 replaced their SSG firewall that was built on ScreenOS, inherited from the NetScreen acquisition. The SRX models span from the branch office to the carrier chassis, and while extremely strong on the routing side due to the presence of JUNOS, they have several drawbacks on the security front. Juniper's move from ScreenOS to JUNOS for their security products created a lot of confusion within the customer base and added unnecessary complexity. Additionally, much of Juniper's security is sourced from 3rd parties, and is not developed in-house and is not available on all models. For example, models above the SRX 650 do not have the ability to perform Application Control and Anti-Malware scanning. For a while, Juniper positioned their SRX series as "Secure Routers" in the Infonetics market share research, and only recently re-categorized them as firewalls.

Dell SonicWALL vs. Juniper SWOT

| Strengths | Weaknesses |
|---|---|
| • NSS Labs Recommended NGFW<br>• SuperMassive™ E10800 running SonicOS is the Highest Overall Protection Next-Gen Firewall Recommended by NSS Labs in the 2012 Security Value Map<br>• Rich SMB Feature Set<br>• Strong market position in SMB UTM<br>• Strong brand in SMB UTM<br>• Strong DPI performance and capabilities<br>• Core DPI Security features available on all platforms<br>• Leader in 2012 UTM Gartner Magic Quadrant<br>• In-house security research & security IP ownership (DPI services)<br>• Better TCO | • Juniper an established enterprise networking/security player<br>• Broad product line into carrier/large enterprise chassis products<br>• Juniper SRX product line is modular/configurable<br>• Challenger in the 2011 Enterprise Firewall Gartner MQ<br>• Challenger in the 2012 SMB UTM Firewall Gartner MQ<br>• Broader support offering includes Professional Services |
| **Opportunities** | **Threats** |
| • SSG -> SRX transition is so far not very successful for Juniper Partners & Customers<br>• Juniper does not offer full DPI security capabilities on all products –has special 'high memory" devices in some cases<br>• High end devices only offer IPS and Stateful Inspection<br>• Juniper ranked in the "caution" quadrant in the 2012 NSS Labs NGFW Security Value Map | • Ease of use in JUNOS addressed for the SMB market<br>• Juniper may add full DPI services to chassis based solutions<br>• Juniper may add SSL VPN into the SRX line<br>• JONOS becoming the standard OS for Juniper products |

## Check Point®

Check Point effectively invented the firewall market 15 years ago, and their brand is synonymous with firewall in the industry. They have competitive products and some of Check Point features are considered best in class, such as logging and reporting. While Check Point does provide Deep Packet Inspection capabilities via their software blades, they were caught unprepared several years ago when the NGFW application control requirements swept the firewall market. They have recently introduced their application control capabilities as another software blade. Check Point is most vulnerable on pricing, since have the most expensive renewal costs and Check Point expertise is some of the most expensive in the market.

Dell SonicWALL® vs. Check Point SWOT

| Strengths | Weaknesses |
|---|---|
| • NSS Labs Recommended NGFW<br>• SuperMassive™ E10800 running SonicOS is the Highest Overall Protection Next-Gen Firewall Recommended by NSS Labs in the 2012 Security Value Map<br>• Attractive pricing for the feature set in SMB with a lower TCO than Check Point<br>• Strong market position in SMB UTM<br>• Strong brand in SMB UTM<br>• Strong DPI performance and capabilities | • Check Point is one of the recognized firewall leaders<br>• Check Point has a Strong Enterprise Market Share<br>• Check Point has strong worldwide presence<br>• Check Point has a large list of reference customers<br>• "Leader" quadrant in 2011 Enterprise Firewall Gartner MQ and 2012 SMB UTM Firewall Gartner MQ<br>• Feature-rich firewall<br>• Very strong logging & reporting |
| **Opportunities** | **Threats** |
| • Replace Check Point on lower TCO for equivalent or better NGFW security<br>• Beat Check Point in the SMB on pricing and features<br>• Rely on Dell SonicWALL ease of use for SMB | • Launched new hardware – could be a performance threat<br>• Have multi-tenancy support on firewalls |

## Palo Alto Networks

Palo Alto Networks (PAN) is a private company and is the newest entrant to the firewall market with an application aware firewall, dubbed NGFW. Up until recently, PAN firewalls targeted primarily mid-size businesses up to medium/large enterprises. In the past year, however, PAN released a branch model, but it is very competitive from a feature and price perspective. Palo Alto Networks caught many enterprise firewall vendors by surprise and has enjoyed a very rapid success in selling application aware firewalls to formerly loyal Cisco, Check Point and Juniper Networks customers. This rapid success and new technology led to them to the Leaders quadrant of the 2011 Gartner Enterprise Firewall Magic Quadrant. PAN lacks many networking features, and instead focuses on the application awareness capabilities and security – they are a hot name in this industry and are a competitor in many deals displacing Cisco, Check Point and Juniper Networks. Dell SonicWALL dominates PAN in performance, scalability on the high end and is much more networking feature rich on the low-end plus recently, edged them out with the SuperMassive™ 10800 as the Highest Overall Next-Gen Firewall Recommended by NSS Labs in the 2012 Next-Gen Firewall Security Value Map.

Dell SonicWALL® vs. Palo Alto Networks SWOT

| Strengths | Weaknesses |
|---|---|
| • NSS Labs Recommended NGFW<br>• SuperMassive™ E10800 running SonicOS is the Highest Overall Protection Next-Gen Firewall Recommended by NSS Labs in the 2012 Security Value Map<br>• Richer networking feature set<br>• Strong DPI performance and capabilities<br>• Firewall portfolio breadth<br>• DPI and App Control capabilities on products down to the $1-5k range<br>• DPI and App Control at 30+ Gbps<br>• Leader in the 2012 UTM Magic Quadrant<br>• Native Apple iOS and Google Android SSL VPN client<br>• Ease of Use & Configuration<br>• Proven scalable centralized management ( Dell SonicWALL Global Management System) | • “Leader” position in the 2011 Enterprise Firewall Gartner MQ<br>• Great name recognition in enterprise firewall accounts<br>• Powerful NGFW demo tools<br>• Focus on firewall technology (sole product line) |
| **Opportunities** | **Threats** |
| • Dell SonicWALL demonstrated as a viable enterprise NGFW by NSS Labs<br>• Dell SonicWALL becoming a recognized NGFW vendor<br>• With the SMB NGFW offering, Dell SonicWALL can become the one-stop-shop for<br>• Diverse product line (Email Security, Wireless, Dedicated SSL VPN)<br>• PAN has serious IP legal issues with Juniper | • PAN moves very quickly to resolve security and feature deficiencies<br>• Strong mobile NAC and LAN NAC initiative<br>• Virtualization (Multi-tenancy on a single device)<br>• Filed for IPO, will have more funding<br>• Starting to move both up and down in the product offerings – may eventually match Dell SonicWALL breadth |

## Cisco

Cisco is synonymous with networking, and their name and past reputation continue to carry the ASA firewall line in many environments.  The large number of Cisco certified professionals and the wide portfolio of networking products guarantee that Cisco firewalls will continue to show up in competitive situations. However, Cisco has neglected its ASA product line for years, and has lost a lot of ground in the firewall space, allowing companies like Dell SonicWALL, Fortinet and Palo Alto Networks to do very well in replacing older Cisco environments.  **This will continues to be a very healthy opportunity, as Dell SonicWALL's success rate in beating Cisco head on is very high.** Cisco finally responded at RSA 2012 by releasing ASA-CX series of firewalls, CX standing for "Context Aware", or Cisco's implementation of application control.  One of the weakest points for Cisco, besides their lack of in-house security research and expertise, is the limited hardware which on the mid-range forces a mutually exclusive choice between intrusion prevention and threat prevention.  The high end range of ASA firewalls did not have either of the services as an option until recently, when an IPS module became available for the 5585-X firewalls.

Dell SonicWALL® vs. Cisco SWOT

| Strengths | Weaknesses |
|---|---|
| • NSS Labs Recommended NGFW<br>• SuperMassive™ E10800 running SonicOS is the Highest Overall Protection Next-Gen Firewall Recommended by NSS Labs in the 2012 Security Value Map<br>• Rich SMB Feature Set<br>• Attractive pricing for the feature set in SMB with a lower TCO than Cisco<br>• Strong market position in SMB UTM<br>• Strong brand in SMB UTM<br>• Strong DPI performance and capabilities<br>• DPI capabilities on the entire product line, no additional hardware necessary<br>• In-house security research & security IP ownership(DPI services) | • Cisco still a de-facto name in network security<br>• Cisco Strong Enterprise Market Share<br>• Cisco has strong worldwide presence<br>• Cisco has Broader Support Offering including Professional Services<br>• Cisco has a full network product portfolio (switches, routers, etc.) |
| **Opportunities** | **Threats** |
| • Channel increasingly seeing ASA as an aging product line<br>• Acceptance of UTM/DPI/NGFW by increasingly larger organizations<br>• Lack of application control on ASA series as it becomes a requirement<br>• Dell SonicWALL Ease of Use trumps Cisco's configuration complexity | • Cisco's refreshed ASA-CX Firewall line claims Application Control, but is not yet proven in the market<br>• Cisco attacking SMB market with the SA product line (Linksys Based)<br>• Increased collaboration with IronPort may result in new products/technology<br>• Strong Virtualization Network & Security Portfolio (VM Appliance & Multi-Tenancy on a single device) |

## Fortinet

Between 2002 and 2010, Fortinet was the most direct competitor for Dell SonicWALL in the UTM space. Dell SonicWALL and Fortinet competed to displace Cisco and Checkpoint in UTM deals and were very successful at doing so. While both the firewall and the overall product portfolios of Fortinet are much wider than those of Dell SonicWALL at this point, Dell SonicWALL can compete extremely well against Fortinet **when the customer wants Deep Packet Inspection (IPS, App control or AV).** This is due to the fact that Fortinet is based on proprietary ASICs, which are extremely fast for stateful packet inspection (what Check Point invented 15 years ago, their products take a *severe* performance hit as soon as Deep Packet Inspection security is enabled. In some cases, the performance hit is approximately 95+%, based on Fortinet's own admissions. Fortinet is often aggressive on pricing. Fortinet has an in-house security research team and despite their performance limitations, scored well on the recent NSS Labs Next-Generation Firewall Security Value Map, although with a number of caveats that should warn any prospective buyer.

Dell SonicWALL® vs. Fortinet SWOT

| Strengths | Weaknesses |
|---|---|
| • NSS Labs Recommended NGFW<br>• SuperMassive™ E10800 running SonicOS is the Highest Overall Protection Next-Gen Firewall Recommended by NSS Labs in the 2012 Security Value Map<br>• Strong market position in SMB UTM<br>• Strong brand in SMB UTM<br>• Strong DPI performance and capabilities<br>• RFDPI Technology (any port/any direction/any size/TCP Stream inspection)<br>• NGFW Feature-set and performance to back it up<br>• Native SSL VPN client on Apple iOS and Google Android<br>• Better architecture (multi-core) for NGFW, more adaptable | • Broad product line into carrier/large enterprise chassis products<br>• "Challenger" and "Leader" positions in Enterprise Firewall/SMB UTM Firewall Gartner Magic Quadrants, respectively<br>• Configurable products, including Chassis<br>• Certifications (Multiple ICSA Certs, DoD)<br>• Strong market position in Enterprise Firewalls |
| **Opportunities** | **Threats** |
| • Growing recognition of DPI and growing WAN speeds will favor Dell SonicWALL products<br>• App control & visualization becoming an increasingly demanded feature<br>• Many Fortinet features cannot function simultaneously | • Fortinet may resolve DPI performance issues<br>• Fortinet may add good application control – already some app control capabilities<br>• Have virtual firewall (VM Appliance & multi-tenancy on a single device) capability across the product line |

## WatchGuard

WatchGuard is a UTM company that during a time of financial trouble was taken private and is still struggling to recover.  Despite a portfolio of firewalls that very closely resemble the Dell SonicWALL lineup, we rarely come across WatchGuard in competitive situations in the United States.  However, WatchGuard is said to have a very strong presence in Germany.  Based on X86 hardware, WatchGuard has recently entered the NGFW market, but was for some reason absent from the recent NSS Labs Next-Generation Firewall Security Value Map test.  Usually it's fairly easy to beat WatchGuard on features and Deep Packet Inspection performance.

Dell SonicWALL® vs. WatchGuard SWOT

| Strengths | Weaknesses |
|---|---|
| • NSS Labs Recommended NGFW<br>• SuperMassive™ E10800 running SonicOS is the Highest Overall Protection Next-Gen Firewall Recommended by NSS Labs in the 2012 Security Value Map<br>• Strong DPI performance and capabilities<br>• Better architecture (Multi-Core) for NGFW, more adaptable<br>• Native Apple iOS and Google Android SSL VPN client<br>• Larger signature set & coverage | • Strong configuration template support in the management UI<br>• Drag & drop VPN configuration |
| **Opportunities** | **Threats** |
| • Dell SonicWALL has a great NSS Labs NGFW test result while WatchGuard was absent<br>• WatchGuard cannot scale as high as Dell SonicWALL firewalls<br>• Dell SonicWALL is becoming a recognized NGFW vendor | • WatchGuard launched a re-branded parallel product line branded XTM and positioned as an NGFW<br>• Virtual firewall appliance – can run in cloud environments<br>• WatchGuard is moving aggressively into the NGFW space |

## NETGEAR

NETGEAR is best known for consumer off-the-shelf firewalls, but has recently started pursuing the low end of Dell SonicWALL's SMB business with its own UTM offering. Dell SonicWALL almost never comes across NETGEAR in competitive deals, most likely indicating that they're mostly relying on a few small partners and mainly a retail/DMR channel for very price sensitive customers. NETGEAR does not have its own security research team and licenses much of the security capabilities from 3rd parties. Their firewalls are very feature deficient and are only applicable in the simplest environments where price is the primary consideration.

Dell SonicWALL® vs. NETGEAR SWOT

| Strengths | Weaknesses |
|---|---|
| • NSS Labs Recommended NGFW<br>• SuperMassive™ E10800 running SonicOS is the Highest Overall Protection Next-Gen Firewall Recommended by NSS Labs in the 2012 Security Value Map<br>• Proven SonicOS architecture is at the core of every Dell SonicWALL® firewall from the SuperMassive™ E10800 to the branch/SOHO TZ105.<br>• More complete networking and firewall feature set<br>• Leadership position in the 2012 UTM Magic Quadrant<br>• Product Line Breadth - DPI and App Control capabilities from SMB to Carrier/Enterprise<br>• FIPS and Common Criteria certifications<br>• Native Apple iOS and Google Android SSL VPN client<br>• Strong & proven centralized management<br>• In-house security research & security IP ownership (DPI services) | • Wider distribution through retail channel<br>• NETGEAR a more recognized name in consumer networking space<br>• "Niche" position in the 2012 SMB UTM Firewall Gartner MQ |
| **Opportunities** | **Threats** |
| • Professional grade firewall vs. consumer grade firewall messaging<br>• Proven deployments in SMB, Large business & Enterprise<br>• NETGEAR does not have 1Gbps+ products | • NETGEAR is aiming for the Dell SonicWALL SMB market |

## Barracuda Networks

Barracuda Network's firewall line comes from the 2009 acquisition of Phion, an Austrian firewall company. While on paper and datasheets the product may look decently feature-capable, their market share does not even register on the Infonetics firewall market research report and Dell SonicWALL corporate has **never** come across a competitive deal in which Barracuda was the other competitor running in the consideration.

Dell SonicWALL® vs. Barracuda SWOT

| Strengths | Weaknesses |
|---|---|
| NSS Labs Recommended NGFW<br>SuperMassive™ E10800 running SonicOS is the Highest Overall Protection Next-Gen Firewall Recommended by NSS Labs in the 2012 Security Value Map<br>Strong market position in SMB UTM<br>Strong brand in SMB UTM<br>DPI capabilities on the entire product line, no additional hardware necessary<br>Leadership position in the 2012 UTM Magic Quadrant<br>In-house security research & security IP ownership (DPI services) | Barracuda has a strong IM recording technology<br>Not included on the 2012 SMB UTM Firewall Gartner MQ |
| **Opportunities** | **Threats** |
| Dell SonicWALL has a great NSS Labs NGFW SVM test result while Barracuda was absent<br>Dell SonicWALL becoming a recognized NGFW vendor | Available as a virtual appliance<br>User their anti-spam market position to push firewalls<br>Developing NGFW feature set and has strong advertising and branding<br>Easy & fast evaluation program |

## Competitive Feature Comparison Table

| Security Services | SonicWALL | Fortinet | Checkpoint | Cisco | Juniper | PAN | Watchguard | Barracuda | NETGEAR |
|---|---|---|---|---|---|---|---|---|---|
| Content/URL Filtering (CFS) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Gateway Anti-Malware (Anti-Virus/Spyware) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Integrated Intrusion Prevention | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| App Flow Visualization | Yes | No | Yes | No | No | Yes | No | No | No |
| Application Control | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | No |
| Anti-Spam | Yes | Yes | Yes | Yes | No | No | Yes | Yes | Yes |
| SSL Inspection (DPI-SSL) | Yes | Yes | Yes | No | No | Yes | Yes | No | No |
| Enforced Client AV (McAfee/Kaspersky) | Yes | Yes | No | No | No | Yes | No | No | No |
| Cloud AV/Threat Prevention | Yes | No | Yes | No | No | Yes | No | No | No |
| **SSL VPN  Remote Access** | **SonicWALL** | **Fortinet** | **Checkpoint** | **Cisco** | **Juniper** | **PAN** | **Watchguard** | **Barracuda** | **NETGEAR** |
| SSL VPN Support | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| iOS SSL VPN Client Support | Yes | No | Yes | Yes | Yes | No | No | No | No |
| Android SSL VPN Client Support | Yes | No | No | No | No | No | No | No | No |
| SSL VPN Endpoint Enforcement | Pending | Yes | Yes | No | Yes | Yes | No | No | No |
| SSL VPN Thin Client Support | Yes | No | Yes | Yes | No | No | No | No | No |
| **Networking Features** | **SonicWALL** | **Fortinet** | **Checkpoint** | **Cisco** | **Juniper** | **PAN** | **Watchguard** | **Barracuda** | **NETGEAR** |
| 10GbE Support | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Wireless AP Support | Yes | Yes | No | Yes | Yes | No | no | Yes | No |
| Integrated Wireless Support | Yes | Yes | Yes | Yes | No | No | Yes | Yes | Yes |
| Centralized Firewall Management | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Virtual Firewalls (Multi-Tenancy) | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Virtual Firewalls (VM Appliance) | No | Yes | Yes | No | Yes | No | Yes | Yes | No |
| WAN Load Balancing | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| WAN Failover | Yes | Partial (2) | Yes | No | Yes | No | Yes | Yes | No |
| DNS Proxy | No | Yes | Yes | TBD | No | Yes | Yes | No | No |
| DynDNS Support | Yes | Yes | No | No | No | No | Yes | Yes | Yes |
| No File Size Limitation on DPI Scanning | Yes | Partial | No | No | Partial | Yes | Partial | No | No |
| USB 3G/4G Failover | Yes | Yes | Yes | Yes | Yes | No | Yes | TBD | No |
| IPSec VPN (Site to Site) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| IPSec VPN (Client) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| VLAN (802.1q) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Single Sign On  (SSO) Authentication | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Syslog Reporting | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Netflow Reporting | Yes | No | No | Yes | No | Yes | No | No | No |
| IPFIX Reporting | Yes | No | No | No | No | No | No | No | No |
| IPv6 Support | Yes* | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| BGP Support | Yes* | Yes | Yes | Yes | Yes | Yes | No | Yes | No |
| OSPF/RIP | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| SNMPv3 | Pending | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| Full Command Line Interface (CLI) | Pending | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Active/Passive + Stateful Sync | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Active/Active DPI Offloading + State Sync. | Yes | No | No | No | No | No | No | No | No |
| Active/Active Clustering | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No |

## Dell SonicWALL Security Subscription Services

Out of the box, Dell SonicWALL firewalls act as powerful traditional firewalls with a wide array of networking and remote connectivity features.  The real security power of Dell SonicWALL firewalls is unlocked when customers purchase and enable any of the security subscription services.

