Software

Achieving Endpoint Protection through the SANS Institute's 20 Critical Security Controls

Abstract

Today's technology provides a wealth of opportunity. For example, by adopting bring your own device (BYOD) policies, you can enable your employees to work from anywhere, anytime, increasing their productivity. And the ever-growing volumes of data you collect present opportunities for data mining and business intelligence.

But these market trends also represent security risks, especially given that attacks are increasing in both number and sophistication. Therefore, protecting your environment is a balancing act. Be too lax on security and you incur too much risk. But apply too much security and your users can't do their jobs. It can seem like an impossible task, especially with limited IT staff and budget.

But it's not. This paper details how you can protect your environment, from endpoint to perimeter, by understanding the critical security controls needed in today's complex IT environments and choosing tools that make it easy to implement those controls.

Introduction

Protecting your environment today is a complex, multi-faceted task. Accurately knowing what devices are connecting to your network and what software is on those devices lays the foundation for security, and it also plays a critical role in effective asset management and system backup and recovery. Once you know what's accessing your network, you need to effectively manage the configurations of your endpoints (desktops, laptops, tablets, mobile devices, servers and more), and automatically and continually scan your network for new assets and vulnerabilities.

You also have to address the security of applications, making sure that they're patched and up to date — especially critical security software such as antivirus applications. And you need tight controls over administrative privileges, since end users

Forrester reports that 200 million employees already bring their own devices to work.

continue to be catalysts for security breaches.

Finally, you need to accomplish all of this in a balanced approach that protects your environment without getting in the way of your day-to-day operations. This paper explores the market trends complicating endpoint security today, explains the 20 Critical Security Controls defined by the SANS Institute for achieving endpoint security, and details how two solutions from Dell cover 16 of the 20 controls — giving you broad coverage of security best practices quickly and easily.

Market trends increasing pressure on endpoint security

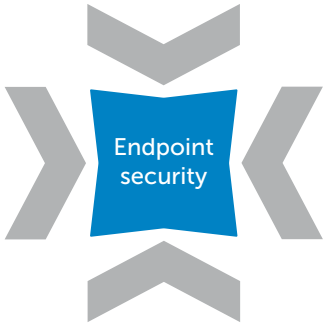
Protecting your environment today is harder than ever. Several market trends in particular are increasing pressure on endpoint security: expanding compliance regulations, evolving user behavior, ever more frequent and sophisticated threats, and limited IT staff and budgets (see Figure 1).

Compliance pressures

You have an increasing variety of regulations, from software licenses to regulatory mandates like SOX, PCI and HIPAA with which to comply — so many, in fact, that 75 percent of organizations say they lack resources to meet compliance regulations, according to Ponemon Institute.

Evolving user behavior

IT infrastructures are already complex, often including distributed locations and multiple operating systems. Trends in user behavior are adding to that infrastructure complexity — and introducing new security concerns. In particular, the scope of devices that are potential catalysts of security breaches is swelling, as previously passive objects become more intelligent and more of them communicate wirelessly with the advent of the Internet of Things (IoT). Forrester reports that 200 million employees already bring their own devices to work, and Infinite Research notes that 96.38 million enterprise



Evolving user behavior
200 million employees bring their own device to work.[1]
26 billion new devices will be connected to the internet by 2020.[2]

Compliance pressures
75% of organizations lack resources to meet compliance regulations.
73% say increasing audit burden is their biggest challenge.[3]

Limited IT staff and budgets
Average growth of IT budgets was 2.1% in 2014.[4]

Growing threats
In just one month, 280 million malicious programs, 134 million Web-borne infections, and 24 million malicious URLs are detected.[5]

Figure 1. Market trends are increasing pressure on endpoint security

[1] "Mobile Is The New Face Of Engagement," Forrester Research, February 2012.
[2] "Forecast: The Internet of Things, Worldwide, 2013," Gartner.
[3] "2013 State of the Endpoint," Ponemon Institute, December 2012.
[4] "Forecast Alert: IT Spending, Worldwide, 2Q14 Update," Gartner.
[5] Kaspersky Threat Report, April 2012.

