Dell Threat Defense

Ultimate malware prevention for Windows-based thin clients, that doesn’t impact resources.

By Nicolas Cuendet
March 21, 2017

Moving from an infrastructure exclusively based on traditional laptop and desktop PCs (where data, applications and the OS reside on the endpoint) to a virtual desktop infrastructure (where data and applications are more securely locked in a datacenter) greatly improves security. While a variety of endpoints can access data and applications, Wyse thin clients offer several advantages. Data is not stored locally, power consumption is lower, and they are designed with a seven-year lifecycle.

About 40% of deployed thin clients today use the Microsoft Windows Embedded Standard (WES) Operating System. WES-based thin client endpoints can offer the increased flexibility to use a local internet browser, to install external peripherals with associated drivers, and small applications running locally. Such Windows-based thin clients must be security patched regularly (like any other endpoint running a Windows OS), since they still run the risk of being infected by a malicious website or a potentially-compromised USB stick.

Thin client protection

To help safeguard your users against the ever present malware threat, Microsoft releases monthly security patches for WES. Dell packages these security patches so that they can be easily deployed through Wyse Device Manager (WDM) on a gold image for Wyse thin clients. We strongly recommend that all security patches be installed as soon as they become available so that all thin clients are up-to-date.

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

The flash memory which stores the operating system image within a thin client is protected from accidental “writes” using a Write Filter (WF). This ensures that a thin client can be quickly restored to a known and desired state by simply rebooting the device.

The WF also has an exclusion feature which allows certain files and folders to be writeable. 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 can expose files and folders stored in onboard memory to virus attacks (and subsequent incorrect or unexpected thin client behavior).

For that reason, WF exclusions must be carefully considered before thin clients are deployed to end-users. If certain WF exclusions are required for a particular user environment, it is recommended to install antivirus software to protect the flash memory from virus attacks.

Key Benefits

- **Proactively stops 99%** of executable malware including advanced threats and commodity malware, far above the 50% of threats identified by top anti-virus solutions [1]
- **Prevents malware** before it can run
- **Provides compliance** auditing and reporting
- **Does not affect end user productivity** very low CPU & RAM impact
- **No frequent AV signature** update needed
- **No constant internet connection** required
- **Satisfies PCI DSS and HIPAA HITECH compliance** requirements as an AV replacement
- **Also works on traditional PCs, Mac OS and Windows** Server systems

Limitations of traditional AV/AM solutions

Additional best-practices include installing some form of antivirus/antimalware (AV/AM) solution on WES-based thin clients. In some organizations, in order to comply with regulations, it is mandatory to have an AV/AM solution on all endpoints, including thin clients.

A common hurdle raised by traditional, signature-based AV solutions installed on a thin client is the impact such programs can have on the user experience. Because they are CPU and RAM intensive, traditional virus scans can slow system performance significantly. In addition, by some estimates, traditional AV can only stop about 50% of threats. For these reasons, only a small percentage of enterprise IT professionals have actually deployed a traditional AV/AM solution on their thin clients.

With Threat Defense, they now have the opportunity to effectively protect both legacy PCs and thin client endpoints – without greatly impacting user productivity – and maintain the highest level of protection and remediation possible.

A revolutionary AV solution

To proactively protect Windows Embedded thin clients against growing cyber threats, Dell offers Advanced Threat Protection packaged in the Dell Threat Defense solution.

This revolutionary innovation delivers proactive malware protection by catching 99% of advanced threats, commodity malware, and ransomware before it can execute.[1] Threat Defense uses dynamic mathematical models and artificial intelligence (AI) to guard against most executables and is therefore able to prevent zero-day attacks.

An agent runs locally on the thin client but because it uses only 1-3% CPU and has only a ~40MB memory footprint, Threat Defense has very little impact on end user productivity. Additionally, it requires very few updates (about twice a year) as it isn't based on signature files that require constant revision to keep pace with the ever growing threats. The solution comes with a cloud-based management console, allowing your IT team to maintain policies, prove compliance, and streamline reporting.

In addition to WES-based thin clients, Dell also offers Wyse zero clients and ThinOS-based thin clients. With a proprietary OS with an unpublished API, Wyse zero clients and ThinOS-based thin clients offer natively maximum security and are malware and virus-resistant, given their 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 Threat Defense can also be used to protect traditional physical PCs (Dell or non-Dell), Mac OS X computers, or Windows Server environments in the datacenter that make up the back end of a VDI architecture. To protect virtual desktops, we recommend Dell Endpoint Security Suite Enterprise.

Nicolas Cuendet is a Senior Marketing Manager in desktop virtualization solutions in the cloud client-computing division at Dell. Nicolas has extensive product marketing experience in software and infrastructure components for client virtualization.

Weaknesses of traditional AV solutions:

- 95% of successful cyberattacks start with an endpoint exploit[1]
- 77% of organizations have been infected with undetected web-borne malware[2]
- 205 days is the median time to detect an intrusion[3]
- $325M in recorded ransomware payments in the US in 2015, requiring 3-5 days for recovery[4]
- In 60% of cases studied in recent attacks, it took only one minute to compromise the victim[5]

[1] *Verizon 2015 Data Breach Investigations Report*, www.verizonenterprise.com/DBIR/2015/
[2] *Ponemon report:* "The Challenge of Preventing Browser-Borne Malware", Feb 2015
[3] https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf
[4] http://www.lavasoft.com/mylavasoft/company/blog/cryptowall-ransomware-cost-users-325-million-in-2015
[5] *Verizon 2015 Data Breach Investigations Report*, www.verizonenterprise.com/DBIR/2015/

Dell Threat Defense

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 and 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.

