

Enforce Security Policies for Removable Devices, Media and Data

Data leakage caused by the accidental or sometimes malicious use of removable devices and/or removable media has reached alarming levels. In fact, over 85% of privacy and security professionals reported at least one breach and almost 64% reported multiple breaches that required notification.¹

Organization-wide Device Management

To enhance productivity, organizations need to provide employees and partners access to data. With more employees working remotely, access is required from outside the network. But the potential impact of data loss, be it accidental or malicious, is a very real concern. And today, removable devices / media are the most common data leakage routes – no file copy limits, no encryption, no audit trails and no central management.

The information contained in customer and corporate data, such as personally identifiable information (PII) and intellectual property (IP), is worth billions to some. In fact, the total average cost of a data breach incident is rapidly rising as well: the latest estimate is \$6.75 million – or \$204 per compromised record – per incident.² And this is likely to continue to increase, as new statutes and regulations impose criminal and civil penalties on organizations which lose PII.

Lumension® Device Control:

- » Centrally manages security policies regarding use of removable devices (e.g., USB flash drives) and media (e.g., DVDs/CDs) using a whitelist / “default deny” approach
- » Enforces encryption policies when copying data to removable devices / media
- » Prevents malware intrusion via removable devices / media, adding a layer of protection to your network
- » Provides the visibility, forensics and reporting needed to demonstrate compliance with applicable laws

Key Features

- » Per-Device Permissions
- » Whitelist / “Default Deny”
- » Flexible Policy with Granular Control
- » Policy Enforced Encryption
- » File Tracking
- » File Type Filtering / Copy Limits
- » Offline Enforcement
- » Centralized Management / Administrators’ Roles
- » Tamper-proof Agent
- » Flexible / Scalable Architecture

Key Benefits

- » Enables Secure Use of Productivity Tools, like USB Sticks
- » Protects Data from Loss / Theft
- » Enhances Security Policy Enforcement
- » Limits Malware Intrusion via USB Devices
- » Delivers Precise Control with Access Limits
- » Available for both stand-alone and Microsoft® SCCM implementations

“One of the main benefits in deploying Lumension Device Control is its whitelist feature, which ensures that no device, unless authorized, can ever be used, no matter how it gets plugged in. Flash memory USB devices represent a significant risk with the potential to steal company data or introduce “malware”, which could render the computer unusable and quickly infect other PCs on the same network. Device Control is a really strong, easy-to-use product which is why Barclays chose this solution.”

Paul Douglas, ADIR Desktop Build Team Manager, Barclays

1. Deloitte & Touche and Ponemon Institute, [Enterprise@Risk: 2007 Privacy & Data Protection Survey](#), December 2007

2. Ponemon Institute, [2009 Annual Study: Cost of Data Breach Study](#), January 2010

How Lumension® Device Control Works



1. Discover: Identify all removable devices that are now or have ever been connected to your endpoints.

2. Assess: Categorize all “plug and play” devices by class, group, model and/or specific ID and define policy through a whitelist approach.

3. Implement: Enforce file copy limitations, file type filtering and forced encryption policies for data moved onto removable devices.

4. Monitor: Track all policy changes, administrator activities and file transfers to ensure continuous policy enforcement.

5. Report: Provide visibility into device and data usage to demonstrate compliance with corporate and/or regulatory policies.

Key Features

Per-Device Permissions: Granular permissions to control access at device class (e.g., all USB flash drives), device group, device model and/or even unique ID levels.

Whitelist / “Default Deny”: Assigns permissions for authorized removable devices (e.g., USB flash drives) and media (e.g., DVDs/CDs) to individual users or user groups; by default, devices / media and users not explicitly authorized are denied access.

Flexible Policy with Granular Control: Permission settings include read/write, forced encryption, scheduled / temporary access, online / offline, port accessibility, HDD / non-HDD devices and much more; can be set for individual and/or groups of users, machines, ports and devices.

Policy Enforced Encryption for Removable Storage: Provides utmost flexibility in enforcing encryption policies when copying data to devices / media – be it centralized (admin-implemented) or decentralized (user-implemented), portable (for use on unmanaged systems) or non-portable (in network only).

File Tracking: Patented bi-directional shadowing technology keeps a copy of all files read from and/or written to removable devices / media; can also track just file types and names.

File Type Filtering / Copy Limits: Restrict and manage file types moved to and from removable devices / media; combine with forced encryption for added protection. Also, restrict amount of data copied to removable devices / media on a per-user basis.

Offline Enforcement: Permissions / Restrictions remain effective even when endpoint is offline; these can be the same as when online or different (i.e., context-sensitive permissions).

Centralized Management / Administrators’ Roles: Centrally defines and manages user, user groups, computer and computer groups access to authorized removable devices / media on the network; by default, those devices / media and users not explicitly authorized are denied access.

Tamper-proof Agent: Installs agents on every endpoint on the network; agents are protected against unauthorized removal – even by users with administrative permissions. Only Device Control Administrators may deactivate this protection.

Flexible / Scalable Architecture: Provides organization-wide control and enforcement using scalable client-server architecture with a central database that is optimized for performance. Supports virtualized server configurations.

System Requirements

- » **Server:** Windows® Server 2003, 2008, 2008 R2
- » **Client:** Windows XP, Windows Vista, Windows 7

[Complete Requirements](#)

Online Resources

- » [FREE TRIAL](#)
- » [Data Protection Blog](#)
- » [Whitepaper: Three Ways to Prevent USB Insecurity](#)
- » [Webcast: Four Practical Steps to Minimizing Insider Risk](#)

Are you an SCCM Customer?

Lumension® Device Control for System Center extends your existing SCCM implementation to provide market-proven, best-of-breed data protection (device / port control and data encryption), and compliance support – ensuring fast and simple set-up of security enforcement and device management within your SCCM infrastructure.

Contact Lumension

- » Global Headquarters
8860 E. Hartford Drive
Suite 300
Scottsdale, AZ 85255
+1.480.970.1025
sales@lumension.com
- » United Kingdom
+44.0.1908.357.897
sales.uk@lumension.com
- » Europe
+352.265.364.11
sales-emea@lumension.com
- » Asia & Pacific
+65.6725.6415
sales-apac@lumension.com

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Compliance and IT Risk Mgmt.

 **Lumension**
IT Secured. Success Optimized.™