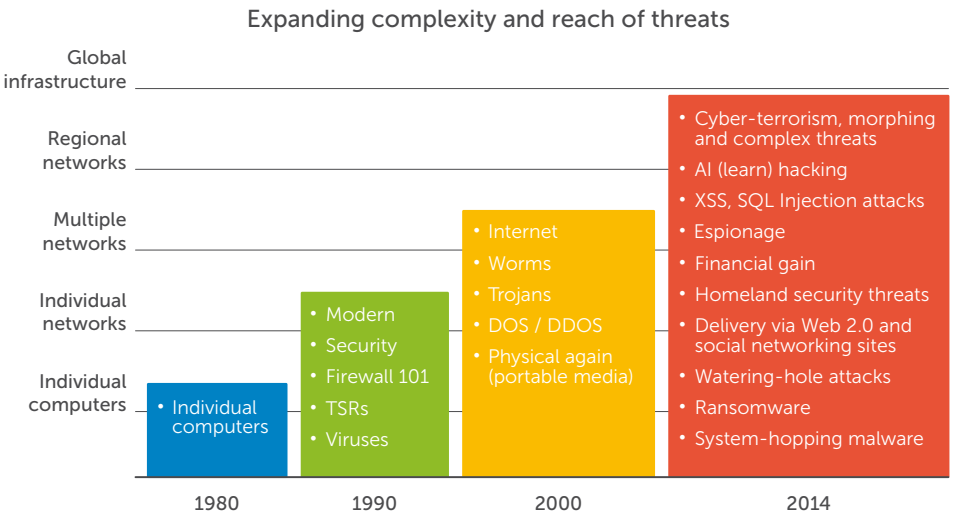


Figure 2. The expanding complexity and reach of threats

tablets are expected to ship worldwide in 2016. Gartner predicts that the installed base of "things," excluding PCs, tablets and smartphones, will grow to 26 billion units in 2020. More connected devices means more catalyst for security breaches.

Enterprises want to take advantage of the benefits of these changes in user behavior, while also protecting their networks, data and users.

Growing threats

Meanwhile, threats continue to grow in both number and sophistication. For example, 280 million malicious programs, 134 million web-borne infections and 24 million malicious URLs were detected — all in just one month.[5] Moreover, the complexity and range of those threats has morphed from "simple" viruses and worms to full-fledged cyber-terrorism and other attacks using sophisticated tactics such as SQL injection (see Figure 2).

Limited IT staff and budget

Finally, despite these growing pressures on endpoint protection, IT staff and budgets grow marginally or not at all (see Figure 3), making it difficult to keep your environment protected. For instance, StatCounter found that more than 16 percent of PCs worldwide still have Windows XP installed even though

> The complexity and range of threats has morphed from "simple" viruses and worms to full-fledged cyber-terrorism and other attacks using sophisticated tactics such as SQL injection.

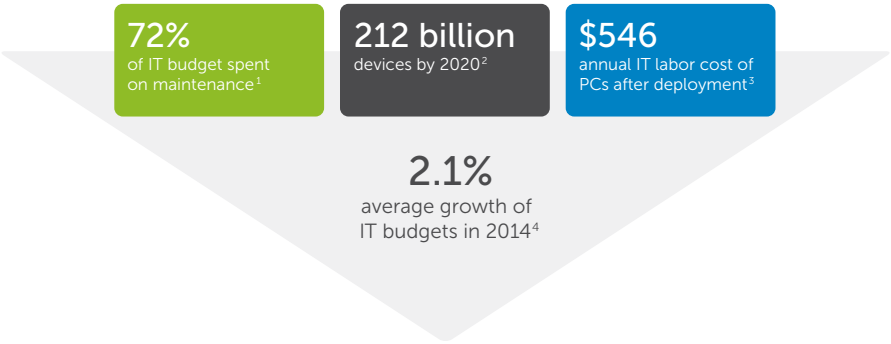


Figure 3. IT departments today must do more with less.

[1]"How to balance maintenance and IT innovation," Computerworld, Oct. 21, 2013.
[2]"Rethinking IT Asset Management in the Age of the Internet of Things," IDC, March 2014.
[3]"Desktop Total Cost of Ownership: 2013 Update," Gartner.
[4]"Worldwide IT Spending Forecast, 2Q14 Update," Gartner.
[5]Kaspersky Threat Report, April 2012.

In concert with a global consortium of agencies and experts from private industry, the SANS Institute created a list of 20 actionable controls with high payoff.