The core subscription services and security features that they enable are:

### Intrusion Prevention Service (IPS)

This security service is fundamental to an effective security stance and forms the backbone of gateway network security by protecting client machines and servers against a wide range of attacks.  These attacks target vulnerabilities and other software mistakes in common client and server software in order to open wider "doors" to plant more insidious and persistent malware such as Trojans, bots, key loggers, etc.

### Gateway Anti-Virus & Anti Spyware with Cloud AV (sometimes Gateway Anti-Malware or Threat Prevention)

This service scans every byte of every network connection coming across the firewall on all ports for known viruses, key loggers, Trojans, ransom-ware, Fake AV and other malware, and is one of the most effective methods of preventing virus infections on a network.  The firewall will interrupt network connections when it detects a virus and will inform the user. The firewall also consults with the Dell SonicWALL Cloud Anti-Virus infrastructure to reference additional 8 Million malware signatures.

### Application Intelligence, Control & Visualization (AICV)

This is the subscription service that is most commonly associated with Next-Generation Firewall (NGFW) capabilities that enable the firewall to fingerprint application traffic by application DNA, removing the dependence on ports and protocols for effective network control.  This type of capability is sweeping the network security market and is one of the most differentiating and attention capturing capabilities in firewalls today.

There are several components to this service:

- **Application Control** – the ability to allow Facebook, but block Zynga® games.  The ability to block P2P Traffic and to throttle down streaming video while prioritizing business applications
- **Application Intelligence/Visualization** – The ability to literally see app traffic classification in real-time and to be able to quickly diagnose and identify problematic application usage or inappropriate bandwidth usage.
- **Geo-IP Recognition - The** firewall can identify the country of origin/destination for connections and allows the administrator to create policies based on such origin.  For example, a small law firm operating locally in Smallville, CA can block all connections coming from China or Eastern Europe for increased security.

### Content & URL Filtering Service (CFS)

The ability to block traffic to sites based on categories, users and schedules.  This is a mandatory subscription service in Educational and Government verticals, and is also frequently deployed by private corporations to enforce corporate policy.

### Comprehensive Anti-Spam Service (CASS)

Utilizing the intelligence from our Email Security solution, Dell SonicWALL firewalls can turn away 90%+ of bad email traffic at the gateway based on the reputation alone and before it can consume valuable internal bandwidth.  The remaining email traffic is sent to the Dell SonicWALL cloud servers to run through the full analysis by the Dell SonicWALL email security products. This gateway anti-spam feature is aimed at companies with less than 250 people.

**SSL Decryption with Deep Packet Inspection (DPI-SSL)**

The ability to decrypt incoming and outgoing SSL traffic in order to perform Data Leakage Prevention (DLP) in addition to blocking attacks and threats (viruses) that may come in over encrypted links.

**Enforced Client Anti-Virus (Enforced AV)**
Dell SonicWALL® Enforced Client Anti-Virus and Anti-Spyware, working in conjunction with Dell SonicWALL firewalls, provides comprehensive gateway-enforced virus and spyware protection for desktops and laptops. With this solution, Dell SonicWALL firewalls confirm that all computers have the latest version of anti-virus and anti-spyware software installed and active before authorizing their access to the network. Automated updates of virus and spyware signatures eliminate the need for time-consuming machine-by-machine anti-virus deployments. Dell SonicWALL Enforced Client Anti-Virus and Anti-Spyware software is available for purchase with either McAfee® or Kaspersky® anti-virus engines.

All Dell SonicWALL firewalls can also act as intelligent controllers for Dell SonicWALL **Wireless Access Points (SonicPoints)** and for **WAN Acceleration Appliances (WXA).** Details on both are listed in separate sections below.

## Dell SonicWALL "Clean Wireless" with Wireless Access Points (SonicPoints)

Laptop shipments have exceeded desktop shipments several years ago, and at this point tablets are about to exceed shipments of laptops. With the proliferation of mobile devices, wireless access is no longer a convenience, but is now a requirement in virtually every network. All Dell SonicWALL firewalls can be configured to operate as wireless controllers and can be extended with Dell SonicWALL access points called SonicPoints.

SonicPoints are fully configured and controlled by firewalls, and can provide seamless wireless access for buildings of various sizes. Dell SonicWALL's Clean Wireless technology is a combination of wireless accessibility and security. Clients connected to SonicPoints are secured and isolated from each other, with traffic traveling back to the firewall for security inspection before going out either to the internet or to the other clients on the network.

## Customer Pain Points

- Wireless Access for a building that is too large for integrated wireless on the firewall
- Need for guest wireless without granting access to the internal network
- Need to extend wireless in a large warehouse, campus, office building
- Need to perform periodic Rogue Access Point detection for PCI-DSS Compliance

There are three key models:

SonicPoint-

SonicPoint-Ne

SonicPoint-N Dual Radio

**SonicPoint-Ni**: The entry level SonicPoint capable of Dual-Band 802.11 a/b/g/n access and 3x3 MIMO with internal antennas. The clean and un-intrusive design is ideal for deployments in offices and hospitals. Ships with a plastic faceplate to completely obscure flashing LEDs (important for hospitals)

**SonicPoint-Ne**: The mid-range SonicPoint capable of Dual-Band 802.11 a/b/g/n access and 3x3 MIMO with external antennas. Due to the presence of external antennas, it can be deployed in more versatile environments. Powered by either an 802.11af PoE injector or an included power supply. Ships with a plastic faceplate to completely obscure flashing LEDs (important for hospitals)

**SonicPoint-N Dual Radio**: as the name suggests, this is the high end Dell SonicWALL SonicPoint and contains two radios that can operate simultaneously on the 2.4 and the 5.0 GHz spectra. This allows an organization to provide connectivity to legacy 802.11 b/g/n devices while allowing newer clients to connect on the faster and cleaner 5.0 GHz 802.11n spectrum. Powered by an 802.11at PoE injector or an included power supply. Ships with a plastic faceplate to completely obscure flashing LEDs (important for hospitals) and is often deployed in retail locations for uninterrupted wireless access on the first radio with simultaneous Rogue Access Point detection scanning on the second radio for PCI-DSS reporting.

**Dual-Band**: The ability for the wireless radio to switch between the 2.4 GHz band and the 5.0 GHz bands. The radio can operate **EITHER** on the 2.4GHz band or the 5.0 GHz band

- The 2.4 GHz band is the legacy band and is fairly noisy. It is used for 802.11 b/g and compatibility mode 802.11n connectivity
- The 5.0 GHz band is less noisy, but requires newer clients. It is used for 802.11 a/n connectivity

**Dual-Radio:** The SonicPoint has two radios and can simultaneously operate on both the 2.4 GHz and the 5.0 GHz bands.

- **VAP:** Virtual Access Point – SonicPoints can emulate multiple wireless networks, allowing for different security policies and access rights to be granted to different classes of users. For example, the same access point can host a "Guest Wireless" and "Dell SonicWALL Wireless" networks, with the former providing only access to the internet and the latter granting access to the internal network. The fact that this can be achieved on a single access point eliminates the need to purchase additional equipment.
- **3x3/2x2 MIMO:** 3x3 or 2x2 Multiple-In/Multiple-Out antenna technology. Communicates how many simultaneous channels the radio is capable of operating. More simultaneous communication channels translate to higher throughput and more wireless clients.
- **PoE: Power over Ethernet** –for convenience and ease of deployment, access points can be powered solely by the RJ45 data cable if connected to a correct switch or a PoE injector. There are two types of PoE injectors that Dell SonicWALL ships: 802.11af and 802.11at, the latter being more powerful.

### Clean Wireless & SonicPoint Benefits

- Secure 802.11 a/b/g/n Wireless connectivity with Roaming – SonicPoints support
- Ability to have multiple wireless networks on the same physical infrastructure – Virtual Access Points (VAP)
- Guest access & authentication
- Client isolation

## Dell SonicWALL Access Point Competition

Dell SonicWALL does not sell SonicPoints by themselves, since they need a firewall in order to provide real benefits. Therefore, competitive situations usually arise when a competing firewall vendor is also providing wireless access points or when a customer wants to roll out a wireless deployment, but choses to simultaneously upgrade the firewall infrastructure instead of buying a dedicated wireless solution such as Aruba.

Dell SonicWALL at the moment scales up to 128 access points on the largest devices, and does not compete in environments that require a larger number of access points.

## Dell SonicWALL WAN Acceleration (WXA)

In today's distributed enterprise, applications such as Microsoft® SharePoint and Windows® File Share transmit an increasing number of files and data sets over Wide Area Networks (WANs), overburdening available WAN bandwidth. To make matters worse, these collaboration applications can inefficiently retransmit entire files (rather than just incremental changes) multiple times, unnecessarily increasing WAN traffic. IT often responds by expending budget on more bandwidth or enhanced services. Alternatively, WAN acceleration technology can resolve the problem by allowing more efficient utilization of the existing network bandwidth.

The Dell SonicWALL WAN Acceleration Appliance (WXA) Series significantly enhances WAN application performance and improves the end user experience for small- to medium-sized organizations with remote and branch offices.

- After initial data transfer, dramatically reduces subsequent traffic by transmitting only new or changed data
- Integrated add-on to Dell SonicWALL E-Class Network Security Appliance (NSA), NSA and TZ Series firewalls
- Streamlines deployment, configuration, routing and management of WAN acceleration
- Available as  hardware appliances, virtual appliance or Live CD

### WAN Acceleration Benefits

- Improve performance of business applications
- Optimize response times for critical applications
- Reduce bandwidth consumption
- Reduce associated bandwidth cost
- Make the network appear faster

### Customer Pain Points

The growth in the number of applications being used by companies is outpacing the bandwidth requirements for many organizations. One reason could be cost. IT organizations may not have the on-going budget to increase bandwidth for all locations. There could also be infrastructure limitations, which might not allow for higher Internet bandwidth to be available.

Traditional Quality of Service might be ineffective and allocating and controlling bandwidth. Companies need to look for products that support the ability to fingerprint specific applications and allow network administrators to either block the application out right or provide some bandwidth controls.

Applications that may have been designed to work great on Local Area Networks where bandwidth is higher and latency is lower, may not be suited to work in situations where the bandwidth is lower and latency is higher. In these cases where latency is high, the application may seem slow or even non-responsive.

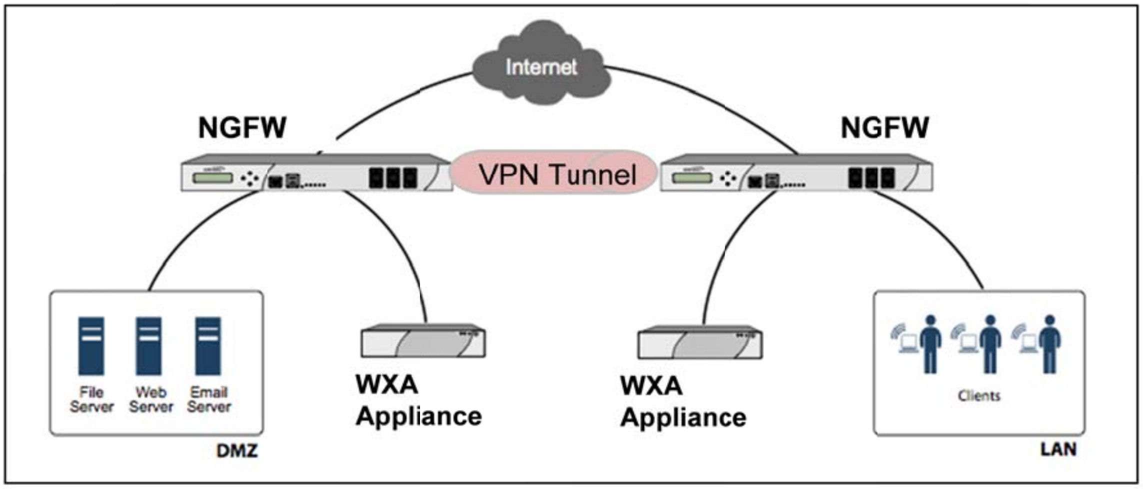
Redundant traffic is also an issue. If the same data is moving between offices, WAN Acceleration can help reduce the amount of data by only sending the delta.

## Target Customers

- Existing Dell SonicWALL Next-Generation Firewall customers
- Customers that have multiple office locations using VPN or MPLS (dedicated WAN links)
- Customers that may have looked at other WAN Acceleration solutions, but found budgetary issues

## Qualifying Questions

- Are your network bandwidth requirements outpacing your current service plan?
- Would you like to reduce bandwidth consumption and cost without paying your service provider more money to increase capacity?
- Do your remote office employees complain that the network is slow?
- Do your employees use applications such as Microsoft Windows File Sharing, SharePoint, Office or FTP?



Solution Requirements

- 2 Dell SonicWALL Next-Generation Firewalls (TZ, NSA, E-Class NSA)
- 2 Dell SonicWALL WXA Appliances (Software or Hardware)
- VPN tunnel or dedicated WAN link (e.g. MPLS) between locations

|  | WXA 500 (Live CD) | WXA 2000 | WXA 4000 | WXA 5000 (Virtual Appliance) |
|---|---|---|---|---|
| Min. SonicOS Version | 5.8.1 | 5.8.1 | 5.8.1 | 5.8.1 |
| Recommended Users[1] | 20 | 120 | 240 | 360 |
| Max WAN Accel. Flows | 100 | 600 | 1200 | 1,800 |
| Byte Caching | Yes | Yes | Yes | Yes |
| TCP Acceleration | Yes | Yes | Yes | Yes |
| Compression | Yes | Yes | Yes | Yes |
| WFS Acceleration | Yes[2] | Yes | Yes | Yes |
| Visualization | TCP/WFS | TCP/WFS | TCP/WFS | TCP/WFS |

1. Max users may vary depending on the number of flows per users.
2. WFS Acceleration is available only when the Live CD image is installed on the provided hardware.

## Competitive Overview

The Wan Acceleration solution that Dell SonicWALL has brought to market is very unique in that we integrate the WXA solution with the Dell SonicWALL Next-Generation Firewall. As far as the competition for WAN Acceleration we've run into solutions from Riverbed, Bluecoat and Cisco. Below is some high level messaging on how to differential Dell SonicWALL from the various competitors.
Integrated management with Dell SonicWALL Next-Generation Firewalls for easy deployment and ongoing management

- Focus on the Dell SonicWALL solution that provides both traffic shaping and traffic acceleration
- Dell SonicWALL has a more economical solution for branch/remote offices

## Dell SonicWALL Email Security Product Line Overview

While most businesses now have some type of anti-spam protection, many must deal with cumbersome management, frustrated users, inflexible solutions, and a higher-than-expected total cost of ownership. SonicWALL® Email Security can help. Elegantly simple to deploy, manage and use, award-winning SonicWALL Email Security solutions employ a variety of proven and patented technology designed to block spam and other threats effectively, easily and economically.

SonicWALL Email Security can be broadly classified as offering inbound and outbound email protection.

In terms of INBOUND protection, at a high level, the product uses two broad methodologies, 'reputation management' and 'content management'.

- SonicWALL GRID technology performs rigorous testing and evaluation of millions of emails every day, and then reapplies this constantly-updated analysis to deliver exceptional spam-blocking results. Every five minutes, the dynamic SonicWALL GRID Network automatically updates SonicWALL GRIDprint and IP reputation information for each SonicWALL email protection solution, as well as user and group LDAP (Light Weight Directory Access Protocol) entries; spam word-and-phrase content; and SonicWALL GRID Anti-Virus and McAfee and/or Kaspersky anti-virus signatures as required.

- Advanced Reputation Management rejects more than 80% of known junk mail upon connection. SonicWALL Advanced Reputation Management utilizes not only a message's sender IP reputation, but also the reputation of its content, structure, links, images, attachments and more. Moreover, Advanced Reputation Management also provides directory harvest attack (DHA) protection, Denial of Service (DoS) protection, backscatter/NDR protection and more, all with comprehensive logging and reporting.
- Advanced Content Management cleans up the remaining messages that come through the Advanced Reputation Management by using a proprietary and patented technique that improves upon traditional Bayesian scanners (it's called "Adversarial Bayesian"). This allows us to clean up >99% of email threats – one of the highest in the industry – while minimizing false positives. Advanced Content Management also offers policy rules to block, allow or route incoming messages based on 15 different email attributes. In the outbound side, once again, the product functionality can be broadly categorized into two functions of namely compliance defense management and threat management.
- Compliance Defense Management offers advanced detection and routing techniques for email compliance management, including compliance dictionaries, record-id (pattern) matching, encryption routing, archive storage/retrieval routing, and approval box routing.

OUTBOUND Threat Management streamlines outbound email policy management. For instance, administrators can easily customize rules to simply detect and block specific types of attachments; re-route e-mail to competitors; or check all outbound e-mail for specific words and phrases. SonicWALL Email Security solutions protect your email server's IP reputation by detecting and stopping zombie generated outbound spam, phishing and virus email.

SonicWALL Email Security can be flexibly deployed as a SonicWALL Email Security Appliance, as a software application on a third party Windows® server, or as a SonicWALL Email Security Virtual Appliance in a VMW® environment.

- Email Security Appliances - Businesses with 25 users or more that desire complete inbound and outbound email protection on one system, from one vendor, can benefit from a SonicWALL Email Security appliance with a hardened Linux-based OS.
- Email Security Software (for Windows Servers and SBS) - For those businesses that standardize on specific hardware, have existing monitoring and backup systems or just want the ultimate in deployment flexibility, SonicWALL Email Security Software is an ideal solution.
- Email Security Virtual Appliance (on VMware) - The SonicWALL Email Security Virtual Appliance provides the same powerful protection as a traditional SonicWALL Email Security appliance, only in a virtual form, to optimize utilization, ease migration and reduce capital cost.
- Anti-Spam Desktop - Single users and small offices of less than ten users should consider SonicWALL Anti-Spam Desktop for client-based, real-time protection against spam and phishing email. Extremely affordable, highly effective and easy to install, SonicWALL Anti-Spam Desktop blocks spam and phishing

email on Windows-based desktops or laptops that use Microsoft Outlook, Outlook Express or Win Mail to receive email. The subscription service works with Exchange, POP or IMAP-based inbound email.

