Advanced Threat Prevention Benefits

- Unparalleled efficacy, stops 99% of malware before it can even run, far above the average 50% efficacy rating of the top anti-virus solutions[1]
- Preventing malware significantly reduces remediation costs and end user down time associated with wiping the drive, reimaging the hard disk and reinstall the operating system and application software
- Low CPU and memory usage enhances system performance to give you back the computer you thought you bought
- Local detection with no need for a constant cloud connection ensures mobile end users can work where and how they want without fear of compromise
- Prevention based on AI and Mathematical models with minimal false positives increases IT productivity by eliminating the need for constant signature updates
- Satisfies PCI DSS, HIPAA HITECH and Microsoft requirements for an anti-virus replacement to reduce your overall data protection cost

[1]Results from Cylance Unbelievable Demo Tour, Austin, Houston and Dallas Texas, May 2015

Dell Data Protection | Endpoint Security Suite Enterprise

Endpoint security and compliance are critical to every organization, no matter the size. Organizations must secure endpoint devices and the data on them, while still satisfying end user requirements to embrace computing trends like bring-your-own-device (BYOD), sharing data in public cloud services and workforce mobility. Traditional data security point solutions attempt to address these needs, but managing multiple clients and consoles is difficult for resource constrained IT teams, especially those without security experts in house. Most endpoint protection solutions are difficult to deploy and manage, lack coverage for all the places employees put and use data, and reduce system performance and end user productivity. Dell's data security suite offers a number of advantages, including:

- Sales and support for your hardware and security solutions from one source
- Protection for heterogeneous environments with full support for Dell and non-Dell hardware
- Automatic deployment and provisioning when factory-installed on Dell commercial devices
- Single integrated client simplifies deployment and updates and ensures all elements of your data security solution work seamlessly together
- Easy compliance and auditing with pre-defined compliance reports and an intuitive management console that quickly guides you to any issues that need to be addressed

Endpoint Security Suite Enterprise offers strong data security for business data, systems, and reputations. The suite offers an integrated client that includes advanced threat prevention, encryption and authentication, all centrally-managed via a single console to help businesses reduce IT management costs and complexity. With consolidated compliance reporting and console threat alerts, businesses can easily enforce and prove compliance for all of their endpoints. Built in security with features like simplified policy configuration with smart defaults and pre-defined report templates is especially helpful as organizations struggle to protect end users and data.

Advanced Threat Prevention

The constantly evolving threat landscape requires a level of security that far exceeds the effectiveness of current solutions deployed throughout enterprises, government and institutions worldwide. Traditional, behavior - or signature-based anti-virus and anti-malware solutions are reactive by design since they depend on previously seen behavior or patterns to identify an attack. Because of this reactive design they are increasingly ineffective against Zero-Day threats, advanced persistent threats and targeted attacks like Spear Phishing and Ransomware.

Endpoint Security Suite Enterprise solves this problem by integrating revolutionary advanced threat prevention with unparalleled efficacy against zero-day threats, advanced persistent threats and commodity malware. This solution uses unique artificial intelligence (AI) and dynamic mathematical models to analyze files prior to their execution and determine which are safe and which aren't, thus stopping malware before it can even run. Based on tens of thousands of markers extracted from careful analyses of hundreds of thousands of real-world exploits and known good files, the Dell approach does not rely on signatures that look for known behaviors or patterns and that must be updated as threats evolve. This allows us to prevent threats without the need for a constant cloud connection or frequent updates, because the intelligence is built into the endpoint. Dell rounds out this advanced threat prevention by checking Dell commercial system BIOS on boot, to quickly alert administrators of any possible BIOS tampering.

Encryption

Dell Data Protection | Enterprise Edition encryption provides a data-centric, policy-based approach to encryption that protects your data without disrupting IT processes or end user productivity. Designed for easy deployment, end-user transparency, and hassle-free compliance, Enterprise Edition delivers a high level of protection, fills critical security gaps and allows you to manage encryption policies for multiple endpoints and operating systems - all from a single management console.

Enterprise Edition offers software - and hardware-based encryption, management of Microsoft® BitLocker, and protection of data on external media, self-encrypting drives, mobile devices and data in public cloud services. It allows the administrator to easily enforce encryption policies wherever the data resides without end user intervention. A perfect solution for even the most complex environments, Enterprise Edition offers many benefits including:

- Detailed, enterprise-wide encryption status reporting to avoid costly fines and damaged reputations if a device is lost or stolen
- No special disk preparation or defragmenting required before encryption
- System disk and external media encryption in a single solution
- Integration with existing processes for authentication, automated patch management and more
- FIPS 140-2 Level 2 validated software encryption
- Encryption of all data, except files essential to booting the operating system or full disk encryption, depending on your preference
- Enhanced port control system to prevent data leakage

Advanced Authentication

Dell Data Protection | Security Tools supports advanced hardware authentication, such as Dell's fully-integrated fingerprint, smart card or contactless smart card reader options. Security Tools helps manage these multiple hardware authentication methods, supports pre-OS login with self-encrypting drives, single sign-on (SSO) and manages user credentials and passwords. The ability to reset a Windows password via an authorized smartphone is just one example of how Security Tools helps enable end users while minimizing help desk calls.

Dell ControlVault, available on select Dell systems, offers secure hardware storage for all user credentials — such as user passwords, smart card data or fingerprint data — used during Microsoft Windows pre-boot. Dell ControlVault fully isolates a user's credentials from potentially unsecured operating systems and hard drives. The cryptographic secrets which protect the user data, when stored on the PC, are kept in a secure cryptographic co-processor hardware device and are processed inside that device instead of in main memory where malicious programs can spy on the process. This option helps ensure the ultimate protection, even against sophisticated hackers attempting to gain access to critical systems.

Technical Specifications

Endpoint Security Suite Enterprise is available for mixed vendor environments that meet the below specifications.

Supported Client Operating Systems:

- Microsoft Windows 7 Ultimate, Enterprise and Professional Editions
- Microsoft Windows 8 and 8.1 Enterprise and Professional Editions
- Microsoft Windows 10 Education, Enterprise and Pro Editions

Dell Data Protection | Virtual Edition Server may be imported into one of the following virtualized environments:

- VMware ESXi 5.1, 5.5 and 6.0
- VMware Workstation 9, 10 and 11

Dell Data Protection | Enterprise Edition Server has been validated in the following operating environments

- Windows Server 2008 R2 SP0-SP1 64-bit Standard and Enterprise Editions
- Windows Server 2008 SP2 64-bit Standard and Enterprise Editions
- Windows Server 2012 R2 Standard Edition
- VMware ESXi 5.1, 5.5 and 6.0
- VMware Workstation 9, 10 and 11

Remote management console and Compliance Reporter access are supported via the following Internet Browsers:

- Internet Explorer 11.x or later
- Mozilla Firefox 41.x or later
- Google Chrome 46.x or later