

Ultimate VDI protection

End-to-end, from the edge all the way to the datacenter.



Pain points

Maintaining security of data and applications as well as compliance is one of the top three IT concerns in organizations of all sizes. Mobile office trends and BYOD initiatives means that more devices and sensitive data are out of direct IT control, increasing the risk for data theft, virus, malware and ransomware attacks. In addition, traditional antivirus (AV) solutions can't keep up with the number of new malware created daily. Non-security IT specialists find security and compliance complex. Moving from an environment based on physical PCs with locally installed OS, applications and data to a virtual desktop environment (VDI) – where data and apps are now located on a centrally secured server – is a great way to significantly reduce these risks. However, virtual desktops and most endpoints can still be targeted by cyber attacks, therefore they also need adequate protection.

Dell offers a comprehensive set of security from the datacenter – even inside the VMs – all the way to the endpoint, being a physical PC running Windows, a Mac OS X system, or a thin client running Windows Embedded.

Protection for virtual and physical desktops

Dell Data Protection | Endpoint Security Suite Enterprise offers complete, integrated endpoint security suite which can be installed on both traditional, physical PCs (Dell and non-Dell), as well as on persistent virtual desktops running in a Citrix or VMware environment.

The suite includes:

-  **Advanced Threat Protection:** a revolutionary, **preventive** approach providing proactive protection by catching 99% of advanced threats, commodity malware and ransomware before they can execute. It uses dynamic mathematical models and artificial intelligence and is able to catch even zero-day attacks. The client runs locally on the Windows physical or virtual desktop with very low CPU and memory usage, thus there is no impact on end user productivity and no need for constant internet connectivity or signature updates created by humans.
-  **Encryption:** Data-centric encryption protects sensitive data via set-and-forget policies to simplify protection for any sized organization. Dell provides maximum data security by encrypting local drives and removable media. On physical PCs only, it is FIPS 140-2 Level 2 validated and also offers Microsoft BitLocker and self-encrypted drive management.
-  **Authentication²:** on physical PCs only, the suite enables advanced hardware authentication, such as Dell's fingerprint, smart card or contactless smart card readers. It also supports pre-boot authentication for self-encrypting drives, single sign-on (SSO) and offers additional security for user credentials via Dell ControlVault™. It is also possible to reset a Windows password via an authorized smartphone, minimizing one of the most common reasons for help desk calls.
-  **Centrally managed console:** Endpoint Security Suite Enterprise offers a single pane of glass view into all your protected endpoints with a web-based, on-premise management console. Detailed compliance reporting is included to greatly simplify security management and compliance.

Protection for thin clients

As the thin client world leader, Dell proposes Wyse zero and thin clients running Wyse ThinOS, Windows Embedded or Linux.

-  **Dell Wyse zero clients and ThinOS based thin clients:** because they run a proprietary OS and have an unpublished API, they offer natively maximum security and are malware and virus resistant, offering zero attack surface. They can thus be used out of the box offering immediate, total security and do not need any threat protection solution.
- Dell Wyse Windows Embedded thin clients:** thin clients running Windows Embedded Standard (WES) 777p or Windows 10 IoT Enterprise can offer the increased flexibility to use a local browser, to install external peripherals with their associated drivers, as well as small applications running locally. As such, Windows-based thin clients must be security patched regularly, as they still run the risk to be potentially infected by a malicious website or file coming from a USB stick.

To proactively protect Windows-based thin clients against today's advanced threats and commodity malware, Dell offers advanced threat prevention, with  **Dell Data Protection | Threat Defense.** This solution also protects traditional physical PCs, as well as servers running Microsoft Windows Server in the datacenter for the VDI infrastructure. It protects against cyber threats and commodity malware, but does not include encryption and authentication. Threat Defense includes cloud-based management to simplify setup and management, even for organizations that may not have security expertise or dedicated IT staff in-house.



Ultimate VDI protection

End-to-end, from the edge all the way to the datacenter.

