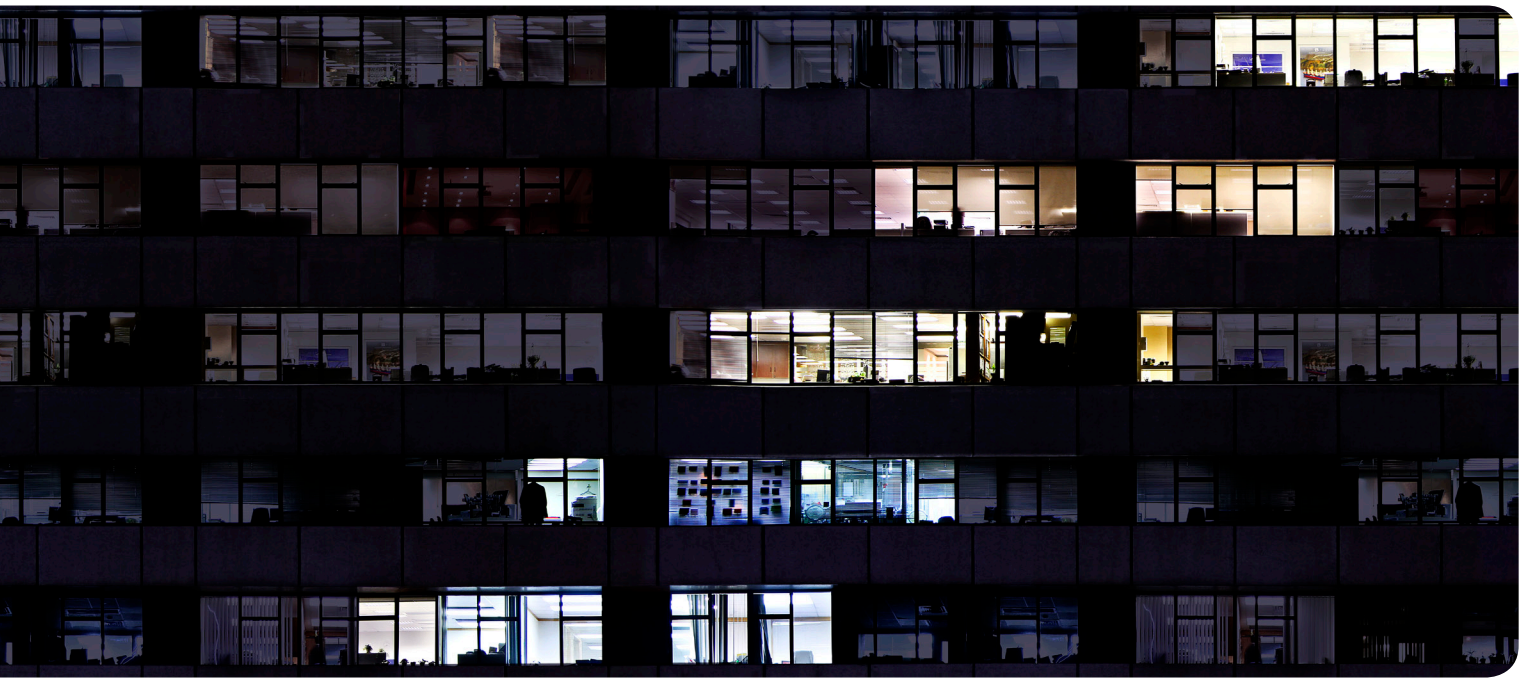
Critical Factors to Endpoint Security



Overview

The modern threatscape of today is very different from the one that existed even five years ago in that organized crime and government operatives are aggressively funding, organizing and building significant offensive capabilities all focused on generating revenue or gaining a competitive advantage in the global economy. "Crimeware" can be bought and sold to anyone and if you're not smart enough to use it, there are even call centers set up providing technical support – we're not in Kansas anymore.

Common attack vectors have also changed dramatically in recent years, shifting from a focus on servers and infrastructure to almost exclusively on users and endpoints. Social engineering and insider attacks are increasing exponentially, effectively making the endpoint the new perimeter. Keeping your data and systems secure has never been more difficult and the bad guys have the upper hand, so we have to respond in kind or become the next headlined data breach for all to see.

