WHITE PAPER: ENDPOINT SECURITY FOR DELL BUSINESS CLIENTS

symantec.

Confidence in a connected world.

Endpoint Security for Dell Business Clients

Jordan Gardner, Technical Alliance Manager, Symantec, Corp.

White Paper:

Endpoint Security for Dell Business Clients

Contents

Introduction

The IT threat landscape has changed dramatically over the past few years. In the past, the majority of attacks were meant simply to make headline news. Today, attacks have become more sophisticated and stealthy, targeting specific organizations to reap financial gain. Peace of mind can no longer be achieved by simply running a decent firewall and anti-virus software. These days IT administrators find themselves in an entirely new world of security threats, which can not only affect a system's functionality or performance, but may also compromise sensitive corporate data as well as personal or financial information. While performance degrading viruses and self replicating worms still exist today, security threats have expanded in scope and complexity. They are also becoming increasingly financially motivated – making comprehensive endpoint security more important than ever.

Today's organizations need proactive endpoint security tools that can protect against zero-day attacks and even unknown threats. They need to take a structured approach to endpoint security, implementing a comprehensive solution that not only protects from threats on all levels, but also provides interoperability, seamless implementation, and centralized management.

To that end, Dell and Symantec have partnered to define the "Secure Dell Business Client". The purpose of this article is to outline the elements which make up a comprehensive endpoint security strategy for Dell Business Clients (i.e., Dell Latitude, OptiPlex and Precision systems) and to provide a recommended "ideal" solution which would yield the greatest protection at the lowest total cost of ownership (TCO) for most organizations.

Elements of the Secure Dell Business Client

Each of the following sections briefly identifies key areas that should be considered as part of your organization's overall approach for securing user endpoints.

Hardware Level Security

Minimizing your vulnerability to security threats can ensure maximum efficiency and performance across your organization. As a member of the Trusted Computing Group (TCG), Dell has helped define open standards for trusted computing and builds security features into each of their business client systems. Hardware level security can provide greater protection than software based solutions which may introduce operating system or application vulnerabilities.

Personal firewall

Given the current threat landscape and the fact that increasingly mobile workforces are extending the perimeters of organizations' computing infrastructures, endpoints have become a primary target for exploits and attacks. A threat often first infects a single laptop while outside the network perimeter, and then when the laptop connects to the internal network, the threat spreads to other endpoints. Endpoint firewalls can be leveraged not only to block internal network attacks from breaching any endpoint connected to the network, but also to prevent these threats from ever leaving the initially infected endpoint.

Intrusion Detection, Prevention & Device Control

Network threat protection is crucial for protecting endpoints from "blended" threats and to inhibit outbreaks. To be effective, it must encompass more than a firewall. Network threat protection should include a combination of state-of-the-art protection technologies, including intrusion prevention and sophisticated capabilities to control network communications.

Intrusion prevention plays a critical role in the solution's network threat protection scheme, especially if the intrusion is vulnerability based using generic signatures. Vulnerability-based intrusion prevention systems (IPS) can use one generic signature to block the hundreds of potential exploits that can attack a given vulnerability—halting the attack at the network layer so it never has a chance to infect an endpoint.

Antivirus and antispyware

Antivirus and antispyware solutions generally employ traditional scan-based technologies to identify viruses, worms, Trojan horses, spyware, and other malware on an endpoint device. Typical antivirus and antispyware solutions detect these threats by searching the system for files that match characteristics, or threat signatures, of a known threat. Once it detects the threat, the solution remediates it, typically by deleting or quarantining it. For many years, this methodology has been effective for protecting endpoints against known threats and, although it's inadequate for protecting against unknown and zero-day threats more common today, it is still an essential element of overall endpoint security.

Proactive threat protection

According to the Internet Security Threat Report (ISTR Vol XI), it takes 47 days on average for an operating system or application provider to release a patch for a published vulnerability. Attacks that exploit these vulnerabilities before a patch becomes available are often referred to as unseen or zero-day attacks. A few hours after the first vulnerability exploit is detected, vendors typically can release a signature to protect against further attacks from the specific exploit.

