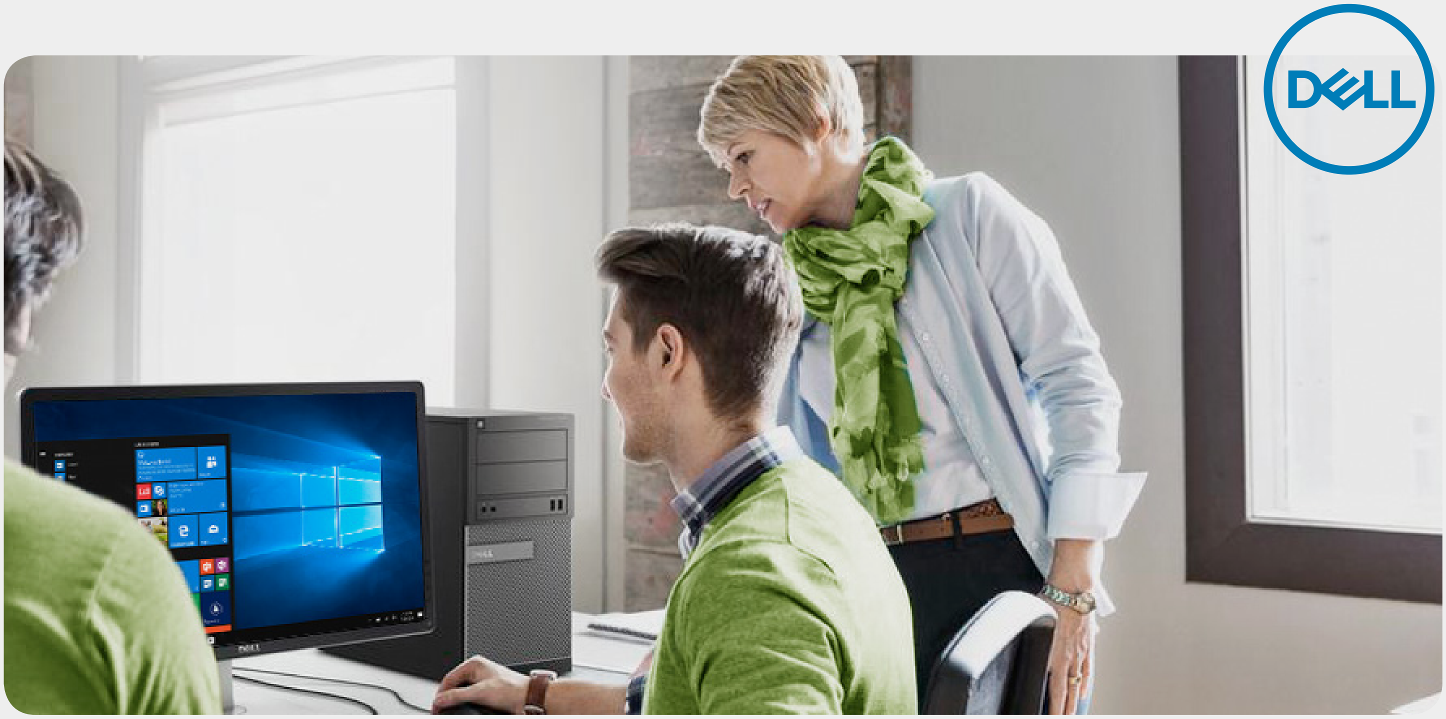
Dell Threat Defense



The Challenge with traditional anti-virus

Most businesses are still relying on traditional signature based anti-virus that can only stop ~50%* of today's sophisticated malware and ransomware. Signature based anti-virus is 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. As a result the majority of zero-day malware is out of reach for these signature based anti-virus solutions. Traditional anti-virus requires 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.

