
Dell Endpoint Security

Comprehensive, Manageable, Secure

Sean Towns

Systems Engineer EMEA



Dell endpoint security solutions

Only Dell offers a fully integrated portfolio of endpoint security solutions with comprehensive protection that are the Most Secure in the industry!

Most Secure ...

Data Encryption

Protect data no matter where end users take it



Dell Data Protection | Encryption

Advanced Authentication

Ensure only authorized users have access to your data



Dell Data Protection | Security Tools

Malware Prevention

Proactively protect users and data against daily threats not captured by Anti-virus



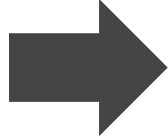
Dell Data Protection | Protected Workspace

Centralized, remote management

Protecting your data has never been more important

A laptop is stolen every

53
seconds



46%
of lost laptops contain confidential data



57%
are not protected with mobile security features



£32,830
€41,040
average value of a lost laptop

>80%
cost is due to data breaches

£3.6M
€4.5M
average organizational cost of a data breach

Data protection = business protection



Compliance
Meeting regulatory requirements



Mitigating Risk
Protecting IP and competitive information



Governance
Ensuring customer and employee trust

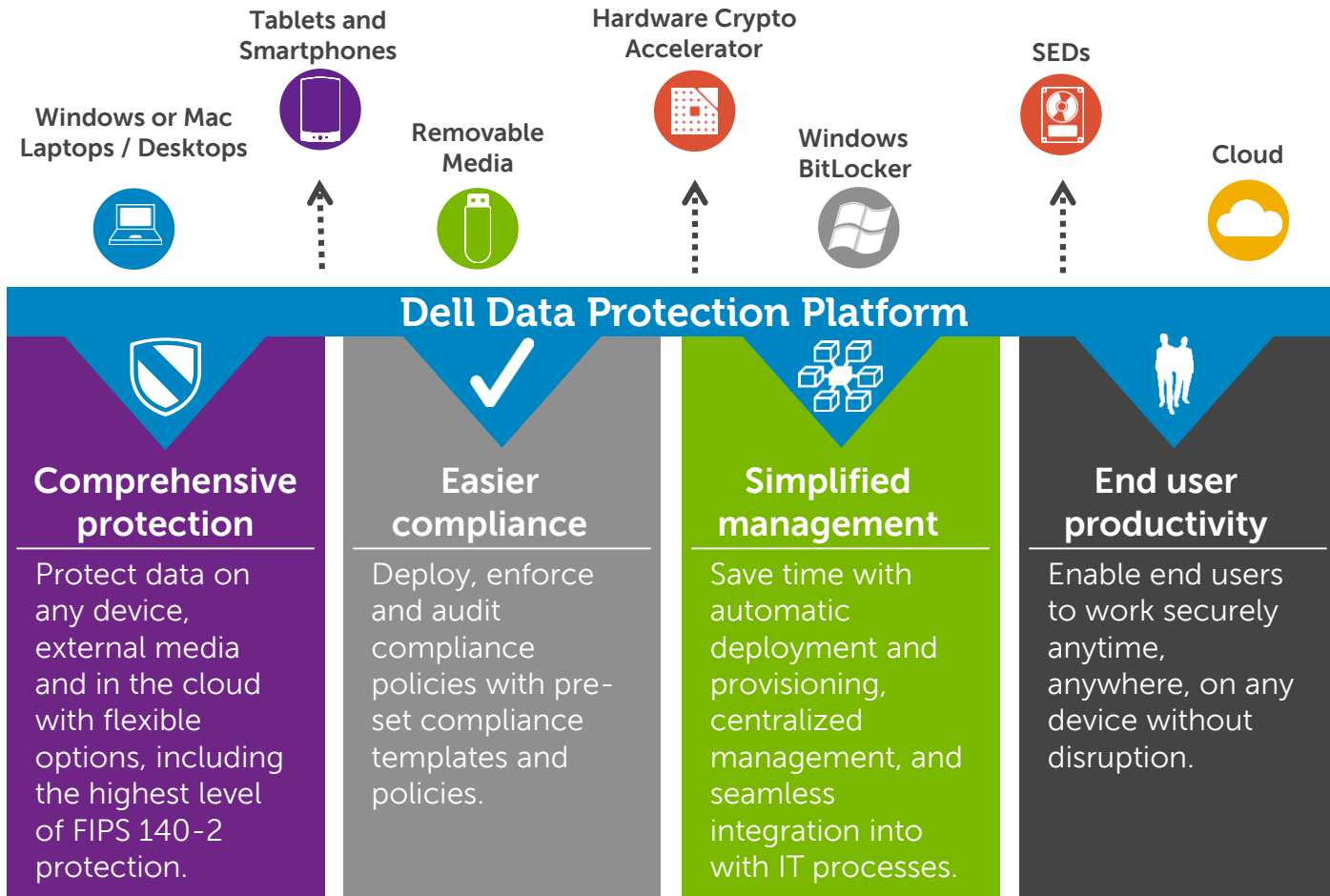
Dell Point of View

Every laptop, desktop, external media device and cloud with intellectual property or sensitive information should be encryption protected