Security professionals for years have recommended a layered, defense-in-depth strategy for protecting networks and data, but with the perimeter increasingly becoming the endpoint, a revised version of this layered strategy is in order. While network security controls continue to be an important part of the overall strategy, Dell believes that the endpoint itself, needs a layered, defense-in-depth approach. This involves the secure implementation of three primary security controls:

1. Advanced authentication technologies beyond basic passwords
2. Strong encryption of sensitive data wherever it resides on various endpoints
3. A preventive malware solution that is proactive versus reactive

Additionally, Dell believes that there are a number of other critical factors to the effective deployment of endpoint security which include such things as transparency to end users and IT processes, centralized policy-based management and reporting, tight integration between security software and hardware and finally, independent third party security certifications that demonstrate a trusted implementation. This is what we call "Most Secure" and is why you should consider Dell for all your security software and hardware solutions.

Solutions statement

Dell Data Protection (DDP) solutions help protect your data from device to the cloud with comprehensive encryption, advanced authentication and leading-edge malware prevention.

Dell enables organizations to:

- Implement a variety of advanced authentication methods inclusive of hardware and software technologies
- Encrypt and secure data across multiple endpoints from a common management platform
- Provide a transparent end user interface that supports user productivity while keeping data safe
- Choose from a wide variety of disk encryption technologies including full disk, data centric or self-encrypting drives
- Implement secure virtual sandbox technology to protect employees and endpoints against advanced malware

With Dell organizations can:

- Safeguard data from unauthorized access
- Protect data on any device, removable media, and in public cloud storage
- Protect against zero-day attacks in real-time

Passwords are passé

Passwords have been around as long as information systems have existed for basic access control, but passwords are widely known by both security professionals and end users to be broken. Passwords are without a doubt, one of the weakest links in security today. When we hear that hackers have gained access to accounts or systems, one of the most likely points of attack was via a user password gained inappropriately or simply by employing brute force attacks.

End users write down passwords on paper or keep a list of them on their PCs. They choose passwords that are easy to remember or use the same password for everything and when asked to change, simply add a '1' at the end. Studies have shown (such as a recent one published by Trustwave[1]) that a shocking number of people use passwords like 'Password1' as their Active Directory password (in that study, 38.7% of AD domains checked found users with that password!).

Passwords also come with a high overhead cost to maintain as any IT department of size will tell you in supporting the reset of accounts or just plain lost productivity while users were unable to access their accounts and systems. Clearly, it's time to move beyond passwords and step up to more advanced authentication technologies, not only because compliance mandates tell us to, but because passwords have outlived their usefulness in the context of the sheer number of systems and disparate platforms that users access on a regular basis, just to do their jobs in the modern workplace.

Authenticating a user relies on something you know (password or pin), something you are (biometric) or something you have (a token or smart card), or combinations thereof. In the past, these technologies have been viewed as less reliable and harder to manage than passwords with expensive infrastructure and high replacement costs. This is no longer the case. With Dell's advanced authentication solutions, you can achieve this higher level of security without impacting your infrastructure and with single sign on (SSO) and Active Directory integration, make that experience seamless for your users.

Let's look at an example of how access policy management can be done easily and securely. You have an admin that needs to logon to endpoints for desk-side service visits, and you don't want her to have to enroll on every system she needs to access. On the other hand, you want to ensure that your end user is the only one who can logon to his laptop, even when he is working from home or traveling to conferences. With Dell Data Protection (DDP) | Security Tools, you can set up a policy requiring your end user to enroll with a biometric plus a passcode, while your IT admin logs on with a contactless smart card. If your end user cuts their finger, you have the option of allowing him to configure Recovery Questions and Answers to mitigate desk-side visits, help desk calls and the typical loss of productivity these events represent.

Another current example deals with integrating encryption technologies and strong authentication to securely enable both data protection and access control, perhaps with self-encrypting drives (SEDs) deployed for your mobile workforce. With Dell's pre-boot authentication solution for SEDs, your user authenticates directly into your network using their existing Domain logon credentials. Additionally, with Dell's SED pre-boot authentication architecture, you can support multiple users and have the option to allow individual users to enroll and configure their own self-recovery questions again, without a desk-side visit or help desk call.

