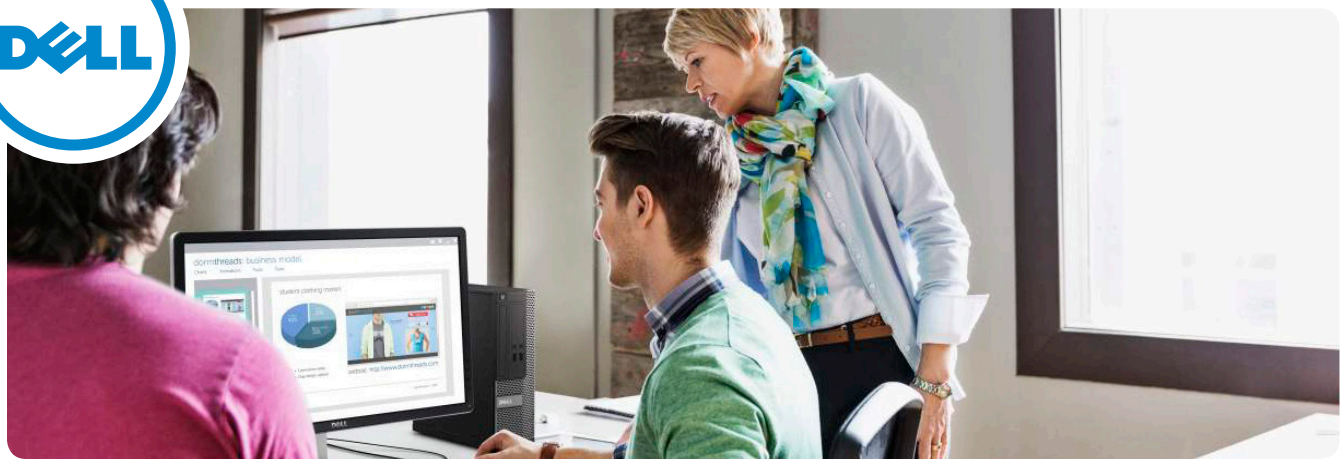

Leading edge, cloud managed threat prevention that stops advanced threats, including zero day malware, from executing

The challenge

Organizations today must deal with the growing complexity and volume of advanced malware. These new malware variants are a growing reality with 74% of small and medium sized businesses having reported a data breach[1]. Most of these businesses are still relying on traditional anti-viruses which focus on detecting and remediating the threats instead of preventing them. The need of the hour is advanced threat prevention to defend against these advanced and persistent threats. Here's why you cannot afford to take any chances:

- 63% of the surveyed organizations have had one or more advanced attacks during the past 12 months[9]
- 2015 witnessed 400k+ ransomware attacks[2]
- 77% of organizations say they very likely have been infected by web-borne malware that was undetected[8]
- 205 days is the median time to detect an intrusion[3]
- $325M in recorded ransomware payments since its discovery in 2015, requiring 3-5 days for recovery[4]
- 71% of data breaches target small businesses[5]

The problems with traditional anti-virus solutions

With the rapidly increasing number of cyber-attacks, traditional anti-virus software can't keep up and can only stop about 50% of threats. They are signature-based and reactive and can only identify behavior or patterns they have seen before. Inherently there is gap between seeing a new exploit and creating a signature to identify it leaving users unprotected. In addition, with over 390,000 new malicious programs registered[6] everyday traditional anti-virus vendors can barely keep up with publishing the antidote to these new malware variants. A recent report found that 99% of malware hashes are seen for only 58 seconds or less[7]. This reflects how quickly hackers are modifying their code to avoid detection. As a result of these a majority of zero-day malware is out of reach for anti-virus solutions. Traditional AV's require frequent updates as well as an internet connection. When they reactively scan a hard drive, they have a heavy impact on system resources such as CPU and RAM, affecting the end user productivity. These solutions are based on 'reactive detection followed by remediation', also known as 'clean and quarantine'. This approach is effective less than 50% of the time, leaving your users and endpoints susceptible to most malware attacks.

In addition to the already existing range of threats, ransomware has emerged as a new threat that has grown to be one of the most dreaded malware types. This is fast shaping up to be a billion dollar business. With threats such as ransomware prevention is the only option. Letting the malware execute and then quarantine is not an option. Once ransomware enters the device the user looses access immediately.

Dell Data Protection | Threat Defense

Dell Data Protection | Threat Defense is a leading edge, advanced threat prevention solution with artificial intelligence and machine learning technology that prevents malware from executing and before it can do any damage. The solution is lightweight and is targeted at businesses that require an effective advanced threat prevention solution. It is easy to setup for businesses that do not have a dedicated IT department. Leveraging algorithmic models and DNA markers, it is easy to deploy, and can be centrally managed via cloud based console, while offering subscription based pricing. This solution stops malicious executables as well as malicious active scripts and PowerShell attacks.

Key Benefits

Prevent damage due to malware:

- Dell Data Protection | Threat Defense stops malware before it can execute. Prevents damage caused by malware instead of a reactive detection method

Requires minimal IT resources:

- For businesses that do not have the IT resources to deal with on-premise setup, the cloud based console lets the business work effectively and focus on revenue generation

High efficacy against advanced threats such as malware, ransomware and zero-day threats:

- With dynamic mathematical models and artificial intelligence prevents 99% of executable malware, far above the average 50% of threats identified by the top anti-virus solutions*

Internet connection not required for detecting malware:

- Constant internet connection not required thereby protects users from malware attacks even when they are offline

Flexible purchase option:

- The flexible subscription pricing is a great way to try Dell security product for organizations that do not want a long term commitment

Compatible with a variety of endpoints:

- A product that is compatible with a wide variety of endpoint such as Windows PC, Mac OS X devices, Windows servers and Windows embedded thin clients supporting mixed environments

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 following Operating Systems.

For devices:

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

For Windows embedded thin clients:

- Windows Embedded Standard 7 (future offering)
- Windows 10 IoT (future offering)

For servers:

- Windows Server 2008 / 2008 R2
- Windows Server 2012 / 2012 R2

*Based on Dell internal testing, June 2016

[1] https://www.gov.uk/government/news/government-urges-business-to-take-action-as-cost-of-cyber-security-breaches-doubles
[2] http://www.lavasoft.com/mylavasoft/company/blog/cryptowall-ransomware-cost-users-325-million-in-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] https://aerissecure.com/blog/smb-data-breach-fallout/
[6] https://www.av-test.org/en/statistics/malware/
[7] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
[8] http://learn.spikes.com/rs/spikessecurity/images/Ponemon-Spikes-Report.pdf
[9] http://www.ponemon.org/blog/new-ponemon-study-on-malware-detection-prevention-released

Learn more at Dell.com/DataProtection

Powered by CYLANCE