Dell Data Protection | Encryption

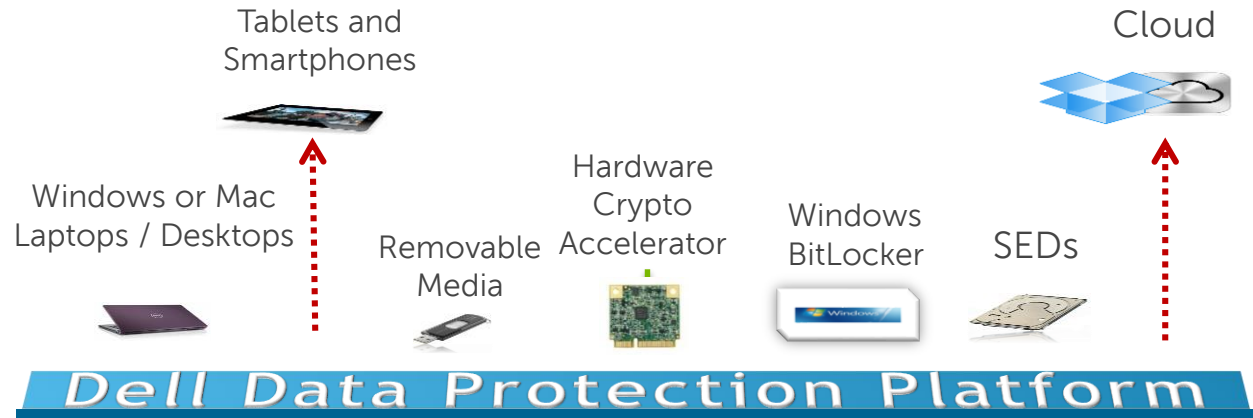
A simple, comprehensive, flexible way to protect data from device to the cloud



Dell Data Protection | Encryption



A simple, comprehensive, flexible way to protect data from device to the cloud



Dell Data Protection | Encryption

Comprehensive lineup of endpoint protection solutions

Enterprise Edition

Centrally managed data-centric encryption software
(Includes External Media Edition)



Personal Edition

Locally managed data-centric encryption software
(Includes External Media Edition)



External Media Edition

Encrypts external media device data; set policies for encryption or disable ports all together



BitLocker Manager

Easily manages Microsoft BitLocker™ for comprehensive protection, auditing and compliance



Self Encrypting Drive (SED) Support

Fully integrated support and centralized management of SEDs ...



Hardware Crypto Accelerator

FIPS 140-2, Level 3 Certified Full Volume Encryption Solution



Mobile Edition

Encrypts mobile devices (Android, iOS) with management capabilities



Cloud Edition

Encrypts end user files in public clouds where user keeps the keys & controls who has access



The multi-key approach to **data-centric** encryption ...

Common encryption

Automatically encrypt data written to any fixed disk

+ User encryption

Automatically enforce encryption of user-specific data

+ External media encryption

Automatic and portable encryption of data moved to external media

+ System data encryption

Optionally encrypt data not already encrypted by other policies (including OS & Program files maintained by IT)

= Granular, policy-based control

Rapid deployment of encryption policies with centralized visibility / control *and* simplified compliance reporting

- Multiple encryption keys for *each* user keeps sensitive data secure, even on multi-user systems like a medical tablet being used on a hospital ward ...
- IT can maintain systems with their existing tools and processes without the ability to view any of the sensitive user data = a *fully compliant & secure* implementation ...