[1] *Based upon the Trustwave 2013 Global Security Report http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf*

One of the things that places Dell in a unique position to offer highly secure implementations is the fact that as a hardware manufacturer, we can tightly integrate security software with our hardware. This is another key design tenet in everything we do, which allows us to differentiate our security software solutions as well as our hardware. For example, all authentication solutions need to keep a copy of a reference credential on the system to compare to the credentials provided by your end user. How you store and process this credential information is of critical importance as this reference copy represents a potential point of attack for malware. Dell integrates security software into our hardware, taking advantage of hardware encryption and FIPS-compliant components to protect your user authentication credentials. Let's take a closer look at how we do this.

Many Dell commercial systems ship with a Trusted Platform Module (TPM). DDP | Security Tools encrypts the containers on the system which store user passwords and biometric templates with a key that is protected by the TPM. Additionally, Dell offers Dell ControlVault™ on select Dell Latitude and Dell Precision™ systems. Dell ControlVault™ is a secure authentication processor that provides an isolated processing environment for matching biometric and smart card credentials. Why is this important? By verifying the authentication credentials in a secure, isolated environment, the Dell solution avoids exposing user credentials to any malware that might be resident on the system, thus ensuring the security and integrity of the authentication process and the endpoint. Additionally, Dell offers the broadest range of fully-integrated advanced authentication options, including fingerprint, smart card and contactless smart card readers with Dell ControlVault for secure hardware credential processing.

It's all about the data

In the previous section surrounding passwords, we discussed the huge number of disparate systems and platforms that the typical user accesses on a daily basis to do their jobs and this same phenomenon has significant implications for data as well – it's everywhere! The increasingly fluid nature of data moving from desktop, to thumb drive, to laptop, a tablet, smartphone, hosted application or cloud storage service makes securing this data increasingly problematic.

While the new, dynamic nature of data has yielded significant productivity gains for many users, IT has found itself playing catch up just to keep some degree of security and control of this sensitive data, especially in light of client computing trends of workforce mobility, distributed workforces, and the rise of BYOD or bring your own device. These trends have IT focusing more on securing the data itself, while defocusing on securing the device. This new focus places a unique emphasis on encryption technologies as the primary means to keeping data secure while enabling users to securely access and share this data, anytime, anywhere.

The response from the vendor community thus far to evolving client computing trends has been to retro-fit legacy encryption solutions such as file/folder and full disk encryption solutions to new devices and cloud services with marginal degrees of success. Unfortunately, these legacy solutions have also driven up IT deployment and management costs because they were never designed to protect data as it moves with end users. Dell believes that a different approach to encryption is needed. Let's take a look at legacy technologies as well as Dell's approach to encryption—a data-centric, policy-based approach which allows a single policy to manage the encryption of data anywhere, anytime.

A key design tenet of Dell commercial PCs is tight integration of security software with the hardware.

DDP | Encryption provides a data-centric, policy-based approach to encryption.

Full Disk Encryption (FDE) is a type of legacy encryption that usually encrypts all sectors of a hard drive, except critical files required for boot processes. Implementations of FDE all rely on one consistent boot method used since the introduction of the original IBM® PC. In order to boot without a unique BIOS assisted method, there must be a master boot record (MBR) located at a defined side-track-sector on a designated active and bootable disk to initiate a traditional OS boot. The MBR is responsible for initiating the boot loader. Control is passed to the boot loader that loads a kernel to initiate the file system and activate a set of device drivers capable of communicating with basic boot and user interface devices. Implementations vary, but the earliest point at which encryption could begin is within the boot loader, meaning that the MBR remains unencrypted in most implementations of encryption.

Typically, software FDE implementations load a Linux operating system as part of a real time operating system (RTOS) to enable a degree of customization in the boot process and a less vulnerable attack target. However, the boot method doesn't change. The master boot record of the user operating system is replaced by the encrypting operating system's master boot record and the requirements of the boot operating system's MBR are no different than the user operating system's MBR. The boot operating system then loads the encrypted user operating system. Methods of accomplishing the initial encryption vary by implementation. Most occur as a background task and encrypt silently. Software FDE usually encrypts 100 percent of the drive, minus what is required for the boot process.