Microsoft's support has already ended — a clear security and compliance risk. Part of the problem is that day-to-day IT operations costs are so high: an IDC white paper sponsored by Dell found that the average deployment cost per PC is $615, and WIPRO pegged the annual cost of supporting a laptop at $969 (assuming a five-year refresh rate). Such costs can quickly erode whatever budgets IT organizations have.

Protecting your environment has never been more important

Understanding the importance of mastering these challenges and protecting your environment requires only glancing at the headlines. Organizations are breached every day, by attacks on their networks and also in other ways, such as theft of laptops containing confidential data (see Figure 4). As a result, organizations lose not only valuable intellectual property but also the customer trust that is the foundation of any business.

Endpoint protection through the SANS 20 Critical Security Controls

How, then, can organizations best protect their IT environments? In 2008, the National Security Agency (NSA) asked the same question, and began assessing which controls have the greatest impact in improving risk posture against real-world threats. In concert with a global consortium of agencies and experts from private industry, the SANS Institute created a list of 20 actionable controls with high payoff. Since these controls were derived from the most common attack patterns and vetted across a broad international community of governments and industries, with very strong consensus on the resulting set of controls, they serve as the basis for immediate high-value action. They provide your organization with a framework or checklist, whether you're just starting your security program or have a more mature model in place.

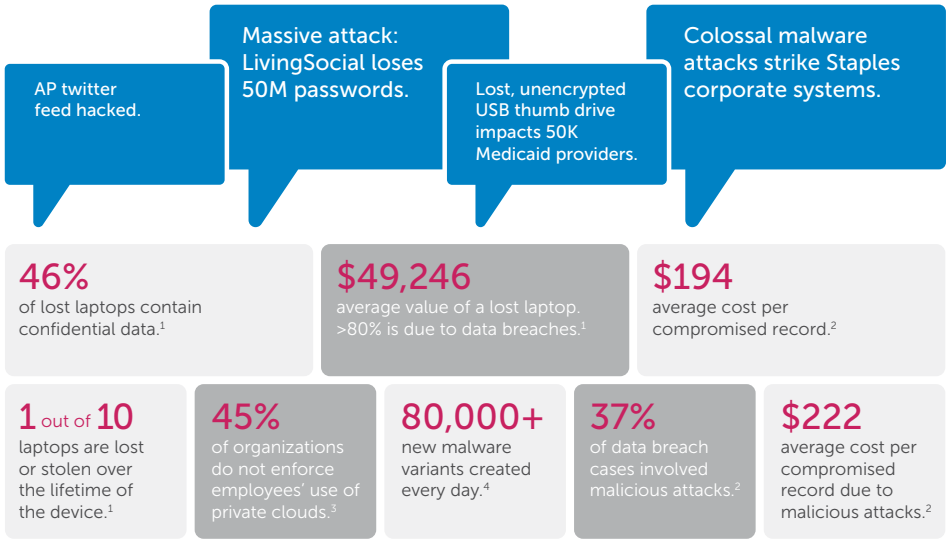


Figure 4. Protecting your environment has never been more important.
[1]"The Billion Dollar Lost Laptop Problem," Ponemon Institute, Sponsored by Intel, October 2010.
[2]"2011 Cost of Data Breach Study," Ponemon Institute, Sponsored by Symantec, March 2012.
[3]"2013 State of the Endpoint," Ponemon Institute, December 2012.
[4]Panda Labs Q1 2012 Internet Threat Report.

The 20 Critical Security Controls, as detailed in "The Critical Security Controls for Effective Cyber Defense, Version 5.0," are:

1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software
3. Secure configurations for hardware and software
4. Continuous vulnerability assessment and remediation
5. Malware defenses
6. Application software security
7. Wireless access control
8. Data recovery capability
9. Security skills assessment and appropriate training to fill gaps
10. Secure configurations for network devices: firewalls, routers and switches
11. Limitation and control of network ports, protocols and services
12. Controlled use of administrative privileges
13. Boundary defense
14. Maintenance, monitoring, and analysis of audit logs
15. Controlled access based on the need to know
16. Account monitoring and control
17. Data protection
18. Incident response and management
19. Secure network engineering
20. Penetration tests and red team exercises

These Critical Security Controls provide a framework or checklist of sorts to all organizations no matter what stage of your security program you're in, whether you're just starting out or have a more mature model in place. If executed in a systematic, automated and streamlined way, these 20 Critical Security Controls not only lay the foundation for a comprehensive security program, but also alleviate the day-to-day IT tasks that bog down many organizations today.