Dell Data Protection | Encryption

Data-Centric Encryption



Making it easy for customers to have the peace of mind that their data is protected

- + **Easy deployment and integration** into your IT environment Supports existing processes for authentication, patching, etc and supports Dell, non-Dell Microsoft Windows and Mac devices
- + **Simplified compliance management and auditing**
One touch-compliance templates, remote management, quick system recovery
- + **Comprehensive protection:** System and attached storage protection in a single solution, covering your external storage security with a single solution
- + **Flexible encryption** – based on end user, data sensitivity and compliance needs
- + **Sales and support from one source**
Purchase and support from one vendor

Dell Data Protection | External Media Edition

Close critical security gaps by protecting external media

Comprehensive protection

- Protect data on any type of USB and removable media, including optical media

More efficient compliance

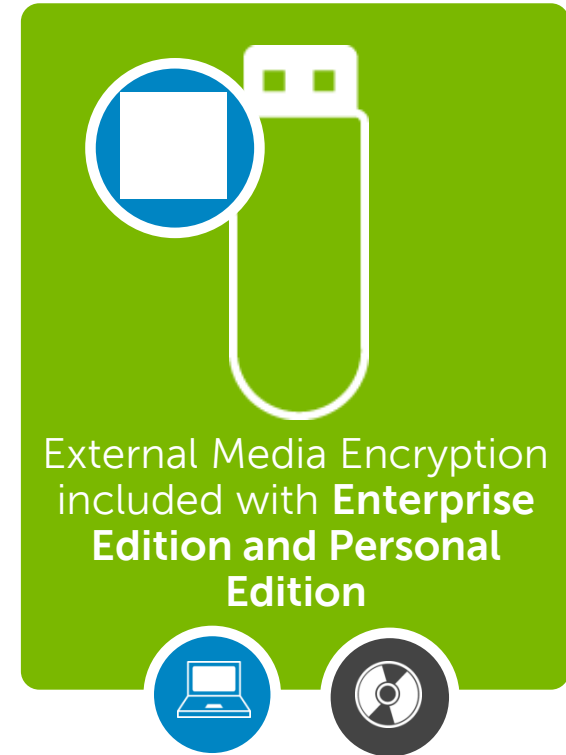
- Set granular policies, automatically update and customize reports
- Gain visibility into external media use across the environment

Simplified management

- No BIOS changes required
- Allows dynamic disablement/enablement of ports to storage without losing function of the port (ex. mice, keyboard, etc.)
- All encryption keys escrowed for ease of recovery

Enhanced end user productivity

- Users log in once, not every time they want to access the drive, including on multiple systems
- No special formatting or “container” and no forced copy, removal or destruction of pre-existing data
- Users can retain unencrypted personal information, such as family photos, while still encrypting new corporate information copied
- Available with password protection to allow data sharing with trusted third parties (consultants, contractors, etc.)



Dell Data Protection | BitLocker Edition

Get the most out of Microsoft BitLocker


Enterprise-level management with centralized reporting and auditing

Centralized escrow of recovery keys/passwords

Full control of all policies without using native AD tools

Improved enforcement of users who are local admins

Automated Initialization and management of the TPM

Use the same console to manage your  Windows 8[®] BitLocker and non-BitLocker systems



Simplified management and comprehensive protection for Microsoft BitLocker

Dell Data Protection | Encryption

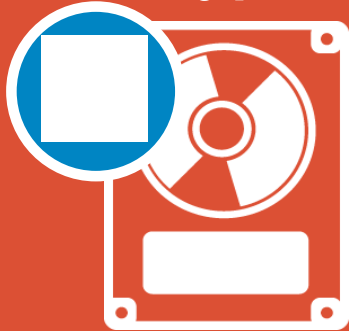
SED Manager

- Simply and securely manage hardware full-disk encryption for your users.
- Automate the administration of devices and user access through the DDP | E console
- Reduce the risk to data and the workload of meeting compliance and audit requirements
- Design objective
 - Manage Opal SEDs with minimal impact to end users and IT operations
- Overview
 - Works with Opal compatible SEDs from all major manufacturers – e.g., Seagate, Hitachi, Toshiba
 - Policy-based management – part of Dell Data Protection Platform
 - Network-aware pre-boot authentication
 - Users authenticate with AD credentials
 - New users can log in without advance configuration
 - Multiple recovery options – both online and offline
 - Remote management
 - Comprehensive reporting for audit and compliance



Dell Data Protection | **Hardware Crypto Accelerator**

Hardware-based full disk encryption



- **Highest level of security commercially available** – Military grade FIPS 140-2 Level 3 security with full volume encryption; Everything including Master Boot Record is encrypted
- **Encryption Accelerator** – Delivers improved system performance by processing encryption activities at speeds similar to self-encrypting drives
- **Tamper resistance** – encryption key is protected by encryption engine and TPM
- **Simple, integrated protection** – Protect data on the drive, plus removable media with port blocking and/or automated encryption of data from ports (optical, USB, 1394, eSata, Express card, etc)
- **Dell Exclusive** technology for Dell Latitude laptops, OptiPlex desktops, Dell Precision workstations

