

Device Control

Minimize Insider Risk by Enforcing Security Policies for Removable Devices, Media and Data

In today's business environment, insider risk is a rising concern. In fact, data breaches attributed to insiders more than doubled in the last year.¹ And with the increased usage of removable devices (e.g., USB flash drives) and media (e.g., CDs/DVDs) by the workforce, these productivity tools are the most common routes for data loss – no file copy limits, no encryption, no audit trails and no central management.

Enabling Productivity and Strong Data Protection

Removable devices are valuable productivity tools that facilitate data access and movement for improved collaboration between employees and partners. But the potential impact of data loss and malware introduction – be it accidental or malicious – is a very real concern. The information contained in customer and organizational 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 \$7.2 million – or \$214 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 and as organizational IP becomes more important in today's competitive environment.

Lumension® Device Control, available as a modular offering on *Lumension®* Endpoint Management and Security Suite, enables organizations to effectively balance productivity and data protection concerns by quickly identifying all end-point-connected devices in the network and flexibly enforce security policies that prevent unauthorized use, limit malware intrusion and force the encryption of sensitive information.

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 flexible whitelist approach
- » Encrypts data being copied to removable devices / media for additional protection
- » 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
- » Integrates with additional IT security and operations modules

Key Benefits

- » Enables Secure Use of Productivity Tools, like USB Sticks
- » Enhances Security Policy Enforcement
- » Protects Data from Loss and Theft
- » Ensures Data is Encrypted
- » Protects against Malware via USB Devices
- » Delivers Precise Control with Access Limits
- » Integrates with Endpoint Operational and Security Modules for Defense-in-Depth

Key Features

- » Per-Device Permissions
- » Device Whitelisting
- » Flexible Policy with Granular Control
- » Policy-based Encryption
- » File Tracking / Shadowing
- » File Type Filtering / Malware Protection
- » Copy Limits
- » Offline Enforcement
- » In-Depth Reporting
- » Centralized Management / Administrators' Roles
- » Integration with *Lumension®* Endpoint Management and Security Suite

1. Verizon Business RISK team, 2010 Data Breach Investigations Report, 2011
2. Ponemon Institute, 2010 Annual Study: Cost of a Data Breach, March-2011



How Lumension® Device Control Works



- 1. Discover:** Identify all removable devices connected to your endpoints in “audit mode.”
- 2. Define:** Create rules at both default and machine-specific levels for groups and individuals with regards to device access by class, group, model and/or specific ID.
- 3. Monitor:** Continuously observe the effectiveness of device and data usage policies in real time and identify potential security threats.
- 4. Enforce:** Implement “enforcement mode” of file copy limitations, file type filtering and forced encryption policies for data moved onto removable devices.
- 5. Manage:** Use dashboard widgets and/or create reports on all device and data activity showing allowed and blocked events.

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.

Device Whitelisting: Assigns permissions for authorized removable devices (e.g., USB flash drives) and media (e.g., DVDs/CDs) to individual users or user groups; use “audit mode” to set up / validate enforcement policies and then simply convert to “enforcement mode.”

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-based Encryption: Use central security policy to force encryption of all data being copied onto removable devices / media using FIPS 140-2 Level 2 validated cryptography module.

File Tracking / Shadowing: 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 metadata (e.g., type, name, etc.).

File Type Filtering / Malware Protection: Restrict and manage file types moved to removable devices / media; combine with forced encryption for added protection. Prohibit download of executables from removable devices for added layer of malware protection.

Copy Limits: Restrict amount