- Comprehensive Anti-Spam Service (CASS) - As an add-on service for SonicWALL firewalls, CASS eliminates inbound junk email at the gateway, before it enters the network. CASS is ideal for smaller organizations and distributed enterprises of up to 250 users that receive email at multiple locations and need gateway-based inbound email protection to reduce network traffic.

| Features | Email Security Appliance, Software, & Virtual Appliance | Email Security for SBS | Comp. Anti-Spam Service (CASS) | Anti-Spam Desktop |
|---|---|---|---|---|
| **Email Protection** | | | | |
| Advanced Reputation Management | | | | |
| *Sender IP Reputation* | Yes | Yes | Yes | Yes |
| *DHA, DoS and NDR Protection* | Yes | Yes | N/A | - |
| Advanced Content Management | | | | |
| *GRIDprint Reputation Services* | Yes | Yes | Yes | Yes |
| *SonicWALL GRID Anti-Virus* | Yes | Yes | Yes | Yes |
| *Patented Phishing Detection Technology* | Yes | Yes | Yes | Yes |
| Policy Rules for Users, Groups or All Users | Yes | Yes | Yes | Yes |
| **Optional Services Available** | | | | |
| McAfee A/V with SonicWALL Time-Zero | Yes | - | - | - |
| Kaspersky A/V with SonicWALL Time-Zero | Yes | - | - | - |
| Email Compliance | Yes | - | - | - |
| **Easy Administration** | | | | |
| Installation and Configuration Time | 1 Hour | 1.5 Hours | 10 Min. | 10 Min. |
| Reputation Auto-Updates | Yes | Yes | Yes | Yes |
| Anti-Spam Auto-Updates | Yes | Yes | Yes | Yes |
| GRID A/V Auto-Updates | Yes | Yes | Yes | - |
| Customize, Schedule & E-mail 30+ Reports | Yes | Yes | Basic Reports | View 4 Reports |
| Automatic Multi-LDAP Sync | Yes | Yes | Yes | - |
| Allow/Deny All End-User Controls | Yes | Yes | Yes | - |
| Per User Junk Boxes | Yes | Yes | Yes | Yes |
| Junk Button for Outlook® | Yes | Yes | Yes | - |
| Per User Anti-Spam Aggressiveness | Yes | Yes | Yes | Yes |
| Per User Allowed/Blocked Lists | Yes | Yes | Yes | Yes |
| Junk Box Summaries in 15 Languages | Yes | Yes | Yes | - |
| Judgement Details | Yes | Yes | Yes | - |
| Rapid Message Search Engine | Yes | Yes | Yes | - |
| Single Sign-on | Yes | Yes | Yes | - |
| **System Features** | | | | |
| Inbound & Outbound in the Same System | Yes | Yes | - | - |
| In-Memory MTA for Enhanced Throughput | Yes | Yes | Yes | - |
| Maximum Domains Supported | Unrestricted | Unrestricted | Unrestricted | Unrestricted |
| Scalable Split-mode Architecture | Yes | - | - | - |
| Clustering & Remote Clustering | Yes | - | - | - |
| Deployment Platform(s) | ES Appliance, Virtual Appliance, Windows Server | Mail Server | Firewall | Client |
| Junk Email Blocking Point | ES Appliance, Virtual Appliance, Windows Server | Mail Server | Firewall | Client |

| Platform | RAM (GB) | CPU (GHz) | DISK (GB) | RAID |
|---|---|---|---|---|
| ESA 3300 | 2 | Intel Celeron 440 2.0 GHz) | 250 | N |
| ESA 4300 | 4 | Intel Core 2 Duo 2.13GHz | 2x 250GB | Y |
| ESA ES8300 | 4 | 4 x 2.0 | 3 TB | Y |
| Email Security Virtual Appliance | Hypervisor ESXi™ and ESX™ (version 4.0 and newer)<br>Operating System Installed Hardened SonicLinux<br>Allocated Memory 2 GB (extendable)<br>Appliance Disk Size 80 GB | | | |
| Email Software Application | Server requires Windows Server 2003, 2008, 2010<br>Processor with a minimum 2 GHz; 3 GHz or faster recommended<br>2 GB of RAM minimum and 4 GB recommended.<br>Hard Disk: 80 GB minimum | | | |

| Platform | Suggested max # users | Key Feature Differences | Upgrade Factor |
|---|---|---|---|
| ESA 3300 Appliance | 1 to 1,000 | Baseline | |
| ESA 4300 Appliance | 1 to 5,000 | RAID - 1 | RAID Hardware, Faster CPU, More Memory |
| ESA ES 8300 Appliance | 1 to 10,000 | E-Class, RAID-5, Redundant Power | More RAM, Faster CPU, Expanded Storage, Redundant Power Supplies |
| Email Security Virtual Appliance | Hypervisor ESXi™ and ESX™ (version 4.0 and newer)<br>Operating System Installed Hardened SonicLinux<br>Allocated Memory 2 GB<br>Appliance Disk Size 80 GB | | |
| Email Software Application | Install the application on a Windows Server system.<br>Server requires Windows SBS/EB Server 2003 or 2008.<br>Minimum server requirements: 2 GB RAM, 2.66 CPU, 40 GB Free Disk. | | |

It is possible that a single Appliance, no matter how large, may not be sufficient to handle the amount of email received by an organization.  As the amount of spam email continues to increase the amount of email and email spam they receive daily is becoming increasingly an issue for many companies.  To address this issue, SonicWALL Email Security systems can be configured in a split-mode environment allowing multiple systems to be quickly added together to deliver a scalable solution.

## Customer Pain Points

The amount of spam has increased exponentially from 30 billion messages per day in 2005 to 183 billion messages per day in 2010. Spam continues to shift from an annoyance to a security threat resulting in approximately $1,243 per incident according to the FTC. Viruses and phishing attacks are evolving rapidly. There are new regulatory and legal requirements affecting organizations of all sizes requiring vigilance among enterprises to preserve and protect data. While most businesses now have some type of anti-spam protection, many must deal with cumbersome management, frustrated users, inflexible solutions, and a higher-than-expected total cost of ownership. Many businesses are migrating to cheaper delivery platforms with the advent of virtualization and cloud based offerings.

## Email Security Product Positioning and Key Messages

Email Security Product Positioning for SMB and Enterprise Customers

Simple to deploy, manage and use, award-winning SonicWALL Email Security solutions employ a variety of proven and patented technology designed to block spam and other threats effectively, easily and economically.

**Effective:** Spam evolves constantly. No single analytic technique is enough to stop it. SonicWALL, a leader in network security and data protection,  uses 14 different techniques–including advanced IP reputation, SonicWALL GRID print analysis, Adversarial Bayesian filtering, Image Inference analysis and more–to not only block spam, phishing and virus emails, but to also confidently ensure delivery of good email.

- Superior Anti-spam, anti-phishing & anti-virus protection
- Responsive to new attacks with multi-layered Anti-virus and spam protection  engines
- Powerful Policy and Compliance Management
- Complete Inbound and Outbound email protection

**Easily Managed:**  SonicWALL Email Security provides automated monitoring and alert reporting.  It also allows administrators to customize and distribute reports on threats, compliance, policy, connection management and more.

- Automated monitoring & reporting
- Advanced configurations
- Self-service for end-users

**Extensible:** SonicWALL offers a variety of anti-spam and email security solutions, including a hardware appliance, server software, a virtual appliance or a subscription service.

- Flexible platforms to choose from
- Highly Scalable

- Highly Redundant
- Proven Technology

## Email Security Product Positioning for Resellers and Managed Service Providers (MSPs)

Email Security is a mature market and most of the business growth is expected from:

- IT shift to Virtual infrastructure and cloud based services
- IT need for an effective product to handle the sophistication of evolving threats beyond just spam protection
- IT need for a scalable product to manage and store data as the volume of email grows

SonicWALL Email Security offers superior email protection and the most platform deployment choice. The same feature set is offered for three platforms: Windows, VMware and Hardware appliances. The product can be sold to address multiple sales trigger points:

- Re-sellers can sell the full email protection solution as part of their email server solution. (for example Exchange)
- A customer undergoing migration to a Virtual VMware platform can migrate from their existing email security solution to SonicWALL ES Virtual appliance
- Re-sellers selling SonicWALL firewall can sell the Comprehensive Anti-Spam service (CASS)  as part of the firewall  attach sale (CASS provides only inbound protection and is recommended for organization with less than 250 users)

For Dell partners who are MSPs, the SonicWALL Email Security solution offers a highly scalable and flexible product and licensing option to build their own cloud offering.

### Benefits:

- Centralized management of multiple domains to remove junk email for everyone
- Centralized email policies for everyone and/or client policies per domain/group/user
- Centralized reporting, with per-domain reporting
- Centralized control over outbound email can be used for some or all of the clients, and policy/routing can be applied on per-domain basis
- Allows email servers and LDAP servers to reside with the customer or with the MSP or in any combination
- Flexible expansion allows the MSP to start with scalable, failover-enabled, split-mode architecture
- Full user interface Re-branding for MSPs to promote their service offering

Note: MSP partners will also have the option of provisioning SonicWALL Hosted Email security (in beta)

## Email Security Competitive Position in the Market

SonicWALL Email Security primarily competes with Barracuda in the SMB market. Barracuda uses their marketing machine to generate a significant volume of leads, which they push, 100% to the channel. Barracuda uses open source software to build a cheaper solution and has a simple all-you-can-eat licensing model to provide an attractive offering in the SMB space.  SonicWALL's solution offers superior protection with multi-layer technology and services and an a la Carte licensing model.

Also, cloud based services, especially from Google Postini and McAfee MX-Logic, offer strong competition in the market place. SonicWALL is currently working on a cloud-based service which will initially be targeted at the SMB market.

**Barracuda**

Barracuda is a leader in email security in the SMB space. They are SonicWALL's key competitor and directly compete with SonicWALL head on with heavy advertising and offer a cost effective solution for the price-sensitive SMB customers.

Dell SonicWALL® vs. Barracuda SWOT

| **Strengths** | **Weaknesses** |
|---|---|
| • Strong brand recognition in the email security space<br>• Supports appliances, virtual appliances and hosted platforms<br>• Simple all-you-can-eat license model is effective in the price-sensitive SMB market<br>• Only industry provider to include home grown Email Encryption in the base subscription | • Uses open source security software such as spam assassin, Postfix MTA<br>• Low end appliance have poor functionality<br>• You need two boxes to do both inbound and outbound for low end appliances<br>• High availability is offered only in select models<br>• Basic virus filtering with no add-on options<br>• Limited branding – co-branding |
| **Opportunities** | **Threats** |
| • Focus on multi-layer AV protection using SonicWALL, McAfee and Kaspersky technology, superior to Barracuda's single technology, open source approach.<br>• Sell scalability, split-mode architecture, off appliance storage, full re-branding<br>• Emphasize MSP-rich functionality and flexible license model<br>• Highlight platform choices and full functionality on all models including entry appliances | • Simple license model befitting the transactional SMB market<br>• Customers who are very cost conscious are happy with 'Good enough' functionality<br>• Not enough differentiation to overcome the switching cost |

**WatchGuard**

WatchGuard is primarily a UTM vendor and entered the email security space by acquiring BorderWare in 2009. Unlike other vendors, WatchGuard offers content security (web and email security) in the same appliance. Also like SonicWALL, WatchGuard offers email security as a service (add-on) for their firewalls. This technology is offered through an OEM relation with CommTouch.

Dell SonicWALL® vs. WatchGuard SWOT

| **Strengths** | **Weaknesses** |
|---|---|
| • Combining web and content security into a single device at a low price point is attractive to SMB<br>• Offering the email security service on their low-end firewall models expands their reach to a broader audience<br>• DLP and policies can be shared across web and email settings<br>• Offers integrated email encryption with Voltage partnership on high-end models | • Just like Barracuda but to a lesser extent they stagger functionality based on the model, leaving low-end models with limited functionality<br>• Just hardware appliances with no software, cloud or virtual appliance offering<br>• Limited DLP and compliance functionality<br>• Flat pricing model per appliance leaves low-end customers paying more for less number of users and limited functionality.<br>• Basic virus filtering with no add-on options<br>• Hardware appliance specs don't compare well in the low end |
| **Opportunities** | **Threats** |
| • Focus on multi-layer AV protection using SonicWALL, McAfee and Kaspersky technology, superior to WatchGuard single technology approach.<br>• Sell scalability, split-mode architecture, off appliance storage, full re-branding<br>• Emphasize MSP-rich functionality and flexible license model<br>• Highlight flexible platform choices, especially virtual appliance<br>• Full functionality on all models including low-end appliances | • Simple license model befitting the transactional SMB market<br>• A good option for WatchGuard firewall customers<br>• Customers who are very cost conscious are happy with 'Good enough' functionality<br>• Not enough differentiation to overcome the switching cost |

**Fortinet**

Fortinet is also a firewall vendor that sells email security appliances. Fortinet also offers their anti-spam service as an add-on on their firewall, though the functionality is very limited with no quarantine box etc.

Dell SonicWALL® vs. Fortinet SWOT

| Strengths | Weaknesses |
|---|---|
| • Fortinet firewall brand is powerful and used to push Fortinet FortiMail.<br>• Feature-rich management interface<br>• Offers attractive per-appliance pricing | • Just hardware appliances and virtual appliance with no Windows software or cloud offering.<br>• Limited DLP and compliance functionality<br>• Basic virus filtering with no add-on options<br>• Hardware appliances specs don't compare well in the low end<br>• HA system is very expensive for low-end customers<br>• Easily configured Anti-Spam techniques are cloud based which introduces possible performance issues |
| **Opportunities** | **Threats** |
| • Focus on multi-layer AV protection using SonicWALL, McAfee and Kaspersky technology, superior to WatchGuard single-technology approach.<br>• Sell scalability, split-mode architecture, off appliance storage, full re-branding<br>• Emphasize MSP rich functionality and flexible license model<br>• Highlight flexible platform choices<br>• Full functionality on all models including low-end appliances | • Simple license model befitting the transactional SMB market<br>• A good option for Fortinet firewall customers<br>• Not enough differentiation to overcome the switching cost |

## NETGEAR

NETGEAR, like WatchGuard, offers content security (web and email security) in the same appliance. Also they offer email security as a service (add-on) on their firewalls. This technology is through an OEM relation with CommTouch, Sophos and Kaspersky.

Dell SonicWALL® vs. NETGEAR SWOT

| Strengths | Weaknesses |
|---|---|
| • Combining web and content security into a single device at a low price point is attractive to SMB<br>• Offering the email security service on their low-end firewall models expands their reach to a broader audience<br>• Unlike WatchGuard, NetGear provides better malware protection through their partnership with Kaspersky and Sophos | • Centralized reporting is offered only in higher-end models<br>• Just hardware appliances with no software, cloud or virtual appliance offering<br>• Limited DLP and compliance functionality<br>• No brand awareness in the Email Security space |
| **Opportunities** | **Threats** |
| • Sell scalability, split-mode architecture, off appliance storage, full re-branding<br>• Emphasize MSP-rich functionality and flexible license model<br>• Highlight flexible platform choices, especially virtual appliance<br>• Full functionality on all models including low-end appliances | • Simple license model befitting the transactional SMB market<br>• Customers who are very cost conscious are happy with 'Good enough' functionality |

### Cisco IronPort

Cisco IronPort is a leader in the midsize to large enterprise on-premises email security solution. IronPort initially focused on the enterprise market and have started focusing more on the SMB market since the Cisco acquisition.

Dell SonicWALL® vs. Cisco IronPort SWOT

| Strengths | Weaknesses |
|---|---|
| • Strong Market perception: “Enterprise company with a reputation for solid reliability, performance and scalability”<br>• IronPort consistently focuses on their core intellectual property - SenderBase and AsyncOS which allows them to achieve higher effectiveness and scalability<br>• Tight integration of encryption capabilities<br>• Gartner has consistently rated them as a leader over the past five years | • Complexity - IronPort’s products, while comprehensive, are complex to deploy and use<br>• Cisco solutions carry a very high list price relative to the market.<br>• IronPort's focus on the needs of large enterprises doesn't always scale down well for the midsize organization.<br>• Integration between even two IronPort appliances is poor |
| **Opportunities** | **Threats** |
| • Sell scalability, split-mode architecture, off appliance storage, full re-branding<br>• Out-of-box experience and simplicity caters to SMB needs<br>• Emphasize MSP-rich functionality and flexible license model<br>• Highlight flexible platform choices, especially virtual appliance<br>• Full functionality on all models including low-end appliances | • Highest employee head count dedicated to this market in the industry<br>• Cisco's  range of products makes it a strategic vendor for organizations looking to consolidate buying around fewer security vendors |

**Google Postini**

Postini offers a pure cloud-based solution and is a good fit for all size enterprise organizations considering enterprise Gmail and other Google SaaS offerings. Google has an enterprise-class product with strong SLAs but lacks good support model.

Dell SonicWALL® vs. Google Postini SWOT

| Strengths | Weaknesses |
|---|---|
| • Strong presence in both SMB, MSP and enterprise markets<br>• Google offers a compelling cloud portfolio with Google apps<br>• Fully featured product<br>• Strong international presence with ability to segregate traffic to different geographic locations. | • Poor technical support<br>• Google factor – Users are concerned about privacy issues when dealing with Google<br>• Google factor – Like Microsoft, Google continue to be a target of malicious attackers as it amasses more potentially lucrative information<br>• Complex setup and configuration<br>• No improvement on the product since the Google acquisition<br>• No on-premises solution |
| **Opportunities** | **Threats** |
| • Award winning 8x5 and 24x7 support options<br>• Sell scalability, split-mode architecture, off appliance storage, full re-branding<br>• Out-of-box experience and simplicity caters SMB needs<br>• Emphasize MSP rich functionality and flexible license model<br>• Highlight flexible platform choices, especially virtual appliance<br>• Full functionality on all models including low-end appliances | • Strong Google and Postini brand presence<br>• Google's push of Google Apps marginalizes the email security portion of the solution (Google can use Postini as a loss leader) |

### McAfee

McAfee has three different email security solutions in its portfolio due to acquisitions.  It has two on-premises solutions in McAfee Email Security Appliance and McAfee Email Gateway, formerly IronMail. McAfee also purchased MX-Logic which is a SaaS based email security solution. MX-Logic focuses on re-seller (MSP) community to reach the SMB market.

Dell SonicWALL® vs. McAfee SWOT

| Strengths | Weaknesses |
|---|---|
| • Strong presence in both SMB, MSP and enterprise markets<br>• Threat research team in McAfee is strong<br>• Flexible deployment options with both on-premises and cloud solutions<br>• Strong DLP and encryption functionality<br>• Enterprise credibility supported by IDC and Gartner | • Many partners dislike McAfee<br>• Three different products yet to be unified<br>• Intel acquisition of McAfee is viewed skeptically in the market place<br>• E-class product is known to be harder to install and manage |
| **Opportunities** | **Threats** |
| • Sell scalability, split-mode architecture, off appliance storage, full re-branding<br>• Out-of-box experience and simplicity caters SMB needs<br>• Emphasize MSP-rich functionality and flexible license model<br>• Highlight flexible platform choices, especially virtual appliance<br>• Full functionality on all models including low-end appliances | • MX-logic focuses on MSPs and SMB straight on in the market we operate and is a strong incumbent<br>• When McAfee combines its two on-premises  products, it can offer a very compelling solution for enterprises |

### Symantec

Symantec has a range of delivery platforms for its email security solution including hardware appliances, SaaS, virtual appliances (VMware), and software for Exchange and Domino. But unlike MX-logic which is tailored towards MSPs, Symantec's hosted solution (MessageLabs) is targeted toward enterprises.