Dell Data Protection | **Mobile Edition**

Secure data accessed on smartphones and tablets

Comprehensive protection

- Protect data on smartphones and tablets running iOS or Android
- Works in tandem with DDP | Cloud Edition

More efficient compliance

- Pre-set templates and consolidated device reporting help you meet and prove compliance
- Immediately execute commands like remote wipe

Simplified management

- Single console to protect data across all endpoints
- Set policies, issue commands, enforce restrictions, and block access on any enrolled device
- Automatically discover new devices

Enhanced end user productivity

- Agentless deployment enables minimal user impact
- Workers can use smartphones and tablets as a standard work tool



Dell Data Protection | Cloud Edition

Enable secure cloud storage, access and sharing

Comprehensive protection

- Protects data as it moves into and out of public cloud storage
- Reinforced by DDP | Mobile Edition

More efficient compliance

- Guards data even from the cloud storage provider
- Central management reduces the compliance workload by giving increased visibility into access, usage and policy enforcement

Simplified management

- Single console to immediately revoke access, remotely enforce policies, monitor and audit
- Granular control over authorized users and endpoints they can use

Enhanced end user productivity

- Provides transparent encryption and decryption as files move into and out of the cloud
- Processes for file sharing, access and storage are unchanged



Simplified deployment and management



Remotely manage all endpoint security needs from a single console: encryption and authentication policies, port control, compliance tracking and reporting, and cloud and mobile device security

Data-centric encryption won't interfere with existing IT maintenance tools, such as patch management

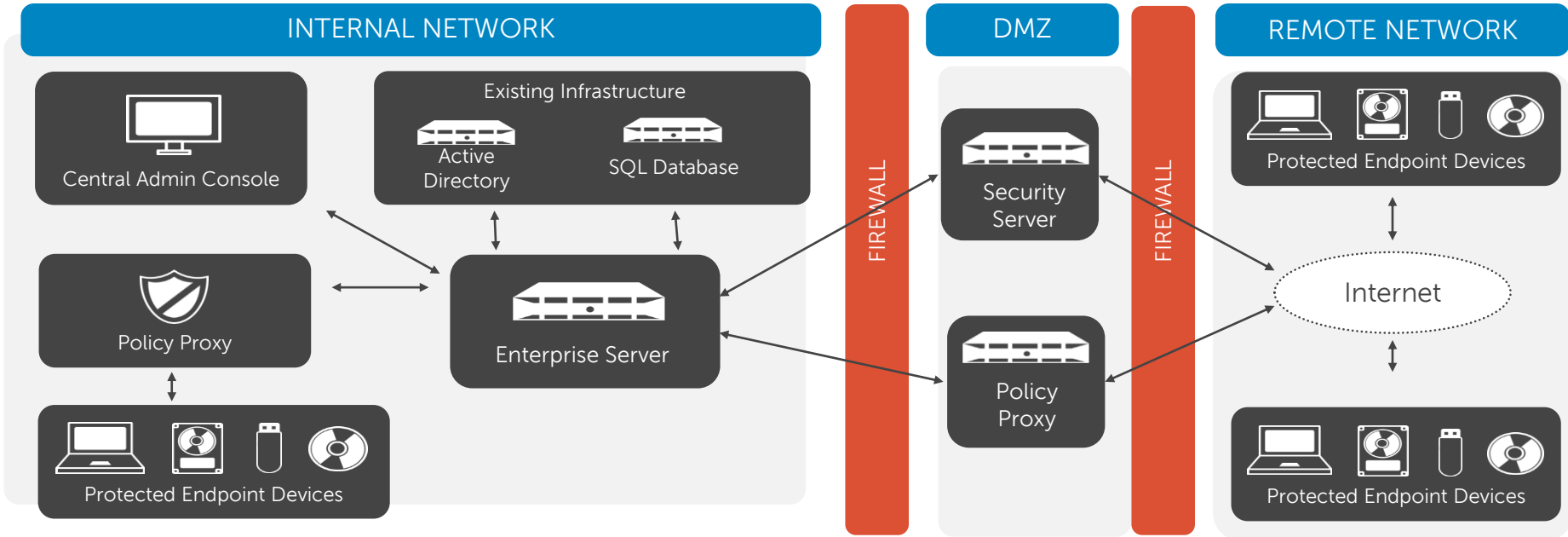
Quick and easy to deploy – Deploy full disk encryption up to 5X faster than traditional encryption solutions, saving >3 hours per PC*