There are downsides to this approach. Implementations are seldom partition aware. These implementations are usually not multiple-OS boot aware and may not support all OS's. Also, there is frequently an installation order requirement. While encryption is taking place, some FDE solutions have a small window of data corruption potential. A typical encryption sequence first builds a progress table. The encryption process then reads an un-encrypted sector, encrypts the sector and writes it to the storage device, changes the file system link(s), updates the progress table and repeats until end of disk. If the system is in use, system requested sector reads and writes are compared against the progress mark for encryption requirements. Vendors' corruption window will vary by the success of methods used to abate the corruption potential.

All of the details described above are what makes FDE solutions so difficult to manage and that the FDE software must also be configured to enable management of the user operating system. The management interface for FDE is usually proprietary and requires a separate vendor console to manage it. Recovery and migration have unique implementations and requirements as there are no industry standards for FDE. Key management varies based on the implementation and may or may not support specific enterprise key management architectures.

File and Folder Encryption differs from FDE in that only specific files and folders are encrypted, while applications and the operating system are not encrypted. Though simple in concept, implementation can be daunting. Temporary files created by applications, file and folder copy and paste, print to file, screen copy and paste, back-up files and page and swap files must also be encrypted as these all contain sensitive user data. Additionally, most file/folder encryption implementations are not policy based in that they require the user to remember to save or copy their sensitive files into specific "encrypted folders" to be protected – obvious implementation and security holes abound.

File and Folder encryption is somewhat more attractive from an IT perspective in that it doesn't extract such a high compatibility cost on operations like patch management or system disk recovery when needed. However, typical implementations leave a large amount of the drive available to an attacker and configuration to ensure that all possible storage locations are protected can be a daunting task. Obviously, this type of an implementation leaves a lot to be desired from a transparency perspective and places too much responsibility in the hands of the end user to assure protection.

Dell Data Protection | Encryption (DDP | E) provides a *Data-Centric Encryption* approach which differs significantly from the legacy solutions described above in that an encryption policy specifies what should or shouldn't be encrypted. Encryption policies are quite flexible and may be based on a number of criteria such as user or group membership, specific file type(s) or even a specific application that generates sensitive data. The user doesn't have to do anything additional for encryption to occur – it just works transparently in the background while the user goes about doing their job, while their data is fully protected.

Another significant differentiator to the DDP | E data centric approach is its use of multiple encryption keys. A common key may be used to encrypt all common system data if desired, or may simply be used by multiple users who want to share specific types of sensitive data. Individual, user-specific encryption keys are used so that sensitive data specific to that individual is only accessible by that specific person. This facilitates a common use case of a multi-user medical tablet device being used by several medical staff, all the while keeping sensitive patient data separate from all of the other users, including the IT staff whenever system maintenance is performed.

User files and folders are encrypted with a user key which is protected by the user's authentication token, while applications and the operating system are encrypted with a another key that is opened based on system authentication. User keys are only required to remain in memory for as long as the file is open and are then discarded. When files are backed up to a secondary drive, those files can also be encrypted.

DDP | E supports Opal 1 and Opal 2 self-encrypting drives (SED), with a fully manageable pre-boot authentication environment. Dell's multi-key approach is extended to SED's, with the User, Common and System Data keys being replaced by the SED data encryption key. Dell's solution uses your native Windows/ Domain logon environment, allowing system and patch management solutions to interoperate seamlessly with the SED protected system.

For the ultimate in security, Dell offers the Dell Data Protection | Hardware Crypto Accelerator (HCA), for the highest level of data protection commercially available for system disks –FIPS 140-2, Level 3. This solution protects every sector on the storage device, including the Master Boot Record. The Common key is doubly protected, both by the system TPM and the Dell HCA, and is never exposed to memory in the operating system. Protection begins in pre-OS with user authentication and extends to verifying the integrity of the encrypted key, the system on which it is instantiated, and the Dell Hardware Crypto Accelerator. Only if all of these checks succeed, will the key be loaded and encryption / decryption enabled.

In addition to protecting fixed disks, the Dell Data Protection | Encryption solution can also encrypt removable media, or basically any drive that Windows reads as a drive letter, including optical media. Additionally, the solution extends data protection to both Android and Apple iOS

The DDP | Hardware Crypto Accelerator is the only FIPS 140-2 level 3 certified solution commercially available for hardware encryption, which is fully tamper resistant and secure out of the box.

