Dell Data Protection - Threat Defense

Ultimate malware prevention for WES thin clients, that doesn't impact resources.

Key Benefits

- Proactively stops 99% of executable malware including advanced threats and commodity malware[1], far above the 50% of threats identified by top anti-virus solutions, on WES-based thin clients
- Prevent malware before it can run
- Provides compliance auditing and reporting
- Does not affect end user productivity: very low CPU & RAM impact
- No frequent signature update needed
- Also works on traditional PCs

Moving from an infrastructure exclusively based on traditional, physical laptop and desktop PCs – where data, applications and OS reside on the endpoint – to a virtual desktop infrastructure (VDI) using virtual desktops – where data and applications are more securely locked in a datacenter – greatly improves security.
In order to access these data and applications, you can use a variety of endpoints, including thin clients. Thin clients offer the advantages that data does not need to be stored on them, they consume very low power and they have up to 7 years lifecycle.
Many thin clients run Microsoft Windows Embedded Standard (WES) Operating System. Using WES, they 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, WES-based thin clients must be security patched regularly (like any other endpoint running a Windows OS), as they still run the risk to be potentially infected by a malicious website or an infected file coming from a USB stick.

Thin client protection

Microsoft releases **security patches** for WES each month. Dell packages these security patches so that they can be easily deployed through Wyse Device Manager (WDM) to its Wyse thin clients. Dell strongly recommends that all security patches be installed as soon as they become available so that all thin clients are "up-to-date" with these patches.

Dell also strongly recommends enabling the built-in **Windows Defender** and **Windows Firewall** settings *before* the thin clients are deployed to end users.

The flash which stores the operating system images within thin clients is protected from accidental "writes" using a **Write Filter** (WF). The WF ensures that a thin client can be restored to a known and desired state when the device is rebooted.
The WF also has an exclusion feature which allows certain files and folders to be "writable". This feature is normally used to store user profiles such as wireless configuration settings and time zone settings. However, incorrect use of the WF exclusion feature exposes files and folders in the flash to virus attacks (and subsequent incorrect or unexpected thin client behavior).
Adding WF exclusions must be carefully considered before the thin clients are deployed to end-users. If having WF exclusions is required for a particular user environment, it is recommended to install antivirus software to protect the flash from virus attacks.

Issues with traditional AV/AM solutions

In addition to the above, it's a good practice to also install an antivirus/ antimalware (AV/AM) solution on a WES-based thin client. In some organizations, it's mandatory to have an AV/AM solution on all endpoints, including thin clients.
The main problem when installing a traditional, signature-based AV solution on a thin client is that it can have a great impact on the end user, as such solutions are CPU and RAM intensive, slowing the system down to a crawl while the virus scan takes place. In addition, such traditional AV can only stop about 50% of threats[1].
Because of these reasons, only a small percentage of customers have actually deployed a traditional AV/AM solution on their thin clients. With Threat Defense, they now have the opportunity to effectively protect also their thin clients without impacting the end user productivity.

A revolutionary AV solution

To proactively protect its Windows Embedded thin clients against such cyber threats, Dell offers Advanced Threat Protection packaged in the **Dell Data Protection | Threat Defense** solution.
This revolutionary, preventive approach provides proactive malware protection by catching 99% of advanced threats, commodity malware and ransomware before they can execute[1]. It uses dynamic mathematical models and artificial intelligence (AI) and is able to **prevent zero-day attacks**.
An agent runs locally on the thin client. Because it uses only 1-3% CPU and has only a ~40MB memory footprint, it has **very little impact on the end user** productivity. Additionally, it requires almost no update as it isn't based on signatures created by humans and requiring frequent updates to keep up with the ever growing threats.
The solution comes with a cloud-based **management console**, allowing IT to maintain policy, compliance and to do reporting.

Feature	Description
Execution Control	Analyzes all **running** processes, including all files that run at system startup, set to auto-run, or manually executed by the user.
Script Control	Protects devices by blocking malicious scripts from running. Supports ActiveScripts and PowerShell
Whitelisting & Blacklisting	Allow or block identified threats (files or applications) for individuals or for the entire organization with the click of a button. Reduces productivity impact and false positives for known good files.
Malware Sample Upload /Download	Allows security admins to: upload a file to the cloud for analysis, or download a malware sample for testing purposes. Enables admins to analyze threat vectors to take better preventive measures.
Cloud-based Management Console	Easy to setup, cloud-based management console for compliance and reporting.
User Group Definition	Endpoints are grouped **in zones** in the management structure.

In addition to WES-based thin clients, Dell also offers Dell Wyse zero clients and ThinOS-based thin clients. Because they run a proprietary OS and have an unpublished API, these Wyse zero clients and ThinOS-based thin clients 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.

Threat Defense can also be used to protect traditional physical PCs (Dell or non-Dell), as well as Microsoft Windows Server systems in the datacenter for the VDI infrastructure.

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[1]. 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.

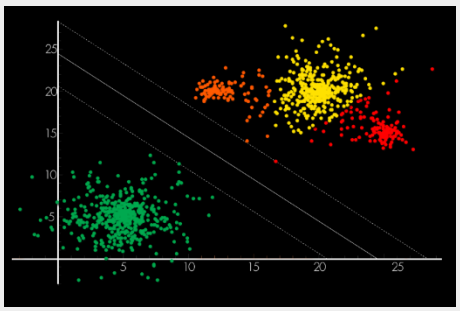
These solutions are based on **'reactive detection followed by remediation'** approach, also known as 'clean and quarantine'. This is a potentially expensive value proposition given the fact that only about 50% of threats are stopped and many infected systems must be reimaged.

What is Dell Advanced Threat Prevention?

Dell's revolutionary advanced threat 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 attacks[1]. 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.

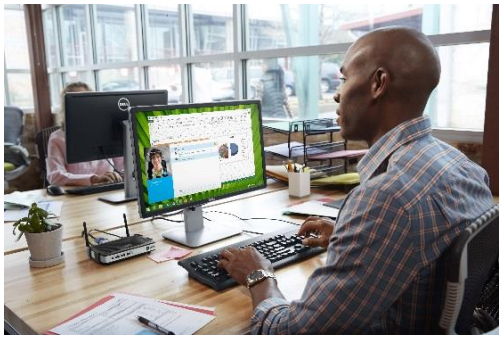
Dell puts the intelligence where it's most needed: right at the endpoint and in the virtual desktop.



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

Weakness of 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 Data Protection - Threat Defense

Technical Specifications

Threat Defense satisfies Microsoft requirements for an anti-virus replacement to reduce overall security cost.

It is available for mixed environments running on the below Operating Systems.

For thin clients:

- Windows Embedded Standard 7/7p
- Windows 10 IoT Enterprise

For physical desktops:

- Microsoft Windows 7, 8.x, 10
- Mac OS X 10.09+

For servers running VDI:

- Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2

Powered by CYLANCE

Learn more at Dell.com/wyse/shield and Dell.com/DataSecurity.

[1] Based on Dell internal testing, November 2016

Dell Cloud client-computing
One Dell Way, Round Rock, TX 78664, USA
Refer to our Web site for regional and international office information