Dell SonicWALL® vs. Symantec SWOT

| Strengths | Weaknesses |
|---|---|
| • Strong presence mid-market and enterprise markets<br>• Threat research team in Symantec is strong<br>• Flexible deployment options with both on-premises and cloud solutions<br>• Strong DLP and encryption functionality<br>• Enterprise credibility supported by IDC and Gartner | • Pricey for SMB<br>• Many products yet to be unified<br>• No real MSP focus |
| **Opportunities** | **Threats** |
| • Sell scalability, split-mode architecture, off appliance storage, full re-branding<br>• Out-of-box experience and simplicity caters SMB needs<br>• Emphasize MSP-rich functionality and flexible license model<br>• Full functionality on all models including low-end appliances | • Symantec  focuses on enterprise market and can use its strong brand to focus on the SMB market<br>• When Symantec combines its acquisition of different technologies like Vontu, PGP etc, it can offer a very compelling solution for enterprises |

**Email Security Competitive Matrix**

| Legend 🟢Full 🟡Partial ⭕No Support –Information Not Available | | SonicWALL | Barracuda | Fortinet | Postini |
|---|---|---|---|---|---|
| **Platform support** | Windows and Windows SBS | 🟢 | ⭕ | ⭕ | ⭕ |
| | Virtual Appliance (VMware) | 🟢 | 🟢 | 🟢 | ⭕ |
| | Hardware Appliance | 🟢 | 🟢 | 🟢 | ⭕ |
| | Firewall Appliance (add-on service) | 🟢 | 🟢 | 🟢 | ⭕ |
| | SaaS Platform (in beta for SonicWALL) | ⭕ | 🟢 | ⭕ | 🟢 |
| **Spam and Email protection** | Reputation Management | 🟢 | 🟢 | 🟢 | 🟢 |
| | Content based spam filtering | 🟢 | 🟢 | 🟢 | 🟢 |
| | Phishing detection | 🟢 | 🟢 | 🟢 | 🟢 |
| | Policy Rules for Users, Groups or All Users - on all models | 🟢 | 🟡 | 🟢 | 🟢 |
| | DHA, DoS and NDR Protection for all models | 🟢 | 🟢 | 🟢 | 🟢 |
| **Email Anti-Virus** | Basic Email Anti-Virus | 🟢 | 🟢 | 🟢 | 🟢 |
| | Premium Anti-Virus with McAfee, Kaspersky add-ons | 🟢 | ⭕ | ⭕ | ⭕ |
| **Compliance & DLP** | Email Compliance in all models | 🟢 | ⭕ | 🟢 | 🟢 |
| | Integrated Email Encryption | ⭕ | 🟢 | ⭕ | 🟢 |
| **Administration Capabilities** | Customize, Schedule & E-mail 30 Reports | 🟢 | 🟢 | 🟢 | 🟢 |
| | Automatic Multi-LDAP Sync for all models | 🟢 | 🟡 | 🟢 | 🟢 |
| | Allow/Deny All End-User Controls for all models | 🟢 | 🟡 | 🟢 | 🟢 |
| | Per User Junk Boxes for all models | 🟢 | 🟡 | 🟢 | 🟢 |
| | Junk Button for Outlook® | 🟢 | 🟢 | – | ⭕ |
| | Per User Anti-Spam Aggressiveness for all models | 🟢 | 🟡 | 🟢 | 🟢 |
| | Per User Allowed/Blocked Lists | 🟢 | 🟡 | 🟢 | 🟢 |
| | Junk Box Summaries in multiple Languages | 🟢 | 🟢 | 🟢 | 🟢 |
| | Full re-branding | 🟢 | 🟡 | 🟡 | 🟡 |
| **System features** | Inbound & Outbound in the Same System for all models | 🟢 | 🟡 | 🟢 | 🟢 |
| | Unrestricted Domains support | 🟢 | ⭕ | ⭕ | ⭕ |
| | Scalable Split-mode Architecture in all models | 🟢 | 🟡 | 🟡 | – |
| | Clustering & Remote Clustering in all models | 🟢 | 🟡 | 🟡 | – |
| **Customer Support** | 24x7 and/or 8x5 phone support | 🟢 | 🟢 | 🟢 | ⭕ |

## Dell SonicWALL Secure Remote Access Product Line Overview

With maturing mobile technologies, booming global markets and heightened focus on disaster preparedness, remote access control has become a business imperative. The modern mobile workforce demands secure access to more resources from more remote devices and platforms than ever before. Dell SonicWALL Secure Remote Access (SRA) solutions offer SSL VPN access to mission-critical resources from virtually any endpoint—including desktops, laptops, smartphones and tablets. Dell SonicWALL provides a wide range of scalable remote access solutions that fit organizations of every size, from small- to medium-sized businesses (SMBs) to the largest global enterprise.

The Global Enterprise is facing several market trends that encourage usage of SSL VPNs.  Those trends include:

- Smartphones and tablets working their way in as IT-approved access options

- Distributed supply chains increasing reliance on Extranets for collaboration
- Distributed operations encouraging employee mobility
- Depreciation of IPSec VPNs leading towards openness for an SSL VPN based replacement
- Compliance pressures encourage tighter access controls
- Virtualization (Virtual Desktop Solutions) being pushed for efficiencies and cost optimization

## Customer Pain Points

- Organizations with a need to provide a secure Bring Your Own Device (BYOD) access policy
- Any organization looking to provide secure remote access for employees, business partners and contractors from almost any web-enabled device
- Organizations needing to perform Endpoint Control (EPC) to assess the integrity of devices in addition to authenticating employees, business partners and contractors
- The ability to scan all remote access user traffic through a Next-Generation Firewall to protect against malware and other Intrusions

## Secure Remote Access Enterprise Positioning

Dell SonicWALL® Aventail® E-Class Secure Remote Access (SRA) delivers full-featured, easy-to-manage, clientless or thin-client "in-office" connectivity for up to 20,000 concurrent mobile-enterprise users from a single appliance. E-Class SRA enhances productivity and business continuity with policy-enforced remote access to network resources from Windows®, Windows Mobile, Apple® Mac OS®, iOS, Linux®, and Google Android™ devices. Built on the powerful Dell SonicWALL Aventail SSL VPN platform, E-Class SRA connects only authorized users to only authorized resources. When integrated with a Dell SonicWALL Next-Generation Firewall as a Clean VPN™, E-Class SRA delivers centralized access control, malware protection, application control and content filtering over the internal wireless network.  Secure Remote Access Key Enterprise Features and Benefits

**Dell SonicWALL Mobile Connect:** Mobile Connect, a single unified client app for Apple iOS and Google® Android, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections.

Benefit:  Provides secure network level access from iOS or Android-enabled smartphones and tablets. Additionally, Endpoint Control can be used to determine if a device has been "Jailbroken" or rooted and connections from those systems can be rejected or quarantined.

**Dell SonicWALL Aventail Connect Mobile:** Connect Mobile provides users of IT-managed Windows, Macintosh and Linux devices with unmatched ease-of-use and a complete "in-office" experience. Connect Mobile delivers the easiest, most complete method of secure remote access available and is ideal for providing strong security for wireless LAN users and road warriors who need full access away from the office.

Benefit:  Connect Mobile, in combination with an Aventail E-Class SRA appliance, provides a robust remote access solution for Windows Mobile smartphones and tablets, with in-office access optimized for the device.

**Dell SonicWALL Aventail Smart Access:** Smart Access offers transparent, dynamic deployment of the appropriate access method based on user identity, end point security or zone classification and resource desired.

Benefit:  Provides the user with the appropriate level of access based on the identity and security posture of the device the user is logging in from.

**Dell SonicWALL Aventail Unified Policy:** Unified Policy significantly reduces work for administrators by providing centralized administration with just a single rule set for all resources and access methods. This extensible object-based policy model consolidates control of all web resources, file shares and client-server resources in a single location. This lets you quickly set policy with a single rule across all objects, so that policy management can take only minutes instead of the hours it takes with other VPNs.

Benefit: Reduces the complexity of managing multiple policy sets for the different access methods SSL VPN provides, leading to a significant decrease in time spent doing the initial setup and ongoing policy management.

**Dell SonicWALL Aventail WorkPlace:** WorkPlace delivers clientless browser access for Web applications, client/server applications and file shares from Windows, Macintosh, or Linux endpoint devices and web-enabled tablets and smartphones.

Benefit: Provides a customized web landing page for all users needing access to corporate resources without the need for any client installation.

**Dell SonicWALL Aventail Advanced Endpoint Control:** Advanced End Point Control (EPC) offers the most comprehensive endpoint detection and data protection for distributed enterprises, all in one easy-to-deploy add-on solution. Integrating advanced interrogation and secure desktop features, Advanced EPC makes Dell SonicWALL Aventail E-Class SRA appliances the easiest secure remote access controllers on the market. Advanced interrogator list includes all supported anti-virus, personal firewall and anti-spyware solutions from leading vendors such as McAfee®, Kaspersky Lab® Symantec®, Computer Associates®, Sophos®, and many more. Secure Desktop incorporates and integrates technology from OPSWAT® to create best-of-breed security for your remote session—a "virtual" Windows session that runs on top of the actual desktop. Additional EPC checks can be enforced for smartphones and tablets running Android, iOS or Windows Mobile.

Benefit: Allows the network administrator to enforce security checks on the endpoints before they are allowed to access any corporate resources.

**Dell SonicWALL Aventail Native Access Modules:** Native Access Modules provide native protocol access to Citrix, Windows Terminal Services and VMware View via a secure Dell SonicWALL Aventail E-Class Secure Remote Access appliance. Native Access Modules deliver access to server-based sessions without any additional configuration. Using a single portal link, remote users receive an easy, seamless experience while accessing all Citrix applications, including support for load-balance Citrix farms.

Benefit: Provides support for common Virtual Desktop Infrastructure (VDI) directly through a web browser without the need for a Layer-3 client.

**Dell SonicWALL Aventail Spike License Pack:** The Spike License Pack is a temporary capacity add-on license that increases your remote user count in the event of a disaster, business disruption or seasonal spike. Included Dell SonicWALL Aventail Platinum Assurance provides global 24/7 customer service and support for the duration of the spike period.

Benefit: Allows the administrator to quickly increase the appliance capacity temporarily to deal with a sudden spike in user capacity requirements.

**Dell SonicWALL Aventail Secure Virtual Assist:** Secure Virtual Assist allows a technician to assume control of a customer's PC or laptop to provide assistance and fix problems. Remote professionals can also connect to their PC to stay productive.

Benefit: Allows helpdesk technicians the ability to provide out-of-band desktop troubleshooting for remote Windows and Mac users.

**Dell SonicWALL Aventail Advanced Reporting:** Dell SonicWALL Aventail Advanced Reporting delivers a dynamic analysis and reporting tool to track and evaluate remote user access to distributed enterprise network resources over SSL VPN. Advanced Reporting is a downloadable add-on application, hosted off-appliance on Windows® or Linux® platforms, and accessible through standard web browsers on Windows, Linux, or Macintosh® platform devices. Advanced Reporting can generate standard or custom statistical reports based upon dynamic filtering of multiple field types, including date, time, source and destination host fields.

Benefit: Provides historical reporting for a single or multiple Dell SonicWALL Aventail appliances.

## Dell SonicWALL Secure Remote Access SMB Positioning

The Dell SonicWALL Secure Remote Access (SRA) platform and appliance series provides easy-to-use, secure and affordable remote access for the SMB. Using a standard web browser, authorized users can easily and securely access email, files, intranets, web and network applications plus remote desktops—from virtually any location.

Dell SonicWALL SRA for SMB offers clientless and tunnel access for Windows, Windows Mobile, Apple Mac OS, iOS, Linux, and Google Android, plus optional Web Application Firewall (WAF) Service and multi-platform remote support. The SRA Series offers small- to medium-sized businesses granular unified policy, two-factor authentication, load balancing and high availability. The SRA Series lets authorized mobile workers and contractors connect over SSL VPN using a standard web browser. Easily and flexibly deployed into virtually any network with no pre-installed clients, the SRA Series eliminates costs of deploying and maintaining traditional IPSec VPNs. Dell SonicWALL Secure Virtual Assist permits Windows-based technicians to support Windows, Mac OS or Linux devices remotely.

## Key SMB Features and Benefits

**Dell SonicWALL Mobile Connect:** Mobile Connect, a single unified client app for Apple iOS and Google® Android, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections.

**Unified policy:** Through the management interface, network administrators have a central location in which they can define administrator bookmarks and create policies to control user access to streamline configuration, troubleshooting and administrative overhead.

**Granular security:** Through granular policy configuration controls, network administrators can easily create policies that lock down users to specific resources and applications to prevent unauthorized access.

**EndPoint Control (EPC):** Allows for the unique identification of Windows-based endpoints as well as the ability to assess the security posture of the device by looking for security components such as anti-virus, anti-spyware and personal firewall software.

**One-Time Passwords (OTP):** A unique one-time password can be generated for every login and combined with the user name and standard network password for enhanced logon protection.

**Redundancy and reliability:** To optimize performance and redundancy for server-based applications, network administrators can take advantage of load balancing features built into the SRA appliances. For increased reliability, High Availability allows administrators to deploy a second SRA 4200 as a backup to the primary to enhance uptime and reliability for all remote access users.

**Customized web portal:** Each remote user launches a personalized web portal for easy access to email, files, applications, internal web sites and other authorized resources.

**Enhanced layered security:** When an SRA appliance is deployed with a Dell SonicWALL Next-Generation Firewall, administrators get the critical dual protection needed to secure both VPN access and VPN traffic.

**Centralized management and reporting:** Dell SonicWALL's management and reporting solutions, including the Dell SonicWALL Global Management System (GMS) and Dell SonicWALL Analyzer, provide a comprehensive architecture for centrally creating and managing remote access policies, enabling real-time monitoring, logging and analyzing remote access activity by user, and delivering intuitive reports.

**Secure Virtual Assist:** Dell SonicWALL Secure Virtual Assist makes it easy for a technician to assume control of a customer's PC or laptop to provide technical assistance and remotely diagnose and fix problems.

**Secure Virtual Access:** Through Dell SonicWALL Secure Virtual Access, end users can remotely access their unattended Windows-based computers from any Internet connection to maintain productivity.

**Secure Virtual Meeting:** Using Dell SonicWALL Secure Virtual Meeting, employees can instantly bring meeting participants together in a secure and cost-effective fashion.

**Web Application Firewall Service:** With automatic signature updates for continuous malware protection, the Dell SonicWALL Web Application Firewall (WAF) Service can help control web site access and protect web applications from being attacked.

**SRA Spike License Pack:** The Dell SonicWALL SRA Spike License Pack is an add-on license that enables distributed businesses to increase remote user count immediately in the event of emergencies, business disruptions or seasonal spikes, enabling seamless business continuity.

### SRA Product Line Enterprise Appliance Overview

| | **E-Class SRA Virtual Appliance** | **E-Class SRA EX6000** |
|---|---|---|
| **Certifications** | - | ICSA Labs SSL VPN, FIPS 140-2 |
| **Target Customer** | Mid-size Enterprise with up to 500 employees | Mid-size Enterprise with 500 to 1,000 employees |
| **Concurrent Users** | Can be licensed with a 25, 50, 100 or 250 concurrent user license | Can be licensed with a 25, 50, 100 or 250 concurrent user license |
| **Max Concurrent Users** | 250 Concurrent users | 250 Concurrent users |
| **Add-on Features** | **Spike License** - Allows for the immediate increase of the remote user count in the event of a business disruption<br>**Native Access Modules** - Optimized access for WTS, VMware View and Citrix applications<br>**Advanced EPC** - Granular control with easy configuration for trusting endpoint devices<br>**Connect Mobile** - Windows Mobile agent<br>**Secure Virtual Assist** - Remote desktop help and support tool<br>**Dell SonicWALL Aventail Advanced Reporting**- Robust hierarchical log analysis tool<br>**E-Class Support** - 24x7 support for E-Class solutions | **Spike License** - Allows for the immediate increase of the remote user count in the event of a business disruption<br>**Native Access Modules** - Optimized access for WTS, VMware View and Citrix<br>**Advanced EPC** - Granular control with easy configuration for trusting endpoint devices<br>**Connect Mobile** - Windows Mobile agent<br>Secure Virtual Assist - Remote desktop help and support tool<br>**Dell SonicWALL Aventail Advanced Reporting** - Robust hierarchical log analysis tool<br>**E-Class Support** - 24x7 support for E-Class solutions |

| | **E-Class SRA EX7000** | **E-Class SRA EX9000** |
|---|---|---|
| **Certifications** | ICSA Labs SSL VPN, FIPS 140-2 | Pending FIPS 140-2 |
| **Target Customer** | Large Enterprise with over 1,000 employees | Large Enterprise with over 1,000 employees |
| **Concurrent Users** | Can be licensed with a 50, 100, 250, 500, 1,000, 2,000 and 5,000 concurrent user license | Can be licensed with a 100, 250, 500, 1,000, 2,000 and 5,000, 7,500, 10,000, 12,500, 15,000, 20,000 concurrent user license |
| **Max Concurrent Users** | 5,000 Concurrent users | 20,000 Concurrent users |
| **Add-on Features** | **Spike License** - Allows for the immediate increase of the remote user count in the event of a business disruption<br>**Secure Virtual Assist** - Remote desktop help and support tool<br>**Dell SonicWALL Aventail Advanced Reporting**- Robust hierarchical log analysis tool<br>**E-Class Support** - 24x7 support for E-Class solutions | **Spike License** - Allows for the immediate increase of the remote user count in the event of a business disruption<br>**Secure Virtual Assist** - Remote desktop help and support tool<br>**Dell SonicWALL Aventail Advanced Reporting**- Robust hierarchical log analysis tool<br>**E-Class Support** - 24x7 support for E-Class solutions |

### SRA Product Line SMB Appliance Overview

| | SRA Virtual Appliance | SRA 1200 | SRA 4200 |
|---|---|---|---|
| **Target Customer** | SMB companies with up to 50 employees | SMB companies with up to 50 employees | SMB companies with up to 250 employees |
| **Concurrent Users** | Stackable user license options include 5 or 10 concurrent users | Stackable user license options include 5 or 10 concurrent users | Stackable user license options include 10, 25 and 100 concurrent users |
| **Included/Max Concurrent Users** | 5/50 | 5/50 | 25/500 |
| **Add-on Features** | **Spike License** - Allows for the immediate increase of the remote user count in the event of a business disruption<br>**EndPoint Control for Windows**<br>**Secure Virtual Assist** - Remote desktop help and support tool<br>**Secure Virtual Access** - Provides remote PC management and control<br>**Secure Virtual Meeting**- Provides remote meeting capabilities[1]<br>**Web Application Firewall** - Detects and protects web applications from web-based threats<br>**Dynamic Support**- Options include 8x5 or 24x7 for one, two or three years | | |

[1] Secure Virtual Meeting is available on the SRA 4200 only.

## SRA Product Line Competitive Position in the Enterprise

For Enterprise Secure Remote Access or SSL VPN, Dell SonicWALL Aventail is considered one of the main competitors against Juniper, Citrix and F5.

- Dell SonicWALL Aventail is seen as one of the Visionary players in SSL VPN according to Gartner's 2011 Gartner Magic Quadrant.
- Granular Endpoint control for a wide variety of device types including iOS and Android.
- Dell SonicWALL Aventail hardware and software are FIPS 140-2 and ICSA Labs certified
- Broad SSL VPN offering to fit both Enterprise and SMB customer requirements

### Juniper Networks

Juniper Networks is one of the leaders in SSL VPN according to Gartner and is the most common competitor that Dell SonicWALL deals with from a competitive perspective in large enterprise accounts. The following SWOT is based on the Juniper SA and MAG products.