The problem is that establishing, maturing and balancing all 20 Critical Security Controls can be daunting task. So, how can you easily put into place this long list of Critical Security Controls? The best way to prevent being overwhelmed is to break down the Critical Security Controls into related areas:

- First look at these controls from an **operational security or endpoint security** lens. In our view those would be Critical Security Controls 1–4, 6, 12 and 18.
- Next you'll want to break down the Critical Security Controls by **network access**. In our view those would be Critical Security Controls 5–7, 10, 11, 13–16 and 19.
- Then you'll want to look at it from a **data protection and backup** lens, essentially Critical Security Controls 8 and 17.

The 20 Critical Security Controls not only lay the foundation for a comprehensive security program, but also alleviate the day-to-day IT tasks that bog down many organizations today.

Dell Endpoint Systems Management

1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software
3. Secure configurations for hardware and software
4. Continuous vulnerability assessment and remediation
6. Application software security
12. Controlled use of administrative privileges
18. Incident response and management

Dell SonicWALL

5. Malware defenses
7. Wireless access control
10. Secure configurations for network devices: firewalls, routers, and switches
11. Limitation and control of network ports, protocols, and services
13. Boundary defense
14. Maintenance, monitoring, and analysis of audit logs
15. Controlled access based on the need to know
16. Account monitoring and control
19. Secure network engineering

Dell AppAssure

8. Data recovery capability

Dell SecureWorks

9. Security skills assessment and appropriate training to fill gaps
20. Penetration tests and red team excersises

Dell Data Protection

17. Data protection

Figure 5. Dell offers the right mix of software and tools to address all 20 Critical Security Controls.

You can address 16 of the 20 Critical Security Controls with just two solutions: Dell Endpoint Systems Management (ESM) solutions and Dell next-generation firewalls.

- Finally, consider them from a **security assessment, performance and training** angle; we see these as Critical Security Controls 9, 18 and 20.

By breaking up the Critical Security Controls this way, you will create the needed synergies between networking groups, security groups and endpoint management groups.

An action plan for implementing the Critical Security Controls

Dell offers the right mix of software and tools to address all 20 Critical Security Controls in your organization, helping you quickly and easily develop, maintain and manage an end-to-end security plan that doesn't require teams or create silos within your organization (see Figure 5).

Even better, you can address 16 of the 20 controls with just two solutions: Dell Endpoint Systems Management (ESM) offerings and Dell SonicWALL next-generation firewalls. These two solutions alone will give you broad coverage of security best practices quickly and easily — without requiring complex and costly security solutions. Let's explore how they enable you to implement this wide range of controls.

Dell Endpoint Systems Management solutions

Dell ESM solutions comprise a combination of the following:

- **Dell KACE K1000 Management and K2000 Deployment Appliances** (K1000 and K2000) are easy to use, comprehensive and affordable, so they fulfill the systems management needs of organizations of all sizes, from systems deployment to ongoing inventory and management of virtually any network connected device.
- **Dell Desktop Authority Management Suite** extends the systems management capabilities of the KACE appliances with granular user environment customization so you can offer each user the workspace that makes him or her most productive.
- **Dell Enterprise Mobility Management Suite** (EMM) is a flexible, comprehensive mobile enablement solution that securely manages endpoints (including smartphones, tablets, laptops and desktops) and provides secure access to corporate resources, user self-service, and real-time reporting and alerts.

Addressing the Critical Security Controls

Dell ESM solutions address endpoint protection needs from issue detection to assessment and remediation, and offer a number of services to protect endpoint integrity (see Figure 6). They address seven of the Critical Security Controls, as listed below, but more importantly, by addressing the first four foundational controls, they lay the basis for a comprehensive security risk program.

