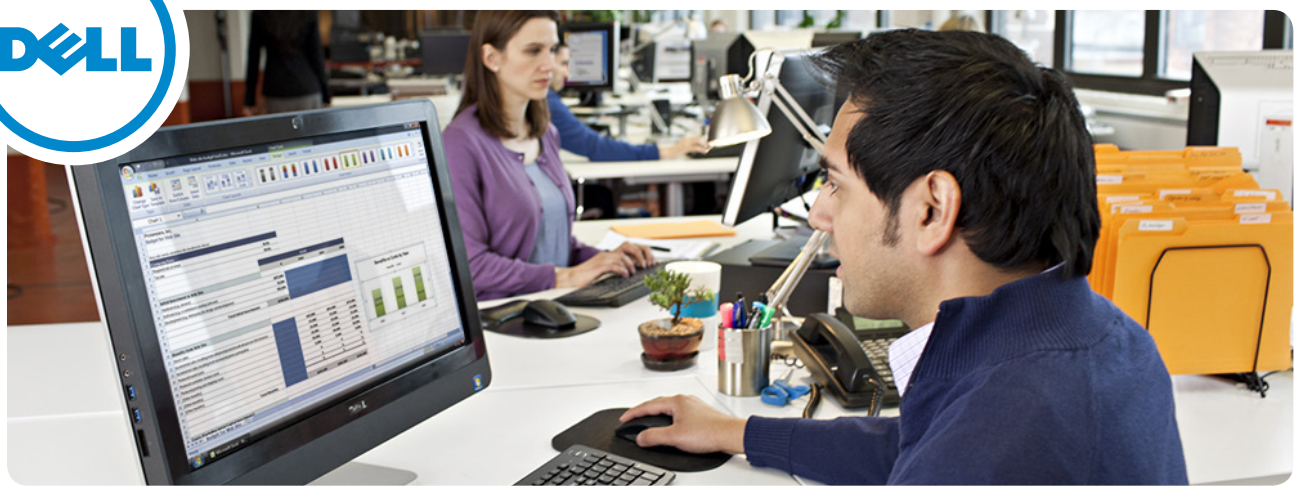

# Protect your employees and data from advanced malware attacks in real-time.

## 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 targeted attacks. The software helps protect users against malicious 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 work in high risk applications. DDP | Protected Workspace is completely unobtrusive to users so their everyday workflow is uninterrupted.

By combining threat prevention via containerization with sensor-based advanced malware detection and risk assessment, your organization is protected from new and existing threats. Sensor technology enables your end user systems to serve as a distributed malware sensor network, identifying existing compromised machines throughout your organization. Suspicious programs and binaries are evaluated via Cynomix technology, with the option to expand risk assessment through additional 3rd party analysis services. Backed by four years of DARPA-funded development, Cynomix is a cloud-based service that determines the similarity of unknown programs to the millions of known malware strains it has mapped. Suspicious programs are analyzed for keylogging, data encryption, FTP usage, packet capture and many other common malware capabilities. The result is an aggregate threat score spanning Cynomix and other available analysis services, indicating the likelihood of the program being malicious. This helps security teams determine whether a device is likely compromised so they can apply corrective controls to eliminate the threat.

## 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 that often slip past traditional anti-virus. After a yearlong review of the technology, the National Security Agency found it to be effective against a wide range 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 prevent zero-day attacks in real-time.

### End user productivity

With DDP | Protected Workspace, your employees can safely access 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 so employees remain productive. There are no new applications to learn – they can still work online with their preferred web browser and they continue using Adobe Acrobat PDF reader and Microsoft Office suite – now securely.

### Easy activation

A one-year, locally managed subscription to DDP | Protected Workspace 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 stops the malware and 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 representative to extend your malware protection or to upgrade to a centrally managed solution at any time.

## 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 that slip past anti-virus solutions.
- **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 included on Dell Precision, Latitude and OptiPlex systems is a locally-managed solution. A centrally managed solution for Dell and non-Dell PCs is available via your Dell account representative.

## Technical Specifications

Operating Systems supported:

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

Browsers supported:

- Internet Explorer®: Versions 7, 8, 9, 10
- Firefox™ Versions 24-current
- Firefox™ ESR 24 & 31
- Google Chrome™ Versions 27-current

Applications supported:

- Microsoft® Office 2010, 2013 & 365 (Word, Excel® & Powerpoint®)
- Adobe® Acrobat® and Adobe Acrobat Reader Versions 9, X & XI
- Java™ Add-on Versions 1.6, 1.7, 1.8 and all updates
- Flash® Add-on - all versions
- QuickTime® Add-on - all versions
- Silverlight® Add-on - all versions
- Windows Media® Player - all versions

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 Dell.com/DataSecurity