Dell SonicWALL® vs. Juniper SWOT

| Strengths | Weaknesses |
|---|---|
| • Initial setup and ongoing policy management is easier<br>• Application policy management is possible, not limited to IP address only<br>• No additional hardware modules or custom software is required to be FIPS compliant<br>• EPC capabilities for Windows, MAC, iOS, Android and Linux devices<br>• Broader SSL VPN offering (NGFW, SRA, E-Class SRA) to meet the needs of both enterprises and SMBs | • Not in the Leader category on the Gartner MQ<br>• Still has two SSL VPN client software offerings for SMB and Enterprise<br>• Appliances are not common criteria certified<br>• No option for license pooling or license stacking on high-end SSL VPN appliances |
| **Opportunities** | **Threats** |
| • Dell SonicWALL has a broader delivery mechanism to offer SSL VPN technology (NGFW, SRA, E-Class SRA)<br>• The EX6000, EX7000, EX9000 (Pending) platforms are FIPS 140-2 certified (No special software or hardware is required)<br>• Differentiate our SSL VPN offering with increased EPC for smartphones and tablets<br>• Continue to cross pollinate SSL VPN technology (NGFW, SRA, E-Class SRA) | • The introduction of SSL VPN technology onto the SRX firewall platform<br>• Scalable virtualized offering targeted at Service Providers to offer a managed SSL VPN service<br>• Continue to leverage the Smobile acquisition to become a bigger player in the mobile security market |

## F5

F5 is also considered a leader by Gartner in the most recent SSL VPN Gartner Magic Quadrant. In most cases Dell SonicWALL does not see F5 as a big competitor in large enterprise opportunities unless the account is already running F5 BigIP equipment. In this case, FirePass will not be the SSL VPN solution of choice; however the customer will typically look to the integrated SSL VPN option available on the F5 BigIP. The following SWOT is based on the FirePass products only.

Dell SonicWALL® vs. F5 SWOT

| Strengths | Weaknesses |
|---|---|
| • Broader SSL VPN offering (NGFW, SRA, E-Class SRA)<br>• Higher user capability (20,000) with the introduction of the EX9000<br>• EX6000, EX7000, EX9000 (Pending) models are FIPS certified<br>• Secure Virtual Assist offering for remote desktop support | • Lack Web Application Security on the high-end SSL VPN solution<br>• Do not provide an ICAP API for 3rd party scanning of attachments |
| **Opportunities** | **Threats** |
| • Dell SonicWALL offers 10x capacity than the FirePass solution<br>• Dell SonicWALL has an SSL VPN offering to fit the SMB and Enterprise markets<br>• Differentiate our SSL VPN offering with increased EPC for mobile devices<br>• Continue to leverage Secure Virtual Assist and Secure Virtual Access features to differentiate | • F5 continues to advance the SSL VPN feature set available on the BigIP products<br>• F5 continues to push additional options on the BigIP platform such as WAN Optimization- and Web Application Firewall (WAF) |

### Citrix

While Citrix is not seen as a leader in SSL VPN, it is considered a Challenger according to Gartner. Because Citrix has a large install base of its Virtual Desktop solution, Dell SonicWALL really only competes with this vendor in situations where the Citrix VDI solution is going to be deployed or is already deployed. The following SWOT covers both the NetScaler and Central Access Gateway (CAG) gateways.

Dell SonicWALL® vs. Citrix SWOT

| Strengths | Weaknesses |
|---|---|
| • Broader SSL VPN offering (NGFW, SRA, E-Class SRA)<br>• EX6000, EX7000, EX9000 (Pending) models are FIPS certified<br>• Support for multiple VDI access including RDP, Citrix and VMview<br>• Higher scalability, 20,000 concurrent users on a single appliance<br>• Secure Virtual Assist offering for remote desktop support<br>• Citrix lacks network level client support for iOS and Android | • Lack Web Application Security on the high-end SSL VPN solution<br>• Lack some advanced features required for certain Citrix deployments (Citrix Farm support, auto reconnect) |
| **Opportunities** | **Threats** |
| • Dell SonicWALL offers 4x more capacity than the Citrix solution<br>• Differentiate our SSL VPN offering with increased EPC for mobile devices<br>• Broader range of connection options that including on-demand tunnel, Mobile Connect | • Citrix continues to expand feature support for its own Citrix VDI solution |

## Secure Remote Access Enterprise Competitive Matrix

| Legend 🟢Full 🟡Partial ⭕No Support –Information Not Available | | Dell SonicWALL | Juniper | F5 | Citrix |
|---|---|---|---|---|---|
| **Endpoint Control** | Endpoint security interrogation used to dynamically provide different levels of allow, deny and quarantine access to resources | 🟢 | 🟡 | 🟡 | 🟡 |
| | Endpoint security control on Windows, Macintosh, Linux, iOS, Android | 🟢 | 🟢 | 🟡 | 🟡 |
| | Endpoint interrogation on logon and on schedule | 🟢 | 🟢 | 🟢 | 🟢 |
| | Obscure portal links based on end point restrictions | 🟢 | ⭕ | - | - |
| | Integrated cache control protection on Windows and Macintosh | 🟢 | 🟢 | 🟢 | 🟡 |
| | Integrated secure virtual desktop data protection | 🟢 | 🟡 | 🟢 | ⭕ |
| | Windows/Mac/Linux /Mobile Device ID | 🟢 | ⭕ | 🟢 | 🟡 |
| **Unified Policy** | Resource or object-based access controls | 🟢 | ⭕ | - | - |
| | Unified resource creation for any type of access | 🟢 | ⭕ | - | ⭕ |
| | Unified access control creation for any access method or group | 🟢 | ⭕ | - | 🟢 |
| | Access controls for bi-directional client/server communication | 🟢 | ⭕ | - | - |
| | Integrated One Time Password Support | 🟢 | ⭕ | ⭕ | ⭕ |
| | Name- and domain-based access controls on layer-3 tunnel | 🟢 | ⭕ | 🟢 | 🟢 |
| **Admin Features, Security, and Monitoring** | ICSA Labs SSL VPN certified product | 🟢 | 🟢 | 🟢 | ⭕ |
| | FIPS Certified Solution (No Additional HW required) | 🟢 | 🟡 | 🟡 | 🟡 |
| | Firewall security model (deny-all as default) | 🟢 | 🟡 | - | - |
| | Role-based (delegated) administration model | 🟢 | 🟢 | 🟢 | 🟢 |
| | User self-service password management | 🟢 | 🟢 | 🟡 | 🟢 |
| | Setup wizard to facilitate easy initial configuration | 🟢 | 🟡 | 🟢 | 🟢 |
| | Configurable user inactivity session timeout setting | 🟢 | 🟢 | 🟢 | 🟡 |
| | Graphical monitoring integrated in management console | 🟢 | 🟢 | 🟢 | 🟡 |
| | Integrated log filtering, searching and export | 🟢 | 🟢 | 🟢 | 🟡 |
| | Secure Virtual Assist (Remote Desktop Support) | 🟢 | ⭕ | ⭕ | ⭕ |
| | Spike License for temporary concurrent user increase | 🟢 | 🟢 | 🟢 | 🟢 |
| **Smart Access & Smart Tunneling** | Clientless access | | | | |
| | Multiple portal instances can run on a single appliance | 🟢 | 🟢 | 🟢 | 🟢 |
| | HTTP compression support | 🟢 | 🟢 | 🟢 | - |
| | Cross-platform support (Windows, Mac, Linux, Tablets, Smartphones) | 🟢 | 🟢 | 🟢 | 🟢 |
| | Native Access to common application protocols (RDP, ICA, Citrix, VMview) | 🟢 | 🟡 | 🟢 | 🟡 |
| | Native ActiveSync Support | 🟢 | 🟢 | 🟢 | ⭕ |
| | Full VPN Agent | | | | |
| | Cross-platform desktop client (Windows, Mac, Linux) | 🟢 | 🟢 | 🟢 | 🟡 |
| | Mobile client for iOS/Android (Dell SonicWALL Mobile Connect) | 🟢 | 🟢 | 🟢 | 🟡 |
| | Pervasive agent mode (installable agent) | 🟢 | 🟢 | - | 🟡 |
| | Support for full IP protocol (includes items like multicast or H.323) | 🟢 | 🟢 | 🟡 | 🟡 |
| | IP address conflict mitigation | 🟢 | ⭕ | ⭕ | ⭕ |
| | Out of the box functionality without having to configure IP pools | 🟢 | ⭕ | - | ⭕ |
| | Support for ESP Mode | 🟢 | 🟢 | ⭕ | ⭕ |

## Secure Remote Access Competitive Position in the SMB

### WatchGuard

WatchGuard is more known in the UTM or firewall market.  It does have a pair of dedicated SSL VPN products that do compete against Dell SonicWALL in the SMB SSL VPN market.  The following SWOT covers the dedicated WatchGuard SSL VPN solutions including the SSL 560 and SSL 100.

Dell SonicWALL® vs. WatchGuard SWOT

| Strengths | Weaknesses |
|---|---|
| • Broader SSL VPN offering (NGFW, SRA, E-Class SRA)<br>• Support for both RDP and Citrix without the need for a client<br>• Secure Virtual Assist, Secure Virtual Access and Secure Virtual Meeting offering for remote desktop support, secure access to remote systems and meetings<br>• WatchGuard lacks layer 3 client support for iOS and Android smartphones and tablets<br>• Offer Spike licensing | • Lack some of the key features for Endpoint control<br>• Provide client enforced firewall option |
| **Opportunities** | **Threats** |
| • Dell SonicWALL has a broader delivery mechanism to offer SSL VPN technology (NGFW, SRA, E-Class SRA)<br>• Continue to differentiate our SSL VPN offering with smartphone and tablet access and security<br>• Continue to leverage our centralized management through Dell SonicWALL Global Management System (GMS)<br>• Continue to cross pollinate SSL VPN technology (NGFW, SRA, E-Class SRA) | • No significant threats |

**Barracuda**

Barracuda is primarily known for anti-spam and backup solutions; however it also provides dedicated SSL VPN appliances.  The following SWOT covers the dedicated Barracuda SSL VPN solutions including the Barracuda 180, 280, 380, 480, 680, 880

Dell SonicWALL® vs. Barracuda SWOT

| **Strengths** | **Weaknesses** |
|---|---|
| • Broader SSL VPN offering (NGFW, SRA, E-Class SRA)<br>• Secure Virtual Assist, Secure Virtual Access and Secure Virtual Meeting offering for remote desktop support, secure access to remote systems and meetings<br>• Barracuda lacks layer-3 client support for iOS and Android smartphones and tablets<br>• Flexible user licensing, including Spike licensing | • Lack some of the key features for Endpoint control<br>• Support for Virtual Keyboard<br>• Multiple admin roles<br>• Single-sign-on for web applications |
| **Opportunities** | **Threats** |
| • Dell SonicWALL has a broader delivery mechanism to offer SSL VPN technology (NGFW, SRA, E-Class SRA)<br>• Continue to differentiate our SSL VPN offering with smartphone and tablet access and security<br>• Continue to leverage our centralized management using Dell SonicWALL Global Management System (GMS)<br>• Continue to cross pollinate SSL VPN technology (NGFW, SRA, E-Class SRA) | • Barracuda lowers its hardware appliance MSRP, and does not charge per user licensing |

## Secure Remote Access SMB Competitive Matrix

| Legend 🟢Full 🟡Partial ⭕No Support<br>–Information Not Available | | **SRA 1200/4200** | **Barracuda 180/280/380** | **WatchGuard** SSL 100/560 | **Barracuda /480/680/880** |
|---|---|---|---|---|---|
| User count (default\|max) | | 1200 (5\|50), 4200( 25 \| 500) | 180 (15) 280 (25) 380 (50) | 100 (25\|100), 560 (250\|500) | 480 (100) 680 (500) 880 (1000) |
| Layer-3 client connectivity | Layer-3 client (NX/Barracuda Connect) | 🟢 (NX) | 🟢 | 🟢 | 🟢 |
| | Layer-3 mobile clients (thin-client) | 🟢 | ⭕ | ⭕ | ⭕ |
| Add-on license based services | Web Application Firewall (add-on license) | 🟢 | ⭕ | ⭕ | ⭕ |
| | Remote PC support (add-on license) | 🟢 | ⭕ | ⭕ | ⭕ |
| | Secure Virtual Meeting (Add-on license) | 🟢 | ⭕ | ⭕ | ⭕ |
| Advanced features | High Availability | 🟢 [1] | ⭕ | ⭕ | 🟢 |
| | Integrated load-balancing | 🟢 | ⭕ | ⭕ | ⭕ |
| | Central web management/reporting | 🟢 | ⭕ | ⭕ | ⭕ |
| | Anti-virus (virus/spyware scanning) | 🟡 | 🟢 | ⭕ | 🟢 |
| | Multi-platform support including Linux/MAC | 🟢 | 🟢 | 🟡 | 🟢 |
| Authentication & policy control | OTP (One-Time Password) | 🟢 | - | 🟢 | 🟢 |
| | Hardware 2-FA token support | 🟢 | 🟢 | 🟢 | 🟢 |
| | Radius auth | 🟢 | 🟢 | 🟢 | 🟢 |
| | Active Directory (AD) and LDAP Auth | 🟢 | 🟢 | 🟢 | 🟢 |
| | Layered/Stacked auth schemes | 🟢 | 🟢 | 🟢 | 🟢 |
| | Endpoint Control (EPC) | 🟡 | 🟢 | 🟢 | 🟢 |
| | Granular policy control | 🟢 | 🟢 | 🟡 [3] | 🟢 |
| Web-based access methods (Clientless) | ActiveSync support (for OWA access) | 🟢 | 🟡 [2] | 🟡 [4] | 🟡 [2] |
| | Application offloading | 🟢 | 🟡 | 🟡 | 🟡 |
| | Bookmark (HTTP/HTTP(s), Fileshares, RDP/Citrix, etc.) | 🟢 | 🟢 | 🟢 | 🟢 |
| Management | Customizable user interface | 🟢 | 🟡 | 🟢 | 🟡 |
| | Virtual keyboard | ⭕ | 🟢 | ⭕ | 🟢 |
| Other features | Cache cleaner | 🟢 | 🟢 | 🟢 | 🟢 |
| | SNMP / API | 🟢 | ⭕ | ⭕ | 🟢 |
| | Syslog reporting | 🟢 | ⭕ | 🟢 | 🟢 |
| | Localization | 🟢 | ⭕ | - | 🟡 |
| | Remote desktop (Single Sign-on) | 🟢 | 🟢 | 🟡 | 🟢 |
| | Basic NAC (endpoint checking) | 🟢 | ⭕ | 🟢 | 🟢 |

[1]: The Dell SonicWALL SRA 1200 does not support HA.

[2] Barracuda has support for OMA (which is not the same as OWA). OMA allows users to access Microsoft Exchange data using mobile devices, and the browser based app is similar to OWA but is supposedly lightweight. Most organizations prefer to use ActiveSync instead of OMA.

[3]: Granular policy control is present, but there is no mention of unified policy control

[4]: WatchGuard appears to support OWA access via ActiveSync but it's not clear on which mobile devices and whether it is with our without authentication enabled. WatchGuard mentions AirSync which is an old MS Exchange 2003 protocol.

## Dell SonicWALL Continuous Data Protection (CDP) Product Line Overview

Dell SonicWALL Continuous Data Protection (CDP) solution provides continuous backup, application –aware snapshot, replication, archiving and a powerful object-based management workflow unified in a scalable and flexible architecture to protect and ensure the preservation and recoverability of files, applications and systems for the heterogeneous IT environment.

CDP is delivered in various purpose-built appliance form factors to reduce the burden and guesswork of implementing a backup and disaster recovery strategy for servers, laptops and desktops running a mixture of Windows, Apple and Linux operating systems.

## CDP Key Value Propositions

**Data Preservation —** business-relevant data asset, including "all" its version history, is properly preserved in a consistent, accurate and unaltered original state throughout its lifecycle.

**Recovery Responsiveness —** protected data and computing systems are readily available and instantly recoverable at all times from anywhere for any specific business purpose.

**Data Governance —** data is secured, governed and readily accessible by those who are given proper authorization and access.

**Disaster Recovery Readiness** – copies of data safely replicated and preserved in multiple geographical locations achieving highest level of availability and recoverability under any disaster circumstances.

### Customer Pain Points

A customer survey was conducted in February of 2012 targeted at all Dell SonicWALL end-customers that had yet to deploy CDP. Approximately 500 end-users responded to the questionnaire. The results reveal what customers are most concerned about when it comes to their current backup and disaster recovery implementation.

The first three outlined are top-of-mind issues for most customers and consistently rated the highest with **"Extremely Important"** or **"Very Important"**.

1. **Customers are not confident that their backups are successful.**

Many legacy backup and recovery solutions such as tape-based system leave system administrators unsure whether backup was successful, unsure if applications, files and folders are ready for restore if necessary.

2. **Backup data is not stored offsite leaving businesses vulnerable in case of local disaster.**
   a. Many businesses either do not have a copy of their backups offsite or manually copy backup data and transport it offsite, a time consuming, error prone task which is a typical problem with tape-based system.
   b. In case of flood, fire or other site-wide disasters, businesses must have their critical data automatically replicated to one or more offsite locations and a sound plan to quickly restore data and operations.

3. **Server restore takes too long**
   a. Limitations of traditional system recovery process require many man-hours or even days to manually recover a computing system from the ground up.
   b. A new generation of image-based snapshot technology is needed to significantly improve server recovery time to hours and minutes.

4. **Backup data growth is unmanageable**
   a. Worldwide total data volume estimated to explode from 1.2 trillion gigabyte in 2010 to 35 trillion by 2020 and 75% of the total is likely to be copies of the original data[1].

b. Businesses are compelled to manage and backup huge information pools that further inflate management and storage costs.
c. Making things worse, many new regulations require data to be kept longer.
d. Legacy backup and recovery solutions allow backup data to grow and become unmanageable. Businesses need a better and smarter way to capture, preserve and manage corporate information and records more efficiently and intelligently.

In addition, some businesses have implemented backup solutions for client devices, including desktops and laptops, and market analysts predict the importance of client backup is increasing.

## Product Line Positioning and Key Messages

Dell SonicWALL® Continuous Data Protection (CDP) eliminates guesswork so that businesses can be confident their data is reliably backed up and can be quickly restored with ease. Easy to use from a simple click-and-go backup and restore window, CDP intelligently discovers, automatically backs up and restores specified applications, folders and files from servers, desktops and laptops. CDP offers granular control over whether a backup is scheduled or continuous, what is included or excluded, the number of retained revisions, the targeted destination of both the backup and the restoration, and more. To ensure success, CDP automatically validates each backup, backs up again if there is an error, and generates status reports and email alerts—so that administrators can identify and resolve any issues before a restore fails. CDP offers a choice of easy-to-configure disaster recovery solutions to match any business or budget. Administrators can restore from Dell SonicWALL's cloud-based service or a secondary offsite appliance, restore locally from a USB device that can be rotated offsite for safekeeping, and restore entire systems to dissimilar physical or virtual environments.