1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software

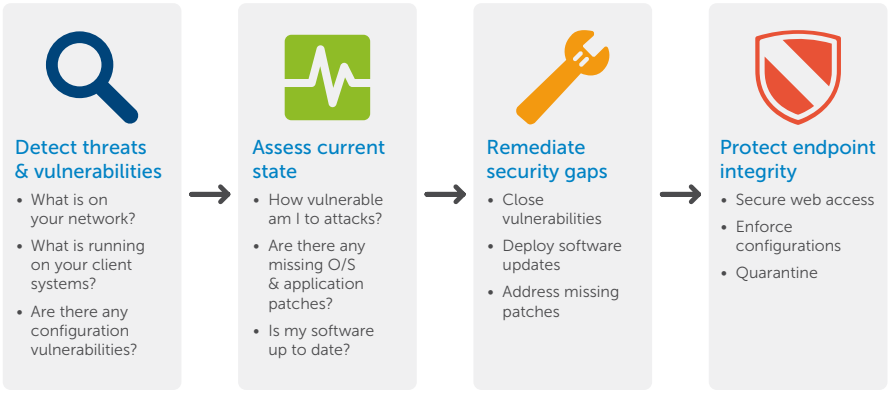


Figure 6. Dell endpoint systems management solutions address many critical security controls.

3. Secure configurations for hardware and software
4. Continuous vulnerability assessment and remediation
6. Application software security
12. Controlled use of administrative privileges
18. Incident response and management

Critical Controls #1 and #2: Inventory of authorized and unauthorized devices and inventory of authorized and unauthorized software

- **Device discovery and inventory** — Many organizations cannot say with a high level of confidence that they have a clear view of everything accessing their network, and that lack of visibility leaves them vulnerable to security attacks. The K1000 provides comprehensive IT asset management through unified discovery, inventory, asset management and reporting for virtually the entire enterprise infrastructure, regardless of platform. By using a variety of protocols to discover all network-connected devices, ICMP-based ping, Telnet, SSH2, SNMP and Socket tests, the K1000 can interrogate the network. If you are unable to authenticate against an endpoint, you can use NMAP to determine the probable operating system residing on a specified IP address. Scanning protocols can be combined and automated to provide fast and reliable identification of all devices, versions of workstations, servers, printers, network devices and any other SNMP-enabled device. Detailed configuration information is captured for desktops, notebooks, servers, printers, and networking equipment such as routers and switches. The full device discovery offered by the K1000 will enable you to capture information about virtually every network-connected device — rogue or legitimate.
- **Software discovery and inventory** — Keeping track of software licenses and usage has become exponentially harder due to the proliferation of versions, inconsistent naming and tracking mechanisms, and increasingly complex license structures. With more than 110 million software entries, the K1000's application catalog contains important information, including application version and name variations, normalized publisher names and categorization of the applications themselves. The application catalog is updated daily and can be downloaded as frequently as needed. It also automatically maps minor versions up to the parent package, thereby enabling tracking of licensing and usage across major versions. The K1000 is able to discern whether an application has been installed in standalone mode or as part of a greater software suite, so you can accurately discover, track and manage software assets across Windows, Mac and Linux operating systems.

Critical Control #3: Secure configurations for hardware and software

- **Configuration management and enforcement** — The K1000 provides fine-grained control over configuration policies so you can easily set up ongoing, automated enforcement as new systems, scripts and software packages are made available. Dynamic policy groupings enable policies to keep the constantly changing content and target systems updated automatically — without administrator involvement.
- **Configuration correction** — With the K1000, you can create and enforce reliable endpoint configurations, as well as maintain a complete audit trail of configuration changes to satisfy regulatory compliance requirements.
- **Software blacklisting** — With the K1000, you can easily blacklist software applications to prevent the execution of undesirable programs known to contain security threats or vulnerabilities, or to prevent the installation of those deemed inappropriate, and enforce secure software configurations on all endpoint devices.
- **Patch deployment** — The huge number of patches released every month can make identifying, prioritizing and tracking patches a challenge. The K1000 offers intuitive search capabilities and views that enable you to quickly filter through large numbers of patches and easily track patch deployment status. In addition, the K1000 provides one of the largest patch repositories and offers WSUS content parity. Plus, it supports Mac patch management, as well as a wide range of

With the K1000, you can create and enforce reliable endpoint configurations, as well as maintain a complete audit trail of changes to configurations to satisfy regulatory compliance requirements.