As previously mentioned, signature-based file scanning and network scanning technologies do provide key areas of protection, but non-signature-based technologies are needed to address the growing number of unknown threats used in stealth attacks. These non-signature-based technologies are referred to as proactive threat protection technologies and they help guard against unknown or undisclosed vulnerabilities.

Encryption

Data protection is a critical issue in many organizations today as an increasing amount of valuable information travels outside and around corporate networks and is stored on an ever-growing array of endpoint devices, including PCs, laptops, and removable storage devices such as hard disks and USB memory sticks.

In addition to the danger of losing critical Intellectual Property (IP) and either customer or competitive information, data stored in an unprotected state on a laptop and desktop PCs places an organization at risk of becoming the next data breach headline. The only sure way to counter these threats is with strong encryption of all data on the platforms, which also provides a "safe harbor" from the high-profile public disclosures and costly remediation mandated by privacy laws. There are various types of encryption available on the market today.

- **File and Folder level encryption:** Individual files or directories are encrypted by the file system itself. The benefit of file level encryption is that it is flexible – even allowing end users to choose which files and folders to encrypt. It is also easy to implement and more affordable in comparison to other encryption methods, however file level encryption does not offer the same level of security which other encryption methods provide.
- **Full Disk Encryption (FDE):** All of the data included on the disk including the operating system, swap space and the temporary files are encrypted. With full disk encryption, the decision of which files to encrypt is not left up to end users. Full disk encryption is often combined with a pre-boot authentication password as an additional layer of security. There are two different approaches to Full disk encryption:
    - **Software-based FDE:** An advantage of software-based FDE solution is software based encryption can be implemented today no matter what hardware you have. A key disadvantage to software-based FDE is software based FDE adds additional CPU overhead to encrypt and decrypt the data – this could have a negative impact on system performance especially dealing with large files. One could also run into additional software incompatibilities between the software based encryption solutions and the applications running in the environment.

- **Hardware-based FDE**: Hardware based FDE provides the greatest level of protection without either the performance impact or software incompatibilities of software-based solutions. A disadvantage to hardware-based FDE solution is the FDE hard drives need to be purchased and replace existing drives which adds cost to implementing such a solution.

Application Control

Companies today are struggling to manage the problem of unwanted software, including viruses, malware, unlicensed software, vulnerable software, and non-business software. Locking down systems privileges can adversely impact the rights various applications may need to perform optimally. Application control can be used to balance the performance and functionality of authorized applications with the access control settings necessary to a secure a system.

Network Access Control

IT administrators go to great lengths to ensure that newly deployed desktops and laptops are configured according to corporate policy, including all the applicable security updates, approved application sets, antivirus software, firewall settings, and other configuration settings. Unfortunately, as soon as those machines are put into production, administrators often lose control of the configuration of those endpoints.

Remote and mobile users create even greater exposure when they use their non-compliant laptops at Internet cafés, hotel rooms, or other non-secure locations where they are even more vulnerable to attack or infection – and then they bring those devices back inside the corporate firewall.

Network access control solutions minimize such risks by ensure endpoints comply with minimum security configurations before they are allowed onto corporate networks. Any devices found to be non-compliant can be temporarily quarantined and remediated before they are allowed access to the network.

Patch management

The CERT Coordination Center (http://www.cert.org/), a security industry standard for Information Technology (IT) professionals, estimates that 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches. So a final key aspect of security involves management, i.e., keeping all OS, application and hardware updated with the latest vendor recommendations.

The ideal endpoint security solution for Dell Business Clients

So, given the above litany of security considerations, how does an IT administrator implement a comprehensive approach to securing an enterprise? Clearly, the right combination of tools can provide necessary levels of automation and monitoring to get the job done.

Total cost of ownership considerations

There are many products on the market today which range in price and functionality to solve specific security pain points. Therefore, the goal when it comes to endpoint security is to enable maximum protection with minimal total cost of ownership. Dell and Symantec believe this goal can be achieved by leveraging the efficiencies gained by consolidating the functionality of numerous point products into a single, comprehensive platform that provides the following benefits:

- **Reduced administrative overhead**—Reduces head count and hours associated with managing multiple point solutions
- **Reduced costs**—Reduces the effort associated with managing multiple support contracts, training classes, and renewals for various point products (i.e., less to learn, license and use)
- **Increased Efficiency and Security**—Provides centralized management of these various technologies and secures systems faster with greater ease than supporting a plethora of consoles, infrastructures, and agents.