- **CDP automatically backs up and restores servers, desktops and laptops to efficiently and reliably protect data and features:**
  - A simple click-n-go backup and restore window
  - Intelligent discovery of applications, files and folders
  - Backup file type inclusion, exclusion, number of revisions to retain, version trimming options
  - Continuous or scheduled backup
  - Backup to secure local, off-site and cloud storage
  - Restore to original location or an alternate location
- **CDP validates data backups and generates email alerts and reports to provide status and confirm backup success**
  - Each backup is automatically validated, and if there is an error, the backup is re-initiated.
  - Email alerts and reports may be configured so system administrators know that backups executed successfully, and know if there is a problem before a restore fails.
  - Reports are also available that summarize backup activity and detail all events, so system administrators know the status of all backups
- **Choice of easy to configure disaster recovery features to best meet business and budget requirements including:**
  - Automated, secure replication to Dell SonicWALL's cloud data center service
  - Automated, secure replication to an offsite CDP storage appliance
  - Secure copy to a local attached USB storage device for rotation to an offsite location
  - Universal System Recovery with Bare Metal Recovery (BMR) technology restores systems and data to dissimilar physical or virtual systems

- **CDP advanced backup and data management technology speeds backup and restore, reduces network and storage utilization**
  - CDP backup software uses snapshot and de-duplication technologies, so backups are fast and only changed data blocks are transmitted to the CDP storage appliance. This minimizes network bandwidth used and the storage required for backup data, reducing network and storage costs.
  - With CDP, you chose what to back up, which file types to exclude or include, the number of backup versions to retain, and the backup frequency. You can minimize your backup sets to include only data relevant to your business, further reducing required storage
  - CDP also delivers fast data restore. Unlike legacy backup technology that rebuilds a version from incremental backups, the CDP intelligently correlates stored data blocks to the backup version time stamps, so point-in-time backup data versions can be recreated in an instant.

- **CDP backup and recovery is administered from an easy to use, central management interface**
  - Server, desktop and laptop backup and restore are administered from a central web interface
  - Administrators can automatically install and upgrade backup software and configure backup policies and backup storage quotas for individual users, groups of users or all users, automating tedious backup configuration tasks.
  - If permitted by Administrators, users can configure backup policies and restore historical versions of their own lost or deleted files without compromising privacy or security. This increases user satisfaction and improves both user and IT productivity.
  - **CDP can back up and recover Mac OS®, Linux®, or Windows® platforms on local or remote laptops, desktops and servers. And CDP supports Microsoft® SQL®, Exchange®, SharePoint®, Active Directory® and Small Business Server®.**

## Features and Benefits:

**Multiple backup methods** (including continuous data protection or point-in-time snapshots) support optimum Recovery Point Objective (RPO) and recovery responsiveness.

**Granular backup policy** lets administrators selectively back up only business-related data, and define the number of revisions to retain, trimming rules, offsite backup and archiving rules.

**Bandwidth and storage efficient** uses agent-based data de-duplication to send less traffic over the network and save more with less space, thus drastically shortening backup windows, improving performance and reducing operational costs

**Choices of disaster recovery options** to best meet business and budget requirements include Site-to-Site and Cloud Backup, Local Archiving and Universal System Recovery.

## Competitive position in the marketplace

The backup and disaster recovery market is highly competitive with many different types of players. Each type provides similar or comparable set of features and capabilities that customers are looking for. To make things easier to understand, the entire competitive landscape is encapsulated in Figure E below, showing the market broken down to different product categories.

Which is the right product for Dell customers? What makes Dell SonicWALL CDP different?

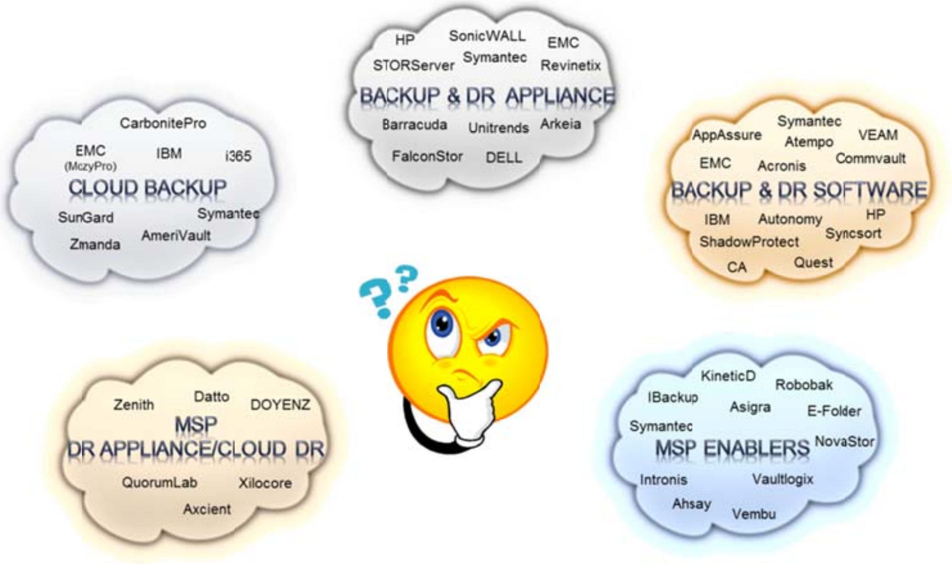
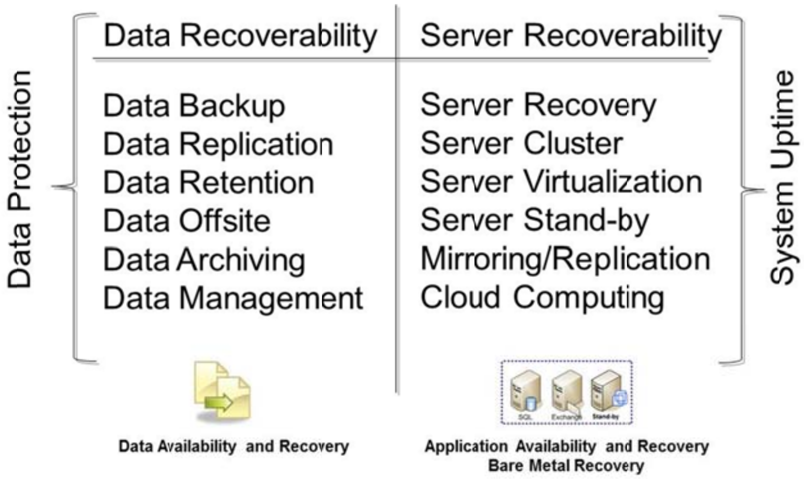


Figure E: Backup and Disaster Recovery Landscape

The customer survey results clearly suggest that an ideal backup and recovery solution must fundamentally relieve any **"fears"** and **"doubts"** about the backup implementation and offer customers assurance that all their important data and systems are unquestionably protected and recoverable according to their required business continuity requirements.

Business Continuity is divided into two important symbiotic components as shown in Figure E:

1. Data Recoverability
2. Server Recoverability



| Data Recoverability | Server Recoverability |
|---|---|
| Data Backup | Server Recovery |
| Data Replication | Server Cluster |
| Data Retention | Server Virtualization |
| Data Offsite | Server Stand-by |
| Data Archiving | Mirroring/Replication |
| Data Management | Cloud Computing |

Data Protection
System Uptime
SQL
Exchange
Stand-by
Data Availability and Recovery
Application Availability and Recovery
Bare Metal Recovery

Figure F: Business Continuity Components

**Data Recoverability** relates to data backup, replication, cloud backup and archiving to ensure the right data retention and recovery coverage is achieved for information continuity, availability and compliance. These operations provide reliable means to quickly restore any historical versions of protected data at one or more different locations to reestablish normal business operations after a severe data loss event.

**Server Recoverability** relates to building a redundant, high availability and failover/failback server environment to eliminate any single-point-of-failure for continuous system uptime and maintaining application services at normal level. These operations provide quick ways to restore any server after common disasters such as a hardware and software failure or location-based disaster such as a fire, flood, tornado or earthquake.

CDP has built its strength and advantage over known competitors by providing customers a better, smarter and more efficient **"data recovery"** solution to confidently address their pain points.

| Pain points | Features required | CDP delivers |
|---|---|---|
| Don't know if backups are successful | • Detail statistical reports<br>• Real-time email notification of fault conditions<br>• Scheduled email report of all backup events<br>• Data validation to ensure integrity.<br>• Detail logs | • Backup validation<br>• Daily email notification<br>• Real-time event-based failure alerts<br>• Reporting dashboard<br>• Aggregated reporting dashboard and event-based failure alerts through Dell SonicWALL Global Management System (GMS) |
| Required solution too expensive | • Affordable production-ready solution<br>• Broad range of deployment choices from low cost entry-level to high performance data center purpose-built backup appliance<br>• Licensing model that is straightforward and customer- and budget-friendly | • CDP is delivered in various purpose-built appliance form factors<br>• Budget conscious entry-level models are ideal for small business and remote or branch offices in a distributed enterprise<br>• Data center models have greater scale at competitive prices for larger IT deployments |
| No disaster recovery in place | • Built-in (not bolt-on) replication technology pre-configured for automated offsite backup that makes disaster recovery deployment effortless<br>• Multiple deployment options that meet customers' recovery and budget requirement | • Archiving to direct attached storage via USB<br>• Integrated replication via LAN/WAN/Internet<br>a. Site(s)-to-Site mode<br>b. Site(s)-to-Cloud mode<br>• Hardware-independent Bare Metal Recovery |
| Backup window too long | • Continuous and automated always-on backup<br>• Real-time impact-free backup that captures, sends and stores only changed data "on the fly"<br>• Data de-duplication technology that eliminates sending the same data twice over the network for fast backup completion | • A choice of two automated backup modes:<br>- Continuous – data is backed up when changes are detected in real time non-stop<br>- Scheduled – data is backed up at an exact day(s) and time and repeated indefinitely until manually stopped<br>• Agent-side data deduplication send only unique data block over the network |

| | | |
|---|---|---|
| Data and backup footprint growing too large to manage | • A smarter backup approach than traditional **“all-or nothing”** backup approaches.<br>• Intelligent ways to capture, manage, and preserve information according to its business relevance<br>• A viable means to apply rules and policies on:<br>o Determining what type of data to backup and not<br>o How information should be retained<br>• Data de-duplication technology that eliminate having to store the same data twice in the backup footprint | • Smart Fileset Backup Technology<br>• Backup rules<br>• Version control<br>• Version trimming rules<br>• Agent-based data de-duplication Technology stores more data using less storage |
| Server recovery takes too long | • A fast and readily-available way to bring failed servers back on-line effortlessly under any circumstances<br>• Recovery Time Objective (RTO) under 30 minutes | • Universal System Recovery using Bare Metal Restore technology |

Known competitors that you are likely to come up against in sales opportunities are:

1. Symantec Backup Exec Appliance
2. Barracuda Backup Appliance
3. Zenith BDR Appliance

In summary, there are 4 distinct product differentiations that give CDP a superior advantage over competitors when it relates to data backup and disaster recovery deployments:

### Automation, Control, Enforcement

The unique CDP object-based, policy- driven approach gives IT Administrators unmatched levels of automation, control and enforcement that simply run backups continuously, reliably and intelligently base on a set of applied rules and commands to ensure data and application are backed up, replicated offsite and archived so it is easily accessible for quick recovery from anywhere and at any time.

### Flexibility

CDP delivers unprecedented scalability and flexibility in a unified platform which enables growing businesses to add client connections and expand platform and application protection with ease.

The CDP Client Software backs up and recovers server, laptop and desktops running a mixture of Windows, Apple and Linux operating systems. It also has native support for most popular business applications such as Microsoft® SQL, Exchange, SharePoint, Active Directory and Small Business Servers. This means CDP doesn’t require any additional software add-ons. Continuous backup, application-aware snapshot, replication and archiving are all built-in which make the backup and disaster recovery process work effortlessly.

For fully effective disaster recovery, CDP provides customers multiple ways to complete their business continuity plans.

1. In case of a hardware disaster, CDP Universal System Restore software with Bare Metal Recovery technology helps minimize system downtime by enabling quick recovery of data files or complete Windows servers to resume mission-critical services such as receiving and sending important emails.
2. In the event of a location-based disaster that destroys an entire site, CDP Offsite Backup Service, Site-to-Site Data Replication, and Archiving ensures copies of business data are safely stored and accessible in multiple geographical locations to achieve the highest level of availability and recoverability no matter what happens.

### Efficiency

CDP Smart Fileset and data de-duplication technology increases backup efficiency and performance while reducing bandwidth and storage costs by never having to transmit and store the same data twice in the backup process.

Less is the new more.  CDP sends less data over the network, completes backups faster and stores more data using far less storage.

### Easy to use

Unlike traditional point-level solutions that involve complex integration, configuration and testing, CDP is delivered as a production-ready backup and disaster recovery appliance completely integrated with hardware, software and storage for ease of deployment that take the burden and guesswork out of data protection.

Its intuitive user interface design simplifies use and management for both IT administrators and users.  With as little as a one-time configuration, backups for the entire organization can be automated and streamlined without further intervention and regular maintenance.

File recovery is fast and easy with its 1-touch point-n-click recovery allows users to restore their own files without the help of IT and breaching data privacy and security policy.

## Barracuda overview and SWOT

The Barracuda Backup Service ascends from a combination the acquisitions namely BitLeaf who is a developer of appliances that allow data backup to a local storage device and to cloud storage and storage software vendor Yosemite Technologies.   The combine products directly compete with Dell SonicWALL's CDP Series backup and recovery appliance and Offsite Data Backup Service.

Dell SonicWALL® vs. Barracuda SWOT

| Strengths | Weaknesses |
|---|---|
| • Automated, validated backups<br>• Best known for CDP technology<br>• Smart Fileset Technology<br>• Desktop & laptop protection including remote system over VPN<br>• Multi-platform support - Windows, Mac, Linux)<br>• Archiving<br>• Fast, easy and secure user self-directed restore<br>• MSP enablement features | • Offsite pricing more expensive<br>• Limited hardware Line-up<br>• No RAID on entry-level models<br>• Single data center<br>• Not all-inclusive licensing |
| **Opportunities** | **Threats** |
| • Sell on validated backup and data corruption detection and self-remediation<br>• Sell on end-to-end continuous backup: Server, laptops and desktop protection even over VPN (not just server)<br>• Sell on multi-platform protection: Windows, Mac and Linux<br>• Cross-sell with SSLVPN  for client backup<br>• Sell workforce productivity with user self-reliance file recovery<br>• Position key differentiations:<br>o Automation, control and enforcement<br>o Flexibility of solution<br>o Efficacy<br>o Ease-of-use | • Aggressively competing on price to gain market share<br>• More appliance selection<br>• Lower offsite pricing<br>• Multiple data centers<br>• No per agent licensing |

## Symantec Overview and SWOT

Symantec is recognized as a market leader in the Storage Software market.  Similar to Barracuda, their backup offering started with the acquisition of VERITAS Software for its leading **Backup Exec** backup product that is typically used with tape-based system.  They currently have the lion share and largest installed-base within the SMB tape drive and tape automation market.  However over the past 4-5 years, trends reveal tape continues to experience sharp decline since the availability and maturity of CDP technology and disk-based backup appliance like Dell SonicWALL CDP.

This presents tremendous selling opportunities into businesses that are looking to do one of the following:

1. Change their backup strategy to either replace tape with Dell SonicWALL CDP.
2. Adding Dell SonicWALL CDP to complement their existing tape backup strategy and serve as the primary data recovery solution while tape is transition for archiving.

Dell SonicWALL SWOT against Backup Exec Software and 3600 Appliance:

| Strengths | Weaknesses |
|---|---|
| • Automated, validated backups<br>• Best known for CDP technology<br>• Smart Fileset Technology<br>• Better desktop & laptop protection including remote system over VPN (no network share needed)<br>• Object-based management and control<br>• Backup rules, permissions and enforcement<br>• Revision & trimming controls<br>• Flexible offsite rules<br>MSP enablement features | • Unix-based OS<br>• Limited support for non-Microsoft application<br>• Storage Targets - NAS, SAN, iSCSI, Cloud<br>• Target-based de-duplication<br>• Wizard and CLI Support |
| **Opportunities** | **Threats** |
| • Tape replacement<br>• Sell on validated backup and data corruption detection and self-remediation<br>• Sell on more efficient direct laptops and desktop protection even over VPN (no network share required)<br>• Cross-sell with SSLVPN  for client backup<br>• Server, laptops and desktop protection even over VPN (not just server)<br>• Sell on multi-platform protection: Windows, Mac and Linux<br>• Cross-sell with SSLVPN  for client backup<br>• Sell workforce productivity with user self-reliance file recovery<br>• Position key differentiations:<br>o Automation, control and enforcement<br>o Flexibility of solution<br>o Efficacy<br>o Ease-of-use | • Vision and  execution - Ability to drive business results<br>• Product innovation & development  - fast time to market<br>• Breadth of product and services offerings  - Frequent  NPI<br>• Aggressive advertising and promotional programs<br>• Competitive Channel and Discounted programs<br>• Sales and Marketing power – global reach |

## Zenith Overview and SWOT

- Zenith is a single tiered channel company so they ship and bill partners directly.
- Zenith provides Fixed-Fee Managed IT Services for partners who consider themselves an MSP.
- Zenith packages all their hardware and services with a flat cost to MSP.
- Zenith enables an MSP to lease or purchase the Zenith BDR and purchase Offsite Storage Service in a pay-as-you-go model. Meaning, MSP are billed for services used on a monthly subscription fee basis.
- Their BDR solution is fully based on the integration of multiple 3rd party technologies with some degree of customization.
- Zenith relies heavily on: StorageCraft "ShadowProtect" disk imaging backup software (a.k.a. Bare Metal Recovery(BMR) ) in combination with Microsoft Volume Shadow Copy Service as their backup methodology, VirtualBox (Oracle) for server virtualization capability, and two OEM restore tools: Storage Craft for mounting BMR images as a virtual drive for file/folder recovery and Kroll OnTrack for Exchange mailbox messages restore.