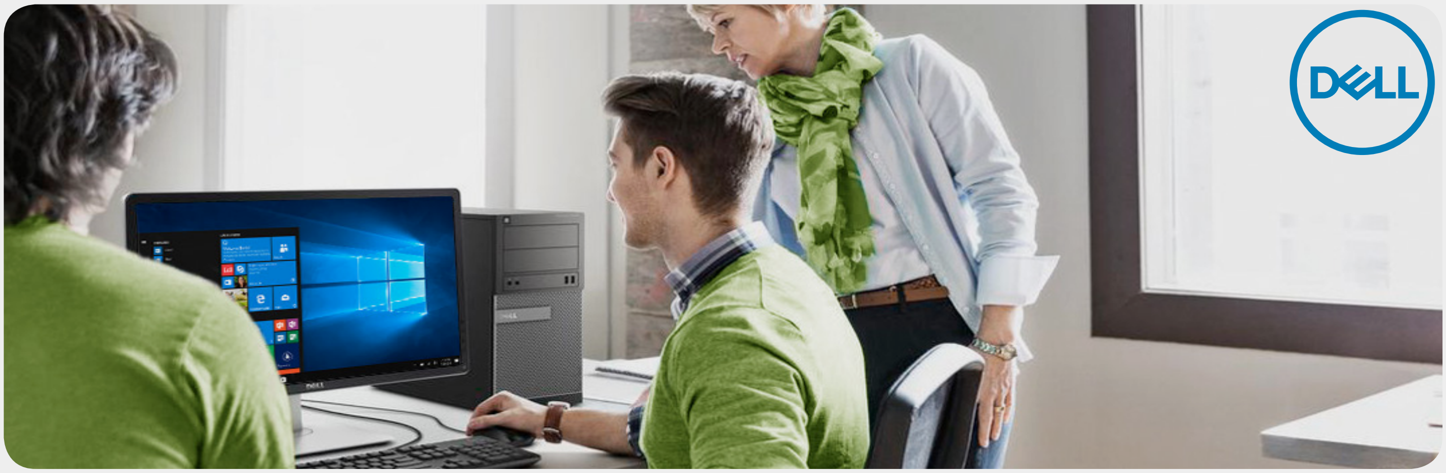
The Solution, Dell Threat Defense

Dell Threat Defense is 99%[2] effective with its leading edge, advanced threat prevention solution with artificial intelligence and machine learning technology that delivers prevention-first. A predictive security product that prevents malware from executing before it can do any damage. Dell Threat Defense provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, zero day attacks, malicious scripts, weaponized docs, and other attack vectors.

The solution is lightweight and is targeted at businesses that require an effective advanced threat prevention solution as an anti-virus replacement. 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 and low IT and system resources.

Learn more at Dell.com/DataSecurity

Powered by CYLANCE



Key Benefits

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

- With artificial intelligence and dynamic mathematical models prevents 99%[2] of commodity malware, far above the average 50%[*] of threats identified by the top anti-virus solutions[*]

Prevent damage due to malware:

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

Requires minimal IT and system 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.
- With Threat Defense the agent runs locally utilizing only 1-4% CPU and ~60MB memory it has very little impact on user productivity. With only a couple updates to the mathematic model in a year, it helps prevent the vast majority of threats without requiring constant updates or internet connection.

Key Features

Execution Control - Analyzes running processes only, including all files that run at system startup, set to auto-run, or manually executed by the user.

Centralized, Cloud-Based Management - Policy, reporting, data management with browser delivered management console, hosted in the cloud.

File Watcher - Scans new and updated files for threats

Background threat detection - Unobtrusively scans files on the system, in the background, for threats. Typically run once when File Watcher is enabled.

Non-Domain support - Support for devices that are not in an Active Directory domain

Client Auto-update - Delivers automated updates to protected endpoints

Script Control - Protects devices by blocking malicious scripts from running. Currently supports Active Scripts and PowerShell.

Certificate based Safe-Listing - Safe-list files via signed certificate, allowing customer software that is properly signed to run without interruption.

Malware Sample Upload/Download – Allows security admins to: 1) Upload a file to the cloud for analysis. 2) Download a file for their own testing purposes.

Security information and event management (SIEM) Support – Export threat events via Syslog to customer provided SIEM products for event correlation and analysis

HIPAA HITECH & PCI DSS compliant - Certified as a compliant anti-virus replacement

Platform Support – Windows clients & servers, Mac OS X and Windows embedded thin clients

Learn more at Dell.com/DataSecurity

Powered by CYLANCE

[*] Based on Dell internal testing, November 2016
[2] NSS Labs Advanced Endpoint Protection Test Report