Hardware Level Security

The ideal endpoint security solution should take advantage of the security features built into the hardware. Some examples include:

- **Trusted Platform Module** (TPM) – An industry standards based microcontroller with cryptographic capabilities for storing encryption keys, passwords and digital certificates which can be used for both system and end user authentication.
- **Intel's vPro** - Provides secure out of band management communication requiring authentication for management. Communication between a management console and vPro enabled clients is encrypted and authentication is performed prior to any action being performed on a client - this provides a secure alternative to less secure and less reliable technologies like WakeOnLan.
- **Hardware based self-encrypting drives** – Hard drives with special firmware which encrypts and decrypts every bit of data as it is either written or read from the platters with minimal impact on performance (<1%). Hardware level encryption is more transparent to the user and independent of the operating system.

Dell and Symantec offer flexible solutions to their customers to manage the total cost of ownership and leverage the integrated security features within the Dell Latitude, OptiPlex and Precision systems. Below you will find some of the solutions offered by both Dell and Symantec, please contact your Dell account team for additional information.

Solution: Dell Client Manager

A well managed endpoint is a secure endpoint. The ideal security solution should include not only software solutions but should take advantage of the security features built into the hardware. Dell Client Manager provides administrators control over the security features built into Dell hardware via a centralized management server accessible via a web-based console with role and scope security. While some may only use Dell Client Manager to remotely upgrade the BIOS on their Dell Systems – The Dell Client Manager console also provides a wealth of security related functions to better secure your systems. Using Dell Client Manager, administrators can:

- Remotely configure BIOS settings including setting a BIOS admin password
- Enable and activate the Trusted Platform Module (TPM).
- Provision ASF, Intel vPro, or DASH capable systems for secure out-of-band management communication.
- Monitor a system's status for changes ranging from chassis intrusion to unauthorized changes in disk, memory or processor counts.
- Monitor if a system has not "checked-in" with the console for a user-defined amount of time.

For any of the above items, administrators can be notified through the console or via email, or the system can be configured to launch a custom, predefined action.

Dell Client Manager is an essential element to not only better manage your Dell business clients, but to better secure them by leveraging the security technology built into the hardware (which most Dell customers pay for but do not effectively use).

Solution: Symantec Endpoint Protection

As previously stated, reduced total cost of ownership can be achieved by consolidating the functionality of numerous point products into a single, comprehensive solution. Symantec Endpoint Protection does exactly that, by incorporating the following technologies into one single agent managed my one single console:

- Antivirus & Antispyware
- Firewall
- Intrusion Prevention (IPS)
- Device Control
- Network Access Control

Through this single Endpoint Protection agent, administrators receive higher levels of real-time protection which outperforms many long-time security solution providers. In an October 2008 comparison, Symantec Endpoint Protection consistently delivered faster scans, boot times, and application & file open times than the competition – twice as fast in some cases.[1]

Antivirus & Antispyware

Symantec Endpoint Protection provides automated malware protection through the antivirus & antispyware component of the agent. This component automatically blocks spyware installation, detects and remediates any existing spyware, and protects from any potential viruses. Behavior blocking and tamper protection techniques are used to help prevent client systems from being used for malicious outbound activities and guarded from unauthorized access. Furthermore, virus definitions are distributed incrementally which reduces network bandwidth while ensuring your systems are consistently up to date.

The accuracy of Symantec Antivirus is unparalleled. Symantec Antivirus has been the only product to pass Virus Bulletin's VB100 last 41 tests (Dating back to Nov 1999)[2]. The VB100 is an in-depth comparison test of the detection rates of anti-virus software.

Firewall

The Symantec Endpoint Protection firewall provides a barrier between the computer and the Internet. The firewall prevents unauthorized users from accessing the computers and the networks that connect to the Internet. It detects possible hacker attacks, protects personal information, and eliminates unwanted sources of network traffic.