Dell SonicWALL SWOT against Zenith BDR Appliance Series

| Strengths | Weaknesses |
|---|---|
| • Automated, validated backups<br>• Best known for CDP technology<br>• Smart Fileset Technology<br>• Desktop & laptop protection including remote system over VPN<br>• Multi-platform support - Windows, Mac, Linux)<br>• Object-based management and control<br>• Backup rules, permissions and enforcement<br>• Flexible offsite rules<br>• Archiving<br>• Fast, easy and secure user self-directed restore | • Server virtualization<br>• Cash flow model<br>• No private-label offering<br>• Pricing<br>• No RAID on entry-level models<br>• Limited hardware Line-up<br>• Single data center<br>• No back office support – Remote Monitoring and Management (RMM) services |
| **Opportunities** | **Threats** |
| • Sell on validated backup and data corruption detection and self-remediation<br>• Sell on end-to-end continuous backup: Server, laptops and desktop protection even over VPN (not just server)<br>• Sell on multi-platform protection: Windows, Mac and Linux<br>• Cross-sell with SSLVPN for client backup<br>• Sell workforce productivity with user self-reliance file recovery<br>• Position key differentiations:<br>o Automation, control and enforcement<br>o Flexibility of solution<br>o Efficacy<br>o Ease-of-use | • Popularity of DR appliance among MSPs<br>• Server virtualization capability – good selling point<br>• MSP focus - more appealing channel business model<br>• Private-labeling<br>• Appealing pricing model<br>• Annuity business attracts partners<br>• Better life-time gross margin dollar opportunity<br>• NOC – fill partner service and support gap |

## DELL Overview and SWOT

Dell SonicWALL SWOT against Dell PowerVault DL Backup to Disk Appliance, powered by Symantec BackupExec 2010.

| Strengths | Weaknesses |
|---|---|
| • Automated, validated backups<br>• Best known for CDP technology<br>• Smart Fileset Technology<br>• Better desktop & laptop protection including remote system over VPN (no network share needed)<br>• Object-based management and control<br>• Backup rules, permissions and enforcement<br>• Revision & trimming controls<br>• Flexible offsite rules<br>• MSP enablement features | • Unix-based OS<br>• Limited support for non-Microsoft Application (i.e. Oracle, Lotus Domino)<br>• Storage targets - NAS, SAN, iSCSI, Cloud<br>• Target-based de-duplication<br>• Wizard and CLI Support |
| **Opportunities** | **Threats** |
| • Sell on validated backup and data corruption detection and self-remediation<br>• Sell on more efficient direct laptops and desktop protection even over VPN (no network share required)<br>• Cross-sell with SSLVPN  for client backup | • No significant threats |

## Chart of Key Features/Functions vs. Key Competitors

| Legend 🟢Full 🟡Partial ⭕No Support –Information Not Available | | Dell SonicWALL CDP | Symantec BE Appliance | Barracuda Backup Service | DELL DL Appliance | Zenith BDR |
|---|---|---|---|---|---|---|
| **Backup** | Continuous Data Protection - Windows, Apple, Linux | 🟢 | 🟢 | ⭕ | 🟢 | 🟢 |
| | Volume Shadow Copy Service (Snapshot) | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| | Centralized Policy-Enforced Backup Automation | 🟢 | ⭕ | ⭕ | ⭕ | ⭕ |
| | Smart Fileset Technology | 🟢 | ⭕ | ⭕ | ⭕ | ⭕ |
| | Target-based Data De-duplication | ⭕ | 🟢 | 🟢 | ⭕ | 🟢 |
| | Source-based Data De-duplication | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Application-Aware Backup** | Microsoft SQL Server 2005 and 2008 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| | Microsoft Small Business Server 2003 and 2008 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| | Microsoft SharePoint 2010 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| | Microsoft Exchange 2003, 2007 and 2010 | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| | Microsoft Active Directory | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| | System State | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| **Disaster Recovery** | Integrated replication to cloud storage | 🟢 | ⭕ | 🟢 | ⭕ | 🟢 |
| | Integrated Sites-to-site replication between Appliances | 🟢 | 🟢 | 🟢 | ⭕ | 🟢 |
| | BMR w/ Universal Restore (P2P,P2V,V2V or V2P) | 🟢 | ⭕ | 🟡 | ⭕ | 🟢 |
| | Integrated Archiving to external disk | 🟢 | ⭕ | ⭕ | ⭕ | ⭕ |
| | Integrated Archiving to Tape | ⭕ | 🟢 | ⭕ | 🟢 | ⭕ |
| | AES-256 bit encryption | 🟢 | ⭕ | 🟢 | ⭕ | 🟢 |
| **Data Recovery** | Automatic Test Recovery | ⭕ | ⭕ | ⭕ | ⭕ | ⭕ |
| | Recovery Verification (integrity and mountability testing) | ⭕ | ⭕ | ⭕ | ⭕ | ⭕ |
| | Data Validation | 🟢 | ⭕ | ⭕ | ⭕ | ⭕ |
| | Version-based restore of application data | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| | Version-based restore of Fileset and files | 🟢 | ⭕ | 🟢 | ⭕ | 🟡 |
| | Direct restore from offsite location | 🟢 | 🟢 | 🟢 | 🟢 | ⭕ |
| | User self-directed restore | 🟢 | ⭕ | ⭕ | ⭕ | 🟡 |
| | Granular Exchange Recovery | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| | Granular SQL Recovery | ⭕ | ⭕ | ⭕ | ⭕ | ⭕ |
| | Granular SharePoint Recovery | ⭕ | 🟢 | ⭕ | 🟢 | ⭕ |
| **Policy and Control Administration** | Centralized Global Management | 🟢 | 🟢 | 🟢 | 🟢 | 🟢 |
| | Advanced Object-based Policy and Control Architecture | 🟢 | ⭕ | ⭕ | ⭕ | ⭕ |
| | Granular Backup Rules | 🟢 | 🟢 | 🟢 | 🟢 | ⭕ |
| | Granular Scheduling Rules | 🟢 | 🟡 | 🟡 | 🟡 | ⭕ |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Data Management** | Version Rule | ● | ○ | ● | ○ | ○ |
| | Version Trimming  Rule | ● | ○ | ○ | ○ | ○ |
| | Offsite Rule | ● | ○ | ○ | ○ | ○ |
| | Centralized Agent Policy Management | ● | ○ | ○ | ○ | ○ |
| | Export and Import Settings and Policy | ● | ○ | ○ | ○ | ○ |
| | Alert Management | ● | ● | ● | ● | ● |
| | Bandwidth Throttling | ● | ○ | ● | ○ | ○ |
| | Quota Provisioning | ● | ○ | ○ | ○ | ○ |
| **Platform Support** | Windows Server 2003 and 2008 R2 | ● | ● | ● | ● | ● |
| | Apple Mac OS X - Leopard, Snow Leopard & Server | ● | ● | ○ | ○ | ○ |
| | Linux (Debian, SuSE, Fedora, Red Hat & Ubuntu, CentOS) | ● | ● | ○ | ● | ○ |
| | Windows XP, Vista and Win 7, Win 8 | ● | ● | ○ | ● | ○ |
| **Virtualization Support** | VM backup and Recovery  -VMware, Hyper-V | ○ | ● | ○ | ● | ○ |
| | Sever Virtualization/Standby Support | ○ | ○ | ○ | ○ | ● |

## Central Management, Reporting, and Analytics Product Line Overview

This section includes product descriptions, value propositions, and key competitive differentiators for Dell SonicWALL's three primary products for central management, reporting, and analytics.

- **Dell SonicWALL Global Management System:** For mid to large enterprises and service providers who need to manage  a number of Dell SonicWALL devices either internally (enterprises) or for their customers (service providers), the Dell SonicWALL Global Management System is a market-leading management, monitoring, and reporting tool that provides granular management, monitoring, and reporting of multiple Dell SonicWALL devices of different types from one central console, increases the productivity of the IT administrator, and is a key enabler of a service provider's business.

- **Dell SonicWALL Analyzer:** For small and mid-sized organizations that need to report on the activity of one or more Dell SonicWALL devices, Dell SonicWALL Analyzer is a market-leading reporting tool that provides granular reporting that allows tracking of network utilization, application usage visualization, remote VPN user connection tracking, and reporting on backup activities.

- **Dell SonicWALL Scrutinizer:** For mid to large enterprise organizations and for service providers who need to report on the activity of one or more network devices. Dell SonicWALL Scrutinizer is a market-leading network traffic monitoring, analysis and reporting tool that provides granular reporting on one or more firewalls, routers and switches from Dell SonicWALL and other vendors to track network utilization and visualize application usage.

## Customer Pain Points

### Enterprises and MSPs: Pain Points addressed by the Global Management System

As distributed networks grow exponentially, businesses face increased complexity and cost in managing, monitoring and reporting on the network infrastructure to maintain maximum network uptime. Many enterprises are subject to regulatory compliance mandates with increasingly strict requirements; all the while budgets remain constrained. Service providers responsible for managing a large number of their customer's network devices have difficulty maintaining service level agreements (SLAs) while achieving an acceptable return on their investment. Without next-generation syslog reporting and application traffic flow analytics, organizations lack insight into their network to really understand bandwidth utilization, application traffic network impact, and employee productivity. As such, many organizations need an easy, affordable approach to network security management, which can scale across thousands of appliances and security policies.

### SMBs: Pain Points addressed by Analyzer

Understanding network events and usage such as slowdowns, outages, security threats, and bandwidth consumption by application is essential for organizations of all sizes. Bandwidth utilization spikes and network threats emerge as employees download files, watch videos and use non-work related web applications. In turn, productivity plummets when employees access web sites for personal reasons (e.g., web mail, Facebook) and utilize non-work related applications (e.g., Skype, instant messaging). When it comes to troubleshooting network problems, time is money.  Providing IT administrators with powerful troubleshooting tools to easily identify the source of the issue is essential to overall efficiency and cost savings. But the majority of third-party application traffic analytics and reporting products available today offer IT administrators limited granularity and can be complex and difficult to integrate with the firewall. To strengthen security awareness, optimize network utilization, manage applications and provide troubleshooting and forensics capabilities, IT administrators require a solution that provides an intelligent, comprehensive view of security events and application traffic utilization throughout the network.

### Enterprises and MSPs: Pain Points addressed by Scrutinizer

Facing budget and costs constraints, businesses are under increasing pressure to minimize costs, optimize capital investment and minimize monthly Internet service costs. At the same time, non-business-related web traffic, such as social media, is increasing exponentially, draining bandwidth and productivity. IT is constrained by outdated monitoring and reporting tools that provide limited visibility into ports and protocols yet lack insight into application traffic flow across the firewalls, routers and switches on the network. What's more, traditional firewalls do not always adequately stop threats originating from infected hosts inside the network. Value Added Resellers carry the added burdens of demonstrating service value to customers while controlling their own costs and the amount of time spent managing individual customer accounts.

### Product Line Positioning and Key Messages

Dell SonicWALL offers a variety of management and reporting solutions to meet these unique needs. Dell SonicWALL Global Management System (GMS®) , Scrutinizer and Analyzer complement and extend Dell SonicWALL security products and services, helping businesses optimize security, manage growth and ease administrative burdens.

| | Analyzer | GMS | Scrutinizer |
|---|---|---|---|
| Target Market | SMBs | Enterprises, MSPs | Enterprises, MSPs |
| Functionality | Reporting & Analytics | Reporting & Analytics<br>Policy Management<br>Monitoring & Alerting | Flow Analytics<br>Deep Forensics<br>Monitoring & Alerting |
| Device Support | Dell SonicWALL Appliances Only: Firewall, CDP, SRA | Dell SonicWALL Appliances Only: Firewall, CDP, SRA, Email Security | Entire Network:<br>Third Party routers, switches (including Dell), firewalls, etc.<br>Dell SonicWALL firewalls |
| Reporting & Monitoring Protocols | Syslog | Syslog, SNMP | Almost all flow based protocols (NetFlow, IPFIX, etcetera) |

## GMS Software for Enterprise and MSP Customers

GMS provides organizations, distributed enterprises and service providers with a powerful and intuitive solution to centrally manage and rapidly deploy Dell SonicWALL firewall, Dell SonicWALL anti-spam, Dell SonicWALL backup and recovery, and Dell SonicWALL secure remote access solutions. Flexibly deployed as software, hardware, or a virtual appliance, Dell SonicWALL GMS offers centralized real-time monitoring, and comprehensive policy and compliance reporting. The incorporation of next-generation syslog for application traffic analysis results in granular, flexible and easy-to-use real-time application level reporting capabilities.

For enterprise customers, Dell SonicWALL GMS streamlines security policy management and appliance deployment, minimizing administration overhead and supporting compliance initiatives. Service Providers can use GMS to simplify the security management of multiple clients, demonstrate value to their customers, maintain Service Level Agreements, and increase profitability. For added redundancy and scalability, GMS can be deployed in a cluster configuration.

Note that GMS and Analyzer share the same software binary.  Depending on what license key is entered during installation, the software manifests itself as either GMS or Analyzer.  GMS offers all the reporting and analytics functionality available in Analyzer. Unlike Analyzer, GMS also offers central policy management and monitoring capabilities.  It is possible to upgrade an Analyzer system to GMS.

## GMS Features and Benefits

- **Centralized security and network management** helps administrators deploy, manage and monitor a distributed network environment.
- **Set policies** for thousands of Dell SonicWALL Firewalls, Anti-Spam, Continuous Data Protection (CDP), and Secure Remote Access (SRA) devices from a central location.
- **Sophisticated VPN deployment and configuration** simplify the enablement of VPN connectivity and consolidate thousands of security policies.
- **Universal dashboard** features customizable widgets, geographic maps, and user-centric reporting.
- **Active-device monitoring and alerting** provide real-time alerts with integrated monitoring capabilities, facilitate troubleshooting efforts allowing administrators to take preventative action and deliver immediate remediation.
- **Centralized logging** offers a central location for consolidating security events and logs for thousands of appliances, providing a single point to conduct network forensics.
- **Flexible deployment options** include software, a hardened high-performance appliance, or a virtual appliance to optimize utilization, ease migration and reduce capital costs.
- **Offline management** enables scheduling of configurations and/or firmware updates on managed appliances to minimize service disruptions
- **Streamlined license management** for Dell SonicWALL appliances via a single unified console, simplifies the management of security and support license subscriptions.
- **Simple Network Management Protocol (SNMP) support** provides powerful, real-time traps for all TCP/IP and SNMP-enabled devices and applications, greatly enhancing troubleshooting efforts to pinpoint and respond to critical network events.
- **Rich integration options** include an application programming interface (API) for web services, CLI support for the majority of functions, and SNMP trap support for both services providers and enterprises.
- **Real-time and historic next-generation Syslog reporting** through a revolutionary enhancement in architecture streamlines the time-consuming summarization process, allowing for near real-time reporting on incoming syslog messages.

- **Extensive cross-platform reporting** capabilities include support for numerous Dell SonicWALL products, including Firewalls, Anti-Spam, Continuous Data Protection (CDP), and Secure Remote Access (SRA) platforms.
- **Intelligent reporting and activity visualization** presents comprehensive management and graphical reports for Dell SonicWALL Firewall, SRA and CDP devices yielding greater insight into usage trends and security events, while delivering a cohesive branding for service providers.

## Scrutinizer Software for Enterprise and MSP Customers

Dell SonicWALL® Scrutinizer is a multi-vendor, application traffic analytics visualization and reporting tool to measure and troubleshoot network performance and utilization while increasing productivity for enterprises and service providers. Scrutinizer supports a wide range of third party routers, switches, firewalls, and data-flow reporting protocols from a large selection of vendors thus providing organizations with increased value and the flexibility of an all-in-one tool to monitor network utilization and visualize application traffic flows across their entire network.

Scrutinizer provides unparalleled insight into application traffic analysis from IPFIX/NetFlow data exported by Dell SonicWALL firewalls. Scrutinizer easily identifies top applications, conversations, flows, protocols, domains, countries, subnets and alerts on suspicious behavior. Scrutinizer also provides historical and advanced reporting, role-based administration, advanced analysis and threshold-based alerts, in addition to numerous special features for MSPs and ISPs.

Note that the Scrutinizer software is based on technology developed by Plixer International. Scrutinizer has been developed completely independently from GMS and Analyzer.

## Scrutinizer Features and Benefits

- **Granular analytics and reporting** provides easy visualization of top hosts, protocols, ports, applications, network traffic, VPN traffic, VoIP traffic and conversations across all network realms and devices. Flexible analysis options can display trend data in bits, bytes, packets or percent of total bandwidth consumed. Scrutinizer offers support for both IPFIX and Flexible NetFlow for fully customizable report templates, and can save all flow records indefinitely.
- **Advanced troubleshooting** of capacity bottlenecks, latency, jigger, Active Timeout, top conversations, top host flows, host volume, pair volume, MAC addresses, VLANs, and domains is available by leveraging IPFIX for deeper insight.
- **Powerful visualization tools** list top interfaces across all routers, switches and firewalls to display real time or archived application traffic data using interactive charts, tables and Google® Maps, an innovative matrix view to show flow fields, and network maps showing relevant flow data.
- **Enhanced forensic capabilities** to detect and alert unauthorized applications, malicious traffic, known-compromised Internet hosts, Flow Sequence Number violations, DNS cache poisoning, rogue IP addresses, DHCP and mail servers, port scanning, excessive multicast traffic, HTTP hijacking and DDOS attacks.
- **Dell SonicWALL Application Traffic Analytics** is a unique solution providing a powerful bundle of industry leading Next-Generation Firewalls and Scrutinizer software. The firewall transmits IPFIX data in real-time to the traffic analyzer collector application, where the administrator can examine usage data by application or user, look at data over different time periods and much more. While some firewall vendors do support NetFlow or IPFIX, only Dell SonicWALL offers this level of application traffic detail.
- **Third-party support** provides compatibility with hundreds of routers, switches, firewalls, and other network devices regardless of vendor to monitor thousands of interfaces simultaneously.
- **Customizable alerting** can be triggered upon interface utilization, unfinished flows, nefarious activities, and degraded voice and video to display how many other alarms the host has violated. Various alerting and notification options including SNMP traps and script execution also facilitates automatic remediation processes.

- **Flexible administration** features allow for customizable dashboards per login, group-based and per login permissions to access flows for specific router, switch, and firewall interfaces. The Scrutinizer Cross Check Module provides integration with third party monitoring and flow analytic tools such as WhatsUp Gold and Orion. MSPs can easily modify style sheets to match branding.

### Analyzer for SMB Customers

Dell SonicWALL® Analyzer is an easy to use web-based traffic analytics and reporting tool that provides real-time and historical insight into the health, performance and security of the network. Analyzer supports Dell SonicWALL firewalls, Dell SonicWALL backup and recovery appliances, and Dell SonicWALL secure remote access devices while leveraging application traffic analytics for security event reports.

### Analyzer Features & Benefits

- **Real-time and historic traffic analysis** utilizing granular next generation syslog data is unique to Dell SonicWALL firewalls and provides advanced troubleshooting capabilities to assist in identifying the location of network outages and slowdowns. While most firewall vendors do support basic syslog reporting, only Dell SonicWALL offers this level of application traffic detail.
- **Comprehensive graphical reports** on firewall threats, bandwidth usage statistics, and application traffic analysis, provides organizations visibility into employee productivity and suspicious network activity.
- **Next-Gen syslog reporting** uses revolutionary architecture enhancements to streamline data summarization, allowing for near real-time reporting of incoming syslog messages. Direct access to the underlying raw data further facilitates extensive granular capabilities and highly customizable reporting.
- **Secure Remote Access (SRA) and Continuous Data Protection (CDP) Event Reporting** leverages next-generation Syslog data to provide powerful insight into appliance health and behavior.
- **Universal scheduled reports** provide a single entry point for all scheduled reports. One report can combine charts and tables for multiple units. Reports can be scheduled and sent out in various formats to one or more email addresses.
- **"At-a-glance"** reporting offers customizable views to illustrate multiple summary reports on a single page. Users can easily navigate through vital network metrics to analyze data quickly across a variety of reports.
- **Compliance reporting** enables administrators to generate reports that fulfill compliance requirements on an ad-hoc and scheduled basis for specific regulatory mandates.
- **Multi-threat reporting** collects information on thwarted attacks providing instant access to threat activities detected by Dell SonicWALL firewalls using the Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service.
- **User-based reporting** tracks individual user activities locally or on remote network sites to provide even greater insight into traffic usage across the entire network and, more specifically, application usage, web sites visited, backup activity, and VPN connections per user.
- **Ubiquitous access** simplifies reporting to provide administrators with analysis of any location using only a standard Web browser.
- New attack intelligence offers granular reporting on specific types of attacks or intrusion attempts and the source address of the attack to enable administrators to quickly react to incoming threats.

## Competitive position in the marketplace

### Key Differentiators

- **GMS:** Unlike management consoles from other hardware vendors our product offers multi-device management at a superior level of granularity for a wider range of devices and very granular, flexible and easy-to-use real-time application level reporting capabilities. Furthermore, GMS includes many more features developed specifically for service providers.
- **Analyzer:** Unlike reporting tools from other hardware vendors our product offers more granularity, flexibility and easier to use real-time application level reporting capabilities.
- **Scrutinizer:** Unlike reporting tools from other hardware vendors our product offers very granular, flexible and easier-to-use real-time application level reporting capabilities and a much deeper and broader level of support for networked devices from a wide variety of third party vendors.

