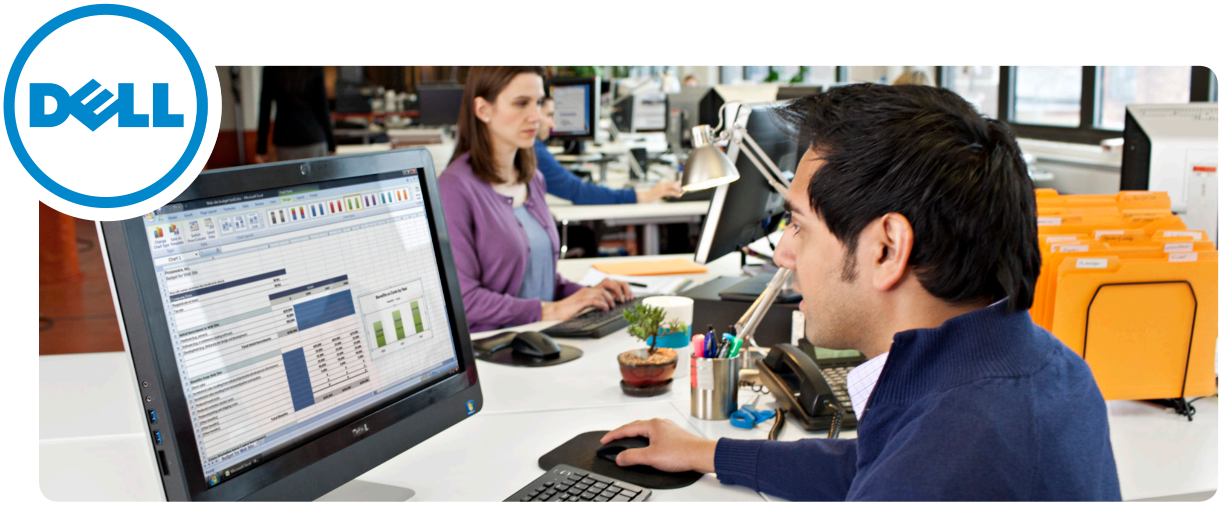

Protect your employees and data from advanced malware attacks in real-time.

Dell Data Protection | Protected Workspace

Organizations of every size now face a daily risk of cyber-attacks, such as spear-phishing, drive-by downloads, poisoned search engine results, and more. These threats put your most critical asset at risk – your data. The easiest way into the network? Your employees. Every time your employees go to the Internet or open an email attachment, they run the risk of becoming the unwitting accomplices to a data breach. New defenses are needed at the endpoint to protect your employees and data from daily attacks.

Dell Data Protection (DDP)| Protected Workspace utilizes a sophisticated new approach to malware prevention to protect your data and users from employee targeted attacks. The software helps protect users against all untrusted content – even Advanced Persistent Threats (APTs) and zero-day exploits – by placing them in a protected environment any time they go to the Internet or encounter untrusted files within email. DDP | Protected Workspace is completely unobtrusive to users so their everyday workflow is uninterrupted.

What's Behind the Technology?

The Invincea™ technology that powers DDP | Protected Workspace was borne out of a DARPA funded project for advanced endpoint protection. It is the brain child of preeminent researchers in the field of malware prevention and has been constructed with an eye toward combating Advanced Persistent Threats. After a yearlong review of the technology, the National Security Agency found it to be effective against all types of malware threats. Combining the power of DDP | Protected Workspace with your anti-virus suite is a proactive approach to protecting your employees from the increasingly aggressive attacks they face on a daily basis.

Benefits

Comprehensive protection
DDP | Protected Workspace is designed to provide the most complete protection possible against malware aimed at the endpoint. It contains the most highly targeted applications in your network in a virtualized environment, thereby preventing all malware from attacking the host operating system. Unlike other solutions, DDP | Protected Workspace does not rely on malware signatures for detection. Instead, it automatically identifies malware attacks based on behaviors inside the contained environment. As a result, DDP | Protected Workspace can detect and thwart zero-day attacks in real-time.

End user productivity
With DDP | Protected Workspace, your employees are given unfettered access to the tools they need to get their jobs done. The software moves highly targeted applications into a new, secure environment in a seamless and transparent way for your employees. There are no new applications to learn – they can still browse with their preferred web browser and can still use Adobe Acrobat PDF reader and Microsoft Office suite – now securely.

Easy activation
A one-year subscription to DDP | Protected Workspace software is included on Dell Precision, Latitude and OptiPlex systems. Once the application is downloaded and activated, it begins moving your users' browsers, PDF readers, Office suite, zip files and executable files into a contained, virtual environment. If DDP | Protected Workspace detects a malware attack, it immediately restores the system to a pristine state, without the need for time-consuming desktop re-imaging. At the end of the first year, simply contact your Dell sales rep to extend your malware protection.

How it Works

DDP | Protected Workspace software uses a unique, three-pronged approach to malware prevention:

- **Containment:** DDP | Protected Workspace places the most highly targeted applications (the web browser, PDF reader, and Microsoft® Office applications) into a secure virtual container to create a malware airlock that prevents infection of the machine. By segregating these applications from the host operating system, DDP | Protected Workspace can reduce the ability of any malicious code to gain access to that host.
- **Detection:** DDP | Protected Workspace does not depend on a library of known malware signatures for detection. Instead, the software looks for the key behavioral indicators of malicious activity, such as changes to the registry, alien processes running, establishment of inbound/outbound connections for command and control, etc. This unique approach enables DDP | Protected Workspace to detect all types of malware – even unknown variants such as Advanced Persistent Threats (APTs) and zero-day exploits.
- **Prevention:** DDP | Protected Workspace kills malware in its tracks and thwarts attacks before they can be successful. The millisecond it identifies an attack, DDP | Protected Workspace begins the process of automatically restoring and remediating back to a clean state.

Available Options

The 12-month subscription to DDP | Protected Workspace that is included on Dell Precision, Latitude and OptiPlex systems is a locally-managed solution. Multiyear subscriptions and volume licensing is available on Dell and non-Dell PCs with options for centralized management and threat data servers via the Invincea Management Server. For more information on these options, contact dellpwsecurity@invincea.com.

Technical Specifications

Operating Systems supported:

- Windows® 7 (32 and 64-bit)
- Windows® 8.1 (32 and 64-bit)

Browsers supported:

- Internet Explorer®: Versions 7, 8, 9, 10, 11
- Firefox™: Versions 15+
- Google Chrome™: Versions 27+

Applications supported:

- Microsoft® Office 2010 and 2013: Word, Excel®, Powerpoint®
- Adobe® Acrobat® Reader : Versions 9, X, XI
- Adobe® Acrobat®: Versions X and XI
- Java™ Add-on: Versions 1.6 and 1.7, all updates
- Flash® Add-on
- QuickTime® Add-on
- Silverlight® Add-on
- Windows Media® Player

Included on select Dell commercial systems (download required):

- Dell Latitude™ laptops
- Dell OptiPlex™ desktops
- Dell Precision™ workstations
- Dell Venue Pro™ Tablets (Windows only)

Learn more at www.Dell.com/DataProtection