The K1000 provides an optimal PC lockdown solution by enabling IT teams to assign flexible user privileges that maintain both security and user productivity.

third-party applications from vendors such as Microsoft, Apple, Adobe, Symantec and Mozilla, so you can keep the software on all your systems up to date and secure.

Critical Control #4: Continuous vulnerability assessment and remediation

- **SCAP scanning** — An integrated SCAP scanner within the K1000 provides easy-to-use, automated scan scheduling and detailed reporting so you can manage common endpoint configurations and confirm organizational compliance against requirements.
- **OVAL™ scanning** — The K1000 supports OVAL-based vulnerability scanning of all managed Windows systems. This includes setting the testing schedule and reporting the results. More than 1700 pre-defined tests are included, and new tests are added as they are published.
- **Patch compliance** — The K1000 also provides summary data on patch management and deployment progress, so you can quickly determine which patches have rolled out successfully and which systems are in compliance, and identify and remediate any systems where patching has failed.

Critical Control #6: Application software security

- **Software deployment and configuration enforcement** — The K1000 makes it easy to ensure that key software (such as anti-virus software) is deployed, patched and maintained in accordance with your requirements. The K1000 enforces anti-virus settings: allow control of settings for McAfee and Symantec Antivirus packages, verifying that the software is installed with the configuration specified.

Critical Control #12: Controlled use of administrative privileges

- **PC lockdown** — The K1000 provides an optimal PC lockdown solution by enabling IT teams to assign flexible user privileges that maintain both security and user productivity. With the self-service software portal, your organization can publish approved software titles, license keys, files and scripts that users can access to install applications or configure their systems, whether or not they have local admin rights. You can also blacklist unauthorized or malicious software to prevent it from executing. The integrated service desk seamlessly merges with the system management console so administrators can view employee requests regarding privileges and address them from a single location.
- **Management of user privileges** — With Desktop Authority Management Suite, you can grant users permission to install software, make desktop changes and install ActiveX controls that you deem secure — without granting them local admin rights that would allow them to install unapproved software, copy data to flash drives or incur other risks.

Critical Control #18: Incident response and management

- **Service desk** — The K1000 service desk provides an easy-to-use, comprehensive

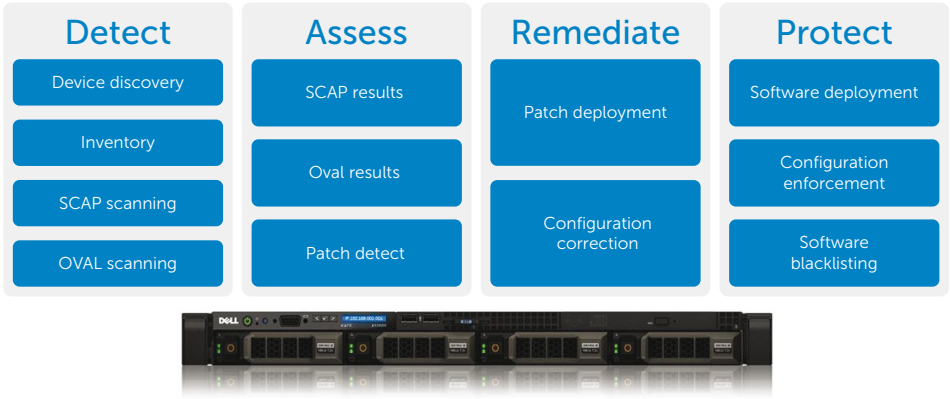


Figure 7. The Dell KACE K1000 Management Appliance addresses endpoint security needs from issue detection to assessment and remediation.

appliance-based alternative to traditional IT helpdesk software management packages. It is fully integrated with the K1000's asset and configuration management capabilities and offers advanced functionality to help automate repetitive management tasks and provide incident management as user or system problems arise.

Dell SonicWALL next-generation firewalls

The Dell SonicWALL family of firewalls tightly integrates intrusion prevention, malware protection, and application intelligence and control with real-time visualization. Dell SonicWALL firewalls provide organizations of any size with a deeper level of network security because they are designed using a scalable multi-core hardware architecture and a patented, single-pass, low-latency, Reassembly-Free Deep Packet Inspection® (RFDPI) engine that scans all traffic regardless of port or protocol.