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

Appendix

The problems with traditional AV solutions

With the volume of cyber attacks increasing each year, traditional AV solutions can't keep up. As a result, IT professionals and users often operate on a false sense of security when they see that their virus definitions have been updated. This, despite the fact that traditional, signature-based solutions depend on previously identified malicious code, which makes them ineffective against zero-day threats.

Whenever a new threat is identified, there is typically a gap in protection while the AV vendor deconstructs the malware, creates a signature to identify it, incorporates that new signature into the product and distributes it to all the end users. Many targeted attacks alter known malware just enough to evade signatures thus creating another protection gap that results in an endless cat and mouse game of definitions versus slightly altered code.

AV scans are neccessary since AV misses so many attacks. Worse still, these scans are very resource intensive on CPU and RAM, which can negatively impact 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 proposition given the fact that only about 50% of threats are stopped and many infected systems must be re-imaged.

What is Dell Advanced Threat Protection?

Dell's revolutionary advanced threat protection (ATP) is based on dynamic mathematical modeling and artificial intelligence (AI) to detect even unknown malware before it can run, thus greatly reducing its impact. The algorithm was trained by analyzing tens of thousands of file attributes for millions of known, real-world good and bad files. Because ATP does not rely on definition updates to protect your data or determine whether a particular file is malicious or not, it is inherently more effective.

Any new file is assessed and immediately classified as "good/suspicious/bad." If identified as potential malware, the file is not allowed to execute. It bears repeating that our solution is able to prevent 99% of known and unknown threats – including zero day attacks – because it analyzes attributes rather than existing virus definitions. This model does not depend on the legacy approach of having to first identify potential threats nor does it require anti-virus storms or frequent signature updates.

The ATP agent, installed on a thin client, any endpoint or even a VM, uses only 1-3% CPU and ~40MB RAM, thus greatly minimizing the impact on system performance or end user productivity. Additionally, ATP does not require a constant internet connection. Microsoft recognizes this solution as AV. Finally, Dell Threat Defense and Dell Endpoint Security Suite Enterprise satisfy PCI DSS and HIPAA HITECH compliance requirements as an AV replacement.

Dell's revolutionary proactive approach operates in real-time and can mitigate the cost and time needed to remediate infected systems. It also prevents ransomware as well as malware that steals data for which there may be no remedy, once the damage is done. Dell puts the intelligence where it's most needed: right at the endpoint and in the virtual desktop.

1. Based on Dell internal testing, November 2016

Malware now also attacks VDI environments

Meanwhile, reports of file-encrypting "ransomware" increased dramatically in 2016 and are only expected to continue in the year ahead. In the healthcare sector alone, a wave of cyberattacks against U.S. healthcare institutions increased by 63% in 2016 to a total of 93 major attacks.[1]

In one well-publicized example in February 2016, computers at the Hollywood Presbyterian Medical Center in Los Angeles were forced offline for more than a week until hospital officials paid hackers $17,000.[2]

Since then the New Jersey Spine Center, California's Marin Healthcare District, and the Oxford Urgent Care Clinic among others have been severely impacted by ransomware that encrypted electronic medical records, making them inaccessible.[3]

Unfortunately, the problem is not limited to traditional endpoints and servers. Up-to-date anti-virus software is absolutely critical when it comes to protecting virtual desktops, since the latest malware variants can now attack virtual desktop infrastructure architectures and erase persistent user data. Using stolen or default credentials, hackers have been able to log into networks and destroy virtual machines and delete stored snapshots that had ineffective anti-virus protection and not been appropriately backed up.[4]

1. *Infosecurity Magazine*, "Healthcare Breaches Spike 63% In 2016," by Tara Seals, December 22, 2016

2. *Los Angeles Times*, "Hollywood Hospital Pays $17,000 In Bitcoin To Hackers," by Richard Winton, February 18, 2016

3. *Health IT and CIO Review*, "New Jersey Spine Center Pays Ransom to Cyberattackers," Akanksha Jayanthi, October 4, 2016

4. *Digital Trends*, "Shamoon Returns With Malware In Hand to Wipe Hard Drives, Virtual Machines," Kevin Parrish, January 10, 2017

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

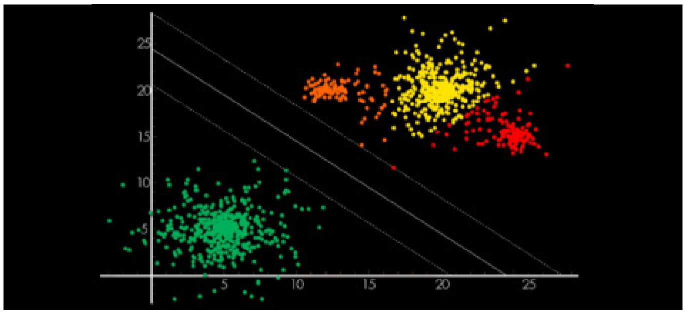
For physical desktops:

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

For servers running VDI:

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

To protect virtual desktops and VMs, use Dell Endpoint Security Suite Enterprise.



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