100,000 new malware variants are introduced each day and are becoming increasingly harder to detect.

based smartphones and tablets, as well as to select cloud service providers, such as Box and DropBox. All of these various endpoints can be managed by policies from a single remote management console, taking manageability to a new level.

Proactive approaches to modern malware

In the beginning of our white paper, we discussed the fact that the user, and their endpoints, have effectively become the new perimeter. In the 2011 US-Cert Investigations Report, phishing and malicious website-based attacks (i.e. attacks involving employees) made up roughly 58% of direct attacks against employees. And according to 2013 reports by Mandiant and Trend Micro, 95% of all advanced attacks involved targeting of the employee via various techniques. Of these techniques, the following are the most successful tactics in getting employees to open the door to your network:

1. *Spear-phishing emails* that deliver the employee to malicious websites that run drive-by download exploits or include weaponized document attachments
1. *Watering hole attacks* that involve hijacking legitimate, trusted sites to push malware to unsuspecting users
1. *Poisoning search results* behind trending news items on popular search engines, such as Google, Yahoo!, and Bing
1. *Social engineering malware* through popular social networks such as Twitter and Facebook

It is estimated by McAfee that 100,000 new malware variants are introduced into the wild each day and these new variants are increasingly using polymorphic techniques to mutate and evade detection. The problem is becoming progressively worse, but is principally comprised of three fundamental issues:

1. Attacks are usually detected months or years after they've invaded your systems, giving the adversary time to colonize the network and steal sensitive data.
2. Millions of dollars are spent on remediation, resulting in unbudgeted, unexpected costs, but what's worse is this money is spent after the damage is done – doing nothing to protect businesses and organizations.
3. While your IT department is fighting the newly discovered virus, the adversary continues to attack other parts of your organization, often times undetected.

As if this weren't bad enough, IT Administrators are at a severe disadvantage to adversaries because many of the security technologies they rely upon require them to be reactive to an attack, not proactive. This reactive mode repeats itself on a nearly continuous basis until the security organization's resources have been completely saturated with detection, remediation and patching cycles, as the attacker(s) have intended. Clearly, there has to be a better way, but before we discuss what Dell is doing in this regard, let's do a quick review of the existing toolsets IT has at its disposal.

Anti-virus (AV) software is inherently reactive because it discovers infections after they occur and is unable to detect new malicious code variants. Typically only a handful of the 40+ AV products will detect new malware. Again, this is because more than 100,000 new malware variants are being released into the wild on a daily basis and malware writers are now using polymorphic techniques to constantly avoid detection.

AV software vendors have made strides to improve their detection rates by adding some behavioral analysis capabilities into their offerings to bolster their signature based technologies, but the software is still reactive and only tells you that something bad has happened after the fact. You still then are left with time consuming remediation and patching activities that could be spent better elsewhere.

Traditional Firewalls are another tool in the arsenal; however, firewalls are designed to stop inbound threats to services that should not be offered outside the organization. In the context of a Web browser or email client, firewalls are ineffective since they block only inbound attacks, and browser malware is initiated by outbound Web page requests that pass through the firewall. Additionally, email attachment based attacks almost always penetrate firewalls to reach employees if the malware is unknown to AV scanners running at firewalls.

Web Gateways like Bluecoat, Websense, and those offered by some of the major AV vendors selectively block Web content from a known malicious source. Their effectiveness revolves around the ability to proactively blacklist untrusted sites or, more restrictively, only allow users to visit certain whitelisted sites so that when a user clicks a link, the gateway may prevent the browser from accessing the site. Similar to AV solutions, Web gateways need to know what is bad beforehand in order to stop your employees from accessing it. Gateways definitely deliver a broader solution than AV because they can blacklist IP addresses and URLs, but they still play a catch-up game of cat and mouse with the adversary.

Application Whitelisting is effective at preventing standalone malware executables from running however, most attacks exploit known trusted applications including the browser, document readers, and document editors. Microsoft Internet Explorer, Adobe Reader and, increasingly, Microsoft Office documents are the most vulnerable, targeted, and widely used applications on the desktop. These applications present a rich environment for attackers to find and exploit vulnerabilities. They also provide fertile ground for adversaries to dupe users into clicking on links and opening documents. As malware exploits those applications, the cyber adversary gains a foothold in the enterprise despite the use of application whitelisting. From that point on, the adversary has access to that machine, the data on that machine, and all network devices to which that machine is connected.