[1] http://www.tolly.com/DocDetail.aspx?DocNumber=208349WC

[2] http://www.virusbtn.com

Intrusion prevention

The intrusion prevention system (IPS) is the Symantec Endpoint Protection client's second layer of defense after the firewall. The intrusion prevention system is a network-based system. If a known attack is detected, one or more intrusion prevention technologies can automatically block the intrusion. Symantec Endpoint Protection includes TruScan™ proactive threat scan technology which automatically analyzes network communications and application behaviors, detecting and actively blocking threats. When operating system or application vendors announce new vulnerabilities that can potentially place organizations at great risk, the characteristics of that vulnerability is used to create a generic signature. This helps protect organizations before exploits begin to surface. Using this method a single vulnerability definition is not only protecting against one type of threat, but perhaps hundreds or thousands - since it looks for vulnerability characteristics and behavior, it can protect against a wide range of threats, even those that are not yet known or developed.

Device Control

Device Control is another feature of Symantec Endpoint protection with the ability to protect from attacks and data leakage that occurs through the use (or abuse) of I/O devices such as USB memory keys, media players, etc.

One example of an attack using this method was “W32.SillyFDC” which used a USB key as the means to deposit a Trojan horse onto a system. With Endpoint Protection, administrators can determine which of these devices have write access to the system, and even what data can be written to the I/O device. This is done through the Device Class ID, which offers many possibilities on how to create different policies based on device type.

Network Access Control

In addition, Symantec Endpoint Protection is network access control ready. The agent can be enabled to provide network access control capabilities that allow organizations to ensure endpoints comply with corporate security policy before gaining access to the network. Symantec Endpoint Protection eliminates the need to deploy additional network access control software on an organization’s endpoint devices.

Solution: Symantec Endpoint Encryption

While self-encrypted hard drives provide the most effective security, a few obstacles must be overcome to reap the benefits including cost, management and logistics. Most organization will take a phased approach in moving to hardware based Full Disk Encrypted drives. During this transition, software based encryption should be utilized to ensure the security of your data. Symantec Endpoint Encryption protects and prevents your information from accidental data loss and assures protection for desktops and laptops against unauthorized access.

Solution: Altiris Client Management Suite

As previously stated, a key factor in determining a cost-effective endpoint security strategy is the understanding that a truly secure endpoint is a well-managed endpoint. According to industry analysts, more than 90 percent of all system vulnerabilities can be eliminated through proper system configuration and patch management. The convergence of security and systems management offers unique and compelling advantages for system administrators increasingly charged to do more with less. Added visibility into and control of an entire endpoint environment can help eliminate exposure to security and compliance risks to ensure confidence in a stable and efficient endpoint operating environment.

Summary

In conclusion, Dell and Symantec have partnered to deliver a common platform for securing and managing Dell Business Client systems. This solution includes:

- The latest OptiPlex, Latitude and Precision systems from Dell
- Managing them with either Dell Client Manager or Altiris Client Management, and
- Securing them with Symantec Endpoint Protection (and optionally Symantec Endpoint Encryption)

These solutions are integrated via the Symantec Management Platform to provide an unprecedented level of endpoint security and systems management, and provide efficient tools for reducing the total cost of ownership and improving the usability of the DELL platforms.

Where to get more information

Symantec security research centers around the world provide unparalleled analysis of and protection from malware, security risks, vulnerabilities, and spam. Please visit Symantec Security Response: http://www.symantec.com/business/security_response/index.jsp for more information.

Appendix A: Security Area | Product Matrix

		Dell Client Manager Standard	Symantec Endpoint Encryption	Symantec Endpoint Protection	Altiris Client Management Suite
Hardware Level Security	TPM Enablement & Activation	X			
	BIOS Password Mgmt & Configuration Device Lockdown	X			X
	vPro Provisioning for Secure OOB Management				X
Data Security	Hardware (Full Disk)	Seagate FDE Drives Available from Dell			
	Software (Full Disk)		X		
Network Security	Personal firewall			X	
	Network access control (NAC)			X	
Endpoint Protection	Antivirus			X	
	Antispyware			X	
	Proactive threat protection			X	
OS & Application Security	OS Patch Management				X
	Application Patch Management				X
	Application control				X

About Dell

Dell Inc., is the leading technology provider to commercial enterprises around the world.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com