Dell SonicWALL NGFWs address 10 additional critical security controls:

5. Malware defenses
6. Application software security
7. Wireless access control
10. Secure configurations for network devices: firewalls, routers and switches
11. Limitation and control of network ports, protocols and services
13. Boundary defense
14. Maintenance, monitoring, and analysis of audit logs
15. Controlled access based on the need to know
16. Account monitoring and control
19. Secure network engineering

Critical Control #5: Malware defenses

- **Regular malware signature updates** — Before you can react to new malware, you need to see it. With more than one million sensors and broad collaboration within Dell and throughout the security community, we can identify cyber-attacks before they get to your network. Dell SonicWALL firewalls receive timely updates on malware signatures to protect you from emerging threats.
- **Cloud assist** — A single firewall cannot maintain a catalog of all the malware signatures that might be used to compromise your network. By maintaining a continuous, expanding signature database of 16 million malware signatures in the cloud, Dell SonicWALL firewalls leverage cloud technology to deliver a higher level of security.

Critical Control #6: Application software security

- **Application intelligence and control** — Dell SonicWALL firewalls enable you to see and manage all the traffic going through your network in real time. You can create rules to prioritize important traffic, throttle less important traffic and block unwanted yet legitimate traffic — all with just three clicks. This traffic management not only protects your network but also makes it more efficient.

Critical Control #7: Wireless access control

- **Integrated wireless controller** — The NSA and TZ models have integrated wireless controllers that allow you to create wireless connectivity with SonicPoint access points. For small installations that need some wireless, the TZ line of products offers the option of built-in wireless antennas.
- **Wireless protection** — The Dell SonicWALL Clean Wireless solution goes beyond mere secure wireless solutions by making wireless network as secure as wired networks. The Dell SonicWALL firewall delivers dual protecting by first inspecting traffic and identifying unauthorized intrusions then encrypting the traffic. With the Enforced Anti-Virus option, the firewall can require any wireless user to have the most current anti-virus profiles prior to allowing access to the network.

Critical Control #10: Secure configurations for network devices, firewalls, routers and switches

- **One-touch configuration** — With a single click, you can apply Dell SonicWALL best practices to more than sixty configurations settings. Think of it as a quick tune-up for your firewall settings. Authorized administrators can easily review rules via the management console.

The Dell SonicWALL family of firewalls tightly integrates intrusion prevention, malware protection, and application intelligence and control with real-time visualization.

Dell SonicWALL firewalls transparently decrypt SSL traffic, scan for and remove any threats, and re-encrypt traffic before sending it to the destination.

- **Passwords** — The first step in the easy-to-use firewall setup wizard requires the administrator to change the default access password. Passwords can be configured such that administrators and users are using secure passwords. You can also require passwords be changed after a specified number of days, lock out an account after incorrect attempts at login, and enforce password complexity and length.

Critical Control #11: Limitation and control of network ports, protocols and services

- **Full scanning** — Unlike many competitors' solutions, the Dell SonicWALL firewall scans every byte of every packet on all ports regardless of file size.
- **RFDPI engine** — The patented Reassembly-Free Deep Packet Engine enables simultaneous, multi-threat and application scanning and analysis at extremely high speeds to protect the network from internal and external attacks with a single-pass, latency-free approach.
- **SSL decryption and inspection** — It is estimated that nearly one third of all traffic is encrypted with SSL. To provide truly deep packet security, organizations need the ability to inspect all traffic on any port, whether or not the traffic is encrypted. Dell SonicWALL firewalls transparently decrypt SSL traffic, scan for and remove any threats, and re-encrypt traffic before sending it to the destination.

Critical Control #13: Boundary defense

- **Granular control over external site access** — All Dell SonicWALL firewalls provide the ability to block access to questionable sites by using the content filtering capabilities. Sites can be added to the content filtering list (blacklisting) or removed from the filter (whitelisting).
- **Detection and blocking of intrusion attempts** — The first line of a strong defense is the ability to block intrusions. Today, the best cybercriminals are often at the top of their class at evading detection. Dell SonicWALL uses sophisticated anti-evasion technology to block intrusion attempts.

Critical Control #14: Maintenance, monitoring and analysis of audit logs

- **Dell SonicWALL Scrutinizer** — Available as an option, Scrutinizer gives insight into application traffic analysis from IPFIX/NetFlow data exported by the Dell SonicWALL firewall.