The problems with traditional AV solutions

With the rapidly increasing number of cyber attacks, traditional AV solutions can't keep up, with top AV vendors stopping an average of only 50% of threats. These traditional, **signature-based** solutions depend on previously seen behaviors and patterns, which makes them ineffective against zero-day threats. When a new threat is seen there is a gap in protection while the AV vendor deconstructs the malware, creates a signature to identify it, gets that new signature into the product (all of this often needing a human intervention) and distributes it to all the end users. Many targeted attacks change known malware just enough to evade signatures thus creating another protection gap and explaining why traditional AV requires frequent updates. AV scans are necessary since AV misses so many attacks, but scans are very resource intensive on CPU and RAM, which negatively impacts system performance and lowers end user productivity.

These solutions are based on **'reactive detection followed by remediation'** approach, also known as 'clean and quarantine'. This is a potentially expensive value proposition given the fact that only about 50% of threats are stopped and many infected systems must be reimaged.

What is Dell Advanced Threat Protection?

Dell's revolutionary advanced threat protection/ prevention is based on dynamic mathematical modeling and artificial intelligence (AI) to **detect even unknown malware before it can run**, thus greatly reducing the impact. The algorithm was trained by analyzing tens of thousands of file attributes for millions of known, real-world good and bad files. Because of the magnitude of data involved, humans are incapable of leveraging this data to make a determination as to whether a file is malicious or not – but an AI system is. Any new file is assessed and immediately classified as 'good/suspicious/bad'. If identified as malware the file is not allowed to run. Because the Dell solution looks at so many attributes vs the limited number a human can assess via signatures, we are able to prevent 99% of known and unknown threats, including zero-day attacks¹. This model does not depend on signatures or known patterns to recognize a threat and it does not depend on human intervention or frequent signature updates. The agent, installed on the endpoint or VM, uses only 1-3% CPU and ~40MB RAM, thus having no impact on system performance or end user productivity. This model is robust, doesn't need frequent updates nor a constant internet connection. Microsoft recognizes this solution as AV and Endpoint Security Suite Enterprise satisfies PCI DSS and HIPAA HITECH compliance requirements as an AV replacement.

Dell's revolutionary **'prevention and proactive protection'** approach operates in real-time and saves significant time and money needed to remediate infected systems. Ransomware or malware that steals data is even worse since there is no remediation once the damage is done. Dell puts the intelligence where it's most needed: right at the endpoint and in the virtual desktop.



Customer Benefits

Peace of mind:

- Prevents 99% of malware, far above the average 50% of threats identified by the top anti-virus solutions¹
- Comprehensive data encryption
- Advanced authentication²
- Simplicity when buying from a single vendor

Meet compliance:

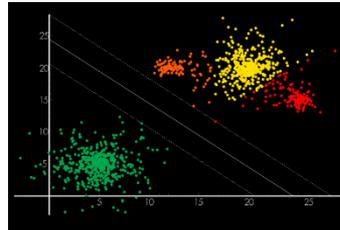
- Compliance reporting with pre-defined report templates included
- Satisfies Microsoft requirements for a traditional anti-virus replacement
- Satisfies PCI DSS & HIPAA HITECH compliance, FIPS 140-2 Level 2 validated, & IPv6 capable

Improved productivity:

- Transparent to end users, low CPU & RAM impact
- Centrally managed console
- Prevent malware before it can run
- No frequent signature updates needed
- No constant internet connection required
- Minimizes the time IT spends remediating infected systems

Issues when using traditional AV solutions:

- 95% of successful cyberattacks start with an endpoint exploit
- 77% of organizations have been infected with undetected web-borne malware
- 205 days is the median time to detect an intrusion
- \$325M in recorded ransomware payments in the US in 2015, requiring 3-5 days for recovery
- In 60% of cases studied in recent attacks, it took only one minute to compromise the victim



Dell's advanced threat prevention evaluates millions of factors to identify and stop malware before it can run.

¹ Results from Cylance Unbelievable Demo Tour, Austin, Dallas and Houston, Texas, May 2015. Also based on Dell internal testing, November 2016.

² Supported only on physical PCs; not supported on VMs.



Visit our website at:
Dell.com/wyse/shield
Dell.com/DataSecurity

Visit our website at:
Dell.com/wyse/shield
Dell.com/DataSecurity

Contact us:
 Sales in North America: 1-800-438-9973
 E-mail: CCC_sales@dell.com