*Principled Technologies Report commissioned by Dell; September 2012 – downloadable from <https://www.principledtechnologies.com/>

Solution and support from the same vendor



DELL Data Protection deployed



+ Leverages existing infrastructure for seamless integration

+ Local policy enforcement ensures data protection travels with the device at all times

+ Device detection and enforced provisioning across all connections

+ Scalable, single point of management and control for all platforms

Dell Data Protection | Security Tools

Comprehensive lineup of authentication options

Dell ControlVault™ Security Processor

- Keeps user passwords and credentials on a separately controlled hardware chip for secure authentication
- Isolates fingerprint processing and storage from OS and physical hard drives for ultimate protection against potential compromise



Smartcard Controller

Contact or contactless SC support, HID iClass or FIPS 201 PIV cards

Simplified Authentication Management

- Configurable policy for users and admins
- Self-recovery questions eliminate help-desk calls
- Attended and un-attended User enrollment
- Local management, remote management with DDP|E

One step Logon

Simple, secure access with pre-boot/ pre-Windows authentication all the way through Active Directory log on. Password manager

Fingerprint Processing

Processes and stores fingerprint credentials on FIPS 201 compliant memory chip

Dell Protected Workspace

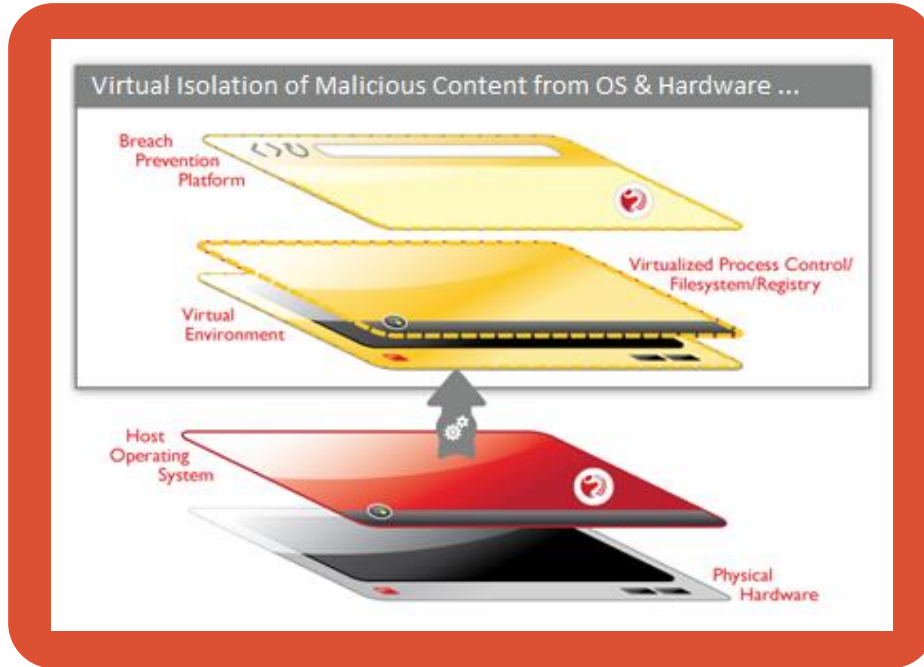


A **proactive approach** to defeating malware and advanced persistent threats in real-time

- Places a protective “bubble” around the browser and other untrusted content
- Detects and stops malicious activity like spear-fishing, drive-by downloads ... for both known and zero-day attacks
- Saves countless hours of IT remediation work

Dell Protected Workspace

Proactive Anti-Malware Detection & Prevention



Virtual Insulation

Apps are launched inside a "sandbox" isolating the OS, registry and hardware from direct attack

App Support

Web browsers
PDF readers
Office Apps
Zip & Exe files ...

Signature-Free

Detection is based upon actual behavior inside the sandbox of both known and zero-day attacks



Dell Endpoint Security

Comprehensive, Manageable, Secure



Most comprehensive protection

Protects end user data wherever it goes with flexible options that scale to fit your data protection needs.



Simplified management

Saves you time with a single console for remote management and seamless integration into your IT environment.



Secure by Design

Dell security hardware integrates tightly with our security solutions to close all the gaps

Q&A



The power to do more