Critical Control #15: Controlled access based on the need to know

- **Zones** — Access to all applications can be controlled with physical interfaces. Security zones are bound to each physical interface where it acts as a conduit for inbound and outbound traffic. Rules and policies can be set within and across zones to restrict access to applications and websites.
- **RADIUS** — Dell SonicWALL appliances can make use of RADIUS to provide secure authentication for individuals and groups. RADIUS can store information for thousands of users and is a good choice for user authentication when many users need access to the network.

Critical Control #16: Account monitoring and control

- **Application control** — From the management console, you can granularly allow or block access to system resources for individual users or groups. Third parties, such as vendors, can access only those resources specifically related to their individual roles; access to all other resources is blocked. You can also securely manage access by guests by creating temporary passwords with expiration dates and use parameters.

Critical Control #19: Secure network engineering

- **Zone functionality** — Dell SonicWALL firewalls enable you to create secure tiers with separate rules, policies and access. In particular, you can create a DMZ zone separate from your internal network, where publicly accessible servers can reside. This separation provides an additional layer of security for your internal network. Even if one of these DMZ servers is compromised, intruders will not be allowed direct access to your internal network.

Dell endpoint systems management solutions + Dell SonicWALL NGFWs

The combination of these two products — Dell endpoint systems management solutions and Dell SonicWALL NGFWs — provides you protection from the outside in and inside out. They:

- Improve security from network perimeters to endpoints
- Increase productivity by minimizing downtime
- Provide dynamic network visibility
- Ensure simplicity without sacrificing security and performance

Moreover, the Dell solutions are fast to deploy and easy to use, ensuring a quick return on investment (ROI) (see Figure 8).

Conclusion

Protecting your IT environment has never been more important, and it has never seemed more difficult. But organizations facing the same challenges as you — complex infrastructures, BYOD, compliance regulations and more — are successfully protecting their environments, from endpoint to perimeter, while enjoying better performance, improved productivity and reduced costs. Dell offers solutions to address all of the 20 Critical Security Controls essential for securing your environment, and with just two solutions, you can cover 80 percent of the controls. Why not get started today?

It's easy to learn more:

Dell KACE:

- KACE live demo: www.kace.com/livedemo
- KACE appliance trial: www.kace.com/trial
- Return on investment (ROI) analysis: www.kace.com/ROIeval
- Website: www.kace.com
- Phone: 1-877-MGMT-DONE
- Email: sales@kace.com

Dell SonicWALL:

- Website: www.sonicwall.com
- Phone: 1-888-557-6642
- Email: sales@sonicwall.com

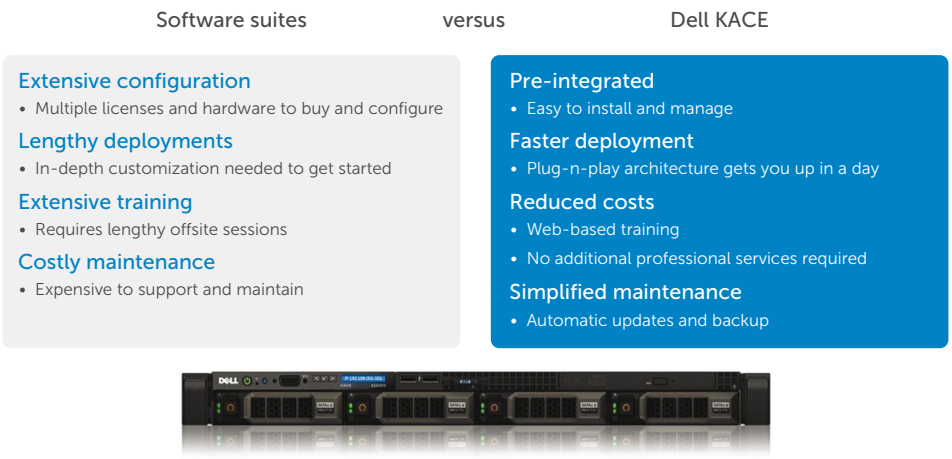


Figure 8. Secure your environment quickly and easily with Dell.

Organizations facing the same challenges as you — complex infrastructures, BYOD, compliance regulations and more — are successfully protecting their environments, from endpoint to perimeter, while enjoying better performance, improved productivity and reduced costs.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.