## Dell SonicWALL GMS and Analyzer versus Key Competitors

**Palo Alto Networks (PAN)**

Panorama (VMware Virtual Appliance)

| Strengths | Weaknesses |
|---|---|
| • Intuitive rule sharing engine<br>• Object sharing for policy management<br>• Configuration auditing (running vs. candidate rule set)<br>• Configuration change tracking even if made locally on firewall<br>• Central management of virtual systems (firewalls)<br>• Packet capture integrated well with reporting<br>• Reporting on the firewall as every firewall has a hard drive (does not require Panorama) | • Very expensive. Panorama starts at $10,000 (US MSRP) for only 25 devices. In comparison Dell SonicWALL Analyzer starts at $125 for one TZ firewall and GMS starts at $1,895 for 5 devices.<br>• Near term reporting is done on the firewalls itself (not Panorama) which is limiting for high throughput environments as capacity is limited by the hard drive inside the firewall<br>• No support for dedicated SSL VPN, backup and recovery, or email security appliances<br>• Devices can only belong to one group in Panorama<br>• Limited scalability for Panorama: no distributed server deployment possible<br>• Limited drill down capabilities; customization of reporting is cumbersome; reports are also not near real-time but need to be scheduled |
| **Opportunities** | **Threats** |
| • PAN is not cost effective for SMB customers. A combination of a Dell SonicWALL firewall with Analyzer is much more cost effective<br>• Even for many enterprise and MSP customers Dell SonicWALL GMS is much more cost effective than Panorama.<br>• Customers with high performance near real-time reporting needs should benchmark PAN's performance versus Dell SonicWALL.<br>• Customers interested in true near real-time analytics, rather than reporting will likely prefer Dell SonicWALL GMS<br>• For customers with thousands of firewalls, GMS offers true scalability through a distributed server architecture | • If a customer is not willing to buy a separate reporting product; PAN devices have a hard drive and provide more historic data (up to 30 days for most reports) and more functionality than Dell SonicWALL's onboard visualization. |

### Fortinet

FortiAnalyzer (reporting appliance) and FortiManager (management appliance)

| Strengths | Weaknesses |
|---|---|
| • Fortinet offers more form factors: hosted version (FortiGuard Management and Analysis Service), more appliance options, and a low-end FortiAnalyzer appliance starting at ~$1,500 (US MSRP)<br>• Policy Management: comparison of device config files, dynamic objects, policy checking (although limited to objects), central management for endpoint security clients<br>• Reporting: FIPS certification, migration tools, auto-discovery of FortiGate firewalls, File Sharing, IP Aliases<br>• Other major features (see threats) | • Separate appliances for reporting and management<br>• No real-time reporting (summarization can take hours)<br>• Limited number of logging categories on FortiOS (10-20); no consistent logging categories across devices<br>• Forti-Analyzer is not easy to use: requires both CLI and web UI, customization of reports requires SQL query knowledge<br>• No application usage reports, no VPN usage reports, no user centric reporting<br>• Limited support for clustering multiple devices to support growth in business; capacity increase may require replacement of appliance |
| **Opportunities** | **Threats** |
| • Fortinet sells two separate appliances, Dell SonicWALL sells one integrated reporting and policy management solution.<br>• Dell SonicWALL offers granular near real-time application visualization and other reporting with drill-down capabilities<br>• Dell SonicWALL offers a large number of logging categories (70+) consistent across all firewall models<br>• Dell SonicWALL reporting is easy to use: web UI is used to drill down and create custom reports on the fly.<br>• Dell SonicWALL offers application usage reports, VPN usage reports, user centric reports<br>• Dell SonicWALL GMS allows clustering of servers for scalability and high availability; add servers as required to support growth.<br>• Dell SonicWALL Analyzer is much more affordable for SMBs than FortiAnalyzer | • Walk away from a deal if a customer is set on having the following features fully integrated in the management solution (Dell SonicWALL does not offer these): DLP archiving, DLP searching and eDiscovery, quarantine repository, integrated vulnerability assessment, packet capture |

## Cisco

Cisco Security Manager (CSM) - Windows application only

| Strengths | Weaknesses |
|---|---|
| • Offers role based access control and workflow<br>• Offers rollback to a previous configuration<br>• Integrates with many other Cisco software products (MARS, Cisco Works, Cisco Performance Monitor)<br>• Object sharing for policy management<br>• Extensive site-to-site VPN management capabilities | • CSM is expensive. CSM major upgrades require an additional significant expense.<br>• CSM reporting is limited and lacks reports on web sites, visited, application usage, and other activities.<br>• Cisco does not offer a separate reporting product for the SMB market.<br>• CSM focuses on Cisco firewalls, secure routers, IPS devices, and Anyconnect security clients. |
| **Opportunities** | **Threats** |
| • Cost conscious customers: Major upgrades for Dell SonicWALL GMS are covered under an active support contract. This is a significant savings compared to CSM.<br>• Enterprise and MSP customers looking for best in class application traffic analytics may choose Dell SonicWALL GMS.<br>• SMB customers looking for an affordable solution will opt for Dell SonicWALL Analyzer. | • Customers with an existing Cisco infrastructure and other Cisco management software products may opt for CSM. |

### WatchGuard

WatchGuard System Manager (WSM) – Windows application only (event processor requires Sun Solaris)

| Strengths | Weaknesses |
|---|---|
| • WSM is mainly focused on multi-device management<br>• Very easy to set up complex site-to-site VPN connections<br>• Workflow approval process for policy changes<br>• Policy change history and audit information | • WSM supports only firewalls<br>• WSM does not offer clustering and high availability<br>• Logging and reporting require servers separate from the WSM server, which is not very suitable for the SMB market<br>• Reporting is limited; no easy to use drill down capabilities |
| **Opportunities** | **Threats** |
| • Enterprise and MSP customers looking for best in class application traffic analytics may choose Dell SonicWALL GMS.<br>• Customers for an integrated policy management, monitoring, and reporting solutions will opt for Dell SonicWALL GMS.<br>• SMB customers looking for an affordable solution will opt for Dell SonicWALL Analyzer. | • Customers and resellers with WatchGuard expertise may continue to choose WatchGuard |

## Dell SonicWALL Scrutinizer versus Key Competitors

### SolarWinds: Orion NetFlow Traffic Analyzer

| Strengths | Weaknesses |
|---|---|
| • Offers a wide variety of network monitoring tools in addition to Netflow Traffic Analyzer<br>• Virtual Server Monitoring | • Does not captures 100% of NetFlow data 100% of the time<br>• Does not offer any customized Dell SonicWALL reporting<br>• Does not have the ability to set thresholds and alarming on all NetFlow fields<br>• Does not actively detect threats or network attacks (Flow Analytics) |
| **Opportunities** | **Threats** |
| • Does not natively support Cisco NBAR technology – NBAR is important to any organization that needs detailed application awareness for QoS and network security<br>• Any prospect with Dell SonicWALL firewalls will benefit from customized reporting<br>• Prospects interested in additional insights into web pages visited (URLs), Voice over IP (VoIP),Latency, Jitter, VLAN using NetFlow v9/IPFIX<br>• Prospect who has a high number of interfaces in relation to number of devices. SolarWinds prices by interface, instead of devices. | • If prospect does not have any devices capable of exporting flow based data.<br>• Prospect looking for a full suite of network management tools and NetFlow aggregation is not a priority |

### ManageEngine: NetFlow Analyzer

| Strengths | Weaknesses |
|---|---|
| • Easy to set up, due to limited information being logged and limited customization options<br>• IP grouping | • Has limited ability to store historical data<br>• Lacks flexibility in creating/customizing reports and dashboards<br>• Does not show multiple reporting methods on one dashboard |
| **Opportunities** | **Threats** |
| • Any prospect that needs detailed reporting on all traffic, not<br>• just reports on what is generating the most traffic ("top n activity reports")<br>• Any prospect with Dell SonicWALL firewalls will benefit from customized reporting<br>• Any prospect interested in historical NetFlow data for Quality of Service (QoS), capacity planning, performance monitoring or reducing Mean Time to Know (MTTK) and Mean Time to Repair (MTTR) in secure network infrastructures. | • If prospect does not have any devices capable of exporting flow based data.<br>• Prospect where IP grouping is an immediate and high priority requirement (tentatively scheduled to be available in Dell SonicWALL Scrutinizer in the near term) |

### PRTG: NetFlow Monitoring

| Strengths | Weaknesses |
|---|---|
| • Virtual Server Monitoring<br>• Extensive event logging | • Must deploy probes to monitor remote sites<br>• Requires a proprietary data base<br>• Uses an inconsistent reporting and data aggregation methodology based on multiple protocols to gather information |
| **Opportunities** | **Threats** |
| • Prospect who wants consistency, not a mix of management tool to compile data (SNMP, WMI, sFlow, NetFlow, packet sniffing)<br>• Any prospect with Dell SonicWALL firewalls will benefit from customized reporting<br>• Any prospect that is looking to manage multiple sites and doesn't want to deploy probes will benefit from customized reporting<br>• Any prospect interested in historical NetFlow data for Quality of Service (QoS), capacity planning, performance monitoring or reducing Mean Time to Know (MTTK) and Mean Time to Repair (MTTR) in secure network infrastructures. | • Prospect requiring  packet sniffing capabilities in tool<br>• PRTG's tool has low system requirements Scrutinizer in the near term) |

## Fluke Networks: OptView NetFlow Tracker

| • Strengths | • Weaknesses |
|---|---|
| • Market presence<br>• Offer a variety of network management solutions and products | • Lacks ability to change/customize reports and dashboard and still pull historical data<br>• Generates reports that are not based on live data |
| • **Opportunities** | • **Threats** |
| • Prospect looking for ability to report on all data without having to preset filters<br>• Any prospect with Dell SonicWALL firewalls will benefit from customized reporting<br>• Requires incremental licenses to be purchased based upon the number of reporting devices | • Prospects will lean towards OptView NetFlow Trackers if they own other Fluke Networks products.<br>• |

## Comparison of Features and Functions: Dell SonicWALL and Key Competitors

**Dell SonicWALL GMS versus Key Competitive Products**

| Features | Dell SonicWALL Global Management System | Palo Alto Networks Panorama | Fortinet FortiManager | Cisco Security Manager | WatchGuard System Manager |
|---|---|---|---|---|---|
| Integrated Solution | Yes | Yes | No | Yes | Yes |
| Policy Management | Yes | Yes | Yes | Yes | Yes |
| Reporting | Yes | Yes (some done on firewall) | No (separate product) | Limited | Limited (requires separate server) |
| Application Visualization | Very extensive | Yes | No | No | Limited |
| Near real-time easy to use analytics | Yes | Limited | No | No | No |

### Dell SonicWALL Analyzer versus Key Competitive Products

| Features | Dell SonicWALL Analyzer | Palo Alto Networks Panorama | Fortinet FortiAnalyzer | Cisco Security Manager | WatchGuard System Manager |
|---|---|---|---|---|---|
| Dedicated Reporting Product | Yes | No | Yes | No | Yes |
| Application Visualization | Yes | Yes | No | No | Limited |
| Custom Reports | Extensive | Yes | Difficult (requires SQL queries) | Limited | Limited |
| Near real-time easy to use analytics | Yes | Limited | No | No | No |
| Price | Very Affordable | Very Expensive | Neutral | Very Expensive | Neutral |

### Dell SonicWALL Scrutinizer versus Key Competitors

| Features | Dell SonicWALL Scrutinizer with Flow Analytics | SolarWinds Orion NetFlow Traffic Analyzer | ManageEngine NetFlow Analyzer | PRTG Network Monitor | Fluke Networks OptiView NetFlow Tracker |
|---|---|---|---|---|---|
| Customized Dell SonicWALL Reports | Yes | No | No | No | No |
| Requires Incremental Licenses | No | Yes | No | No | Yes |
| Cisco NBAR Support | Yes | No | Yes | No | Yes |
| Required Vendor Proprietary Hardware | No | No | No | No | No |
| Includes VoIP Metric Analysis | Yes | Yes | Limited | No | Yes |
| Ability to capture historic data | Yes | limited | Limited | limited | limited |
| Collects 100% of NetFlow traffic | Yes | No | No | No | Yes |
| Priced by Device | Yes | No | No | No | No |

## Dell Sales Details

## Impact to on-going Dell Partnerships

**Channel Experience**

- SonicWALL has a strong channel program with 15,000 resellers and distributors providing extensive global coverage; this go-to-market flow will be preserved.
- Like we have with other acquisitions, we will offer SonicWALL's existing channel members an opportunity to join our current PartnerDirect program, which will enable them to preserve the investments made with SonicWALL.
- Dell plans to take the very best of the SonicWALL channel programs and model and combine it with our PartnerDirect program to bring the best to channel members.
- SonicWALL's partners will have access to PartnerDirect's certifications, training, support, marketing resources and other benefits.
- Dell's PartnerDirect program is available in 148 countries with more than 100,000 partners worldwide.
- SonicWALL partners will be able to utilize the PartnerDirect deal registration tool that will also honor any legacy deals.
- SonicWALL partners will have the access and support to sell the full Dell product and solution portfolio.
- Dell intends to expand its own channel team's customer relationships by further enabling our existing partners to sell SonicWALL solutions.

## Sales Engagement Process

The process for selling Dell SonicWALL products will not change initially.  Sales will continue to work with their S&P representatives to quote and sell the SonicWALL products.  The plan is to modify the existing S&P skus into Dell product skus.  Sales will be notified when those changes take place.

## Deal Registration

In order to determine if an opportunity exists in either the Dell Direct or Dell SonicWALL Channel sales pipeline, the Deal Registration process will be followed.  Direct sales representatives will need to forecast opportunities that are valued at or above $10,000 (Retail) in Salesforce.com.  (The $10,000 value is for SonicWALL hardware and software only.  You would not include servers or client hardware in this threshold amount.)  A questionnaire will be emailed to the Sales rep for completion.  This questionnaire is required to complete the deal registration.  The questionnaire will need to be returned for review.  A Tiger team will review all net new deal registrations to determine if a similar valid opportunity exists in the Channel Partner registration portal.  The Tiger team will notify all sales teams which team (direct or channel) has been granted deal registration.

**From the Rules of Engagement Guidelines:**

## ROLES AND RESPONSIBILITIES

In order to have a successful deal registration program that is mutually beneficial to Dell (Direct Sales) and our Channel Partners, we must have clear roles and responsibilities for our Segment Teams, our Channel Teams, and our Channel Partners.

### Role of the Segment Team

It is the Segment Team's responsibility to forecast all opportunities which are not the subject of a deal registration for their accounts within Salesforce.com (SFDC). Forecasts should contain all details of the opportunity: project description, products being promoted, the end-user contact details, notes, trip reports, etc. Except with respect to opportunities which are the subject of a deal registration, the Segment Team is also expected to update their opportunities as they move through the sales cycle and make sure opportunities do not go beyond the book date. Segment Teams should also make sure their accounts are up to date and scrub for any duplicate accounts and/or contacts. Except as expressly permitted by your region's Deal Registration Official Guidelines, the Segment Team may not proactively pursue a registered Channel Partner opportunity. The Segment Teams are encouraged to call Channel Partners on approved registrations only after coordination with the Channel Team. The Segment Teams should not contact an end-user about other potential opportunities related to active registered opportunities (for example, propose a server on an existing storage opportunity).

The Segment Team should not set up new accounts for Channel Partners or alter, modify, cancel, update, or otherwise change an approved deal registration. Segment Teams should ensure all Channel Partners are transferred to the Channel Team when appropriate and that they are not identified as an end-user in SFDC. As noted above, it is the responsibility of the Segment Team to maintain their forecasted opportunities in SFDC – including run-rate business. If an opportunity has not been updated for more than 120 days and/or is more than 120 days beyond the book date, the opportunity will be considered invalid. The opportunity can then be removed from the Segment Team's forecast through a request via the designated Segment SPOC. Once removed from the Segment Team's forecast, the opportunity will be available for Channel Partners to pursue deal registration.

### Role of the Channel Team

The Channel Team is responsible for developing trust and building relationships with, and providing education and support to, the Channel Partner. The Channel Team should ensure that any opportunity that qualifies for registration is submitted through deal registration and that registered opportunities are kept up-to-date by adding notes, trip reports, and updates throughout the sales process – ensuring that the stage, expected revenue and opportunity does not go beyond the book date. The Channel Team should ensure that the Channel Partner complies with the applicable Deal Registration Official Guidelines for that region. In addition, the Channel Team is responsible for informing the Segment Teams of any business plans and/or agreements as appropriate.

## DEAL REGISTRATION

The Deal Registration Team will decide if a Channel Partner can be granted deal registration by checking the segment end-user account and any parent and subaccounts for any similar valid opportunities that may exist in the segment for the opportunity requested to be registered by the Channel Partner.

## Sales FAQs

**Q: Who is SonicWALL and what do they sell?**

**A:** SonicWALL is a leader in advanced network security and data protection. SonicWALL provides integrated Web Security, Firewall, VPN, Anti-Virus/Malware, Intrusion Detection & Prevention, Content Filtering and Application Control in an appliance. SonicWALL has a strong channel program with 15,000 channel partners providing extensive global coverage. Small and large enterprises trust SonicWALL solutions to detect and control applications and protect networks from intrusions and malware attacks.

**Q: Why is Dell acquiring SonicWALL?**

**A:** IT security threats, like viruses, spam, and malware, continue to evolve and grow more complex. Protecting secure information is a top concern and challenge for our customers. For system administrators to ensure a stronger shield against security threats, a single integrated solution is becoming a necessity. SonicWALL offers comprehensive solutions to customers that include protection against these multiple IT security threats. SonicWALL's capabilities complement Dell's security solutions portfolio.

**Q: How does Dell intend to use and benefit from the SonicWALL technology?**

**A:** At this time, we are not discussing the potential product integration roadmap. We will provide additional information in the future.

**Q: How will this acquisition impact our strategic relationships?**

**A:** Our strategic relationships have not changed. At Dell, we will be driven and directed by customer choice – our strategic relationships allow us to offer a wide range of products and solutions to meet customer needs.

**Q: Will our sales teams be able to sell SonicWALL's existing product line today?**

**A:** Yes, you can now sell SonicWALL products through our global reseller agreement. You should coordinate with your S&P team representative as you have previously. They will engage the SonicWALL team for you.

**Q: Will Dell support existing SonicWALL customers?**

**A:** Following the close of the transaction, it is Dell's intention to continue to support customers who have purchased SonicWALL solutions.

**Q: How does this announcement relate to Dell's software solutions strategy and competitive offering?**

**A:** Software plays an increasingly important role in Dell's future as an end-to-end IT solutions provider. Dell already has strong software capabilities in fast-growing areas, including systems management (KACE), cloud integration (Boomi), and infrastructure virtualization and workload orchestration (Scalent), as well as more recently next-generation unified backup, archive and replication (AppAssure). In addition to these capabilities, Dell has world-class software expertise in servers, storage, networking, and mobility solutions. SonicWALL's capabilities complement Dell's security solutions portfolio and will enable us to provide a stronger network security and data protection solution to our customers. SonicWALL offers a comprehensive Unified Threat Management solution to SMBs and Next Generation Firewall to Large Enterprise and Public customers.

All documents relating to this announcement are available on the Dell SonicWALL SalesEdge Dashboard located here

DELL CONFIDENTIAL
*Do not distribute or share with non-employees for any reason.*