Recently there has been a push for perimeter security solutions that promise to do behavioral analysis of suspicious content using virtual machines. However, there are limitations with this approach:

1. These network devices are typically not placed inline due to the potential to block legitimate traffic (false positives) and the potential delay in analyzing the content
2. Users who are mobile and not at corporate HQ are not covered because the network device does not see their traffic
3. Network security devices have already been circumvented by advanced VM-aware malware.

So, we are beginning to run out of options here and we really haven't addressed how to solve this increasingly prevalent problem set. Let's take a look at how Dell is taking a different approach to meeting this problem in a way that is unlike others that have come before it – it's called Dell Data Protection | Protected Workspace.

Dell Data Protection | Protected Workspace, powered by Invincea, addresses the gaps left by other security solutions by protecting the most important attack surface in the enterprise – the employee and the endpoint. DDP | Protected Workspace employs application virtualization to create a protective "bubble" around applications that run untrusted content – including web browsers, PDF readers and the Microsoft Office suite. It protects users against both known and zero-day malware delivered via spear-phishing, watering hole attacks, drive-by downloads, social networking attacks, fake anti-virus and other online threats. By utilizing Invincea's proprietary secure virtual container technology and running these applications within

Only Dell provides proactive malware prevention on every commercial PC. DDP | Protected Workspace can detect and thwart zero-day attacks in real-time.

Dell offers the world's most secure commercial PCs with best-in-class solutions for comprehensive encryption, advanced authentication and leading-edge malware prevention.

the protected environment on the endpoint, Dell Data Protection | Protected Workspace creates an enterprise "airlock" that stops the potential attack vector from infecting the endpoint and prohibits lateral movement within your network.

The product is quickly deployed as a lightweight Windows application, and is licensed on a subscription basis with flexible renewal options to meet your specific needs. The product has the ability to protect your users against all untrusted content by moving browsers, PDF readers and the Office suite into a contained, virtual environment. You simply configure which applications you want protected and the software turns on the virtual environment to support it. The endpoint solution deploys quickly and easily, just as you would push any Windows-based application.

Unlike other products, the Dell solution does not rely on malware signatures for detection. Instead, it automatically identifies malware attacks by "observing" the behaviors and actions of the applications in real-time within the contained, controlled, and isolated environment. If the product detects any malicious activity or attempts to exploit the application, it gracefully closes the secure virtual container and restores the application back to its pristine state: thereby flushing the malware from memory and denying it the ability to infect the system.

As a result, DDP | Protected Workspace can detect zero-day attacks in real-time as well as Advanced Persistent Threats (APTs) and thwart those attacks with ease. Once an attack has been detected inside our contained environment, we immediately alert the user, discard the tainted environment, and rebuild to a clean state typically inside 20 seconds. The actual file system, the registry, config files, etc, remain untouched . Only Dell provides this proactive malware prevention on every commercial platform we ship.

Summary

We began this white paper by discussing the increasingly sophisticated nature of today's modern threatscape and it is indeed, a very scary place. However, with secure, trusted implementations of the right security solutions, it is possible to significantly reduce the potential impacts of the threat, while keeping users productive and secure.

In the context of endpoint security, Dell believes that by focusing on the three primary areas of advanced authentication, strong encryption and preventive malware solutions, you can successfully secure the new perimeter and meet increasing compliance requirements while you are at it. By addressing each of these areas with software solutions available factory-installed on our commercial PCs, we are able to offer the world's most secure commercial PCs.

Tight integration between the security software and the hardware it is running on is absolutely essential to ensure that authentication credentials and encryption keys are properly maintained and the implementations can be trusted to ensure the integrity of the system. Additionally, independent, third party validation of these implementations, like FIPS or Common Criteria, are equally essential to validate the solution as trusted.

Obviously, there is a lot to consider in effectively choosing the right combination of solutions and services to secure your small business or growing enterprise, and Dell has the expertise to help. At Dell, we believe endpoint security and compliance don't have to be difficult or disruptive. Dell endpoint security solutions protect data wherever it goes without disrupting IT processes or end user productivity. Call one of our sales experts today to learn more about our comprehensive security solutions and services.

For more information on Dell Data Protection solutions, visit **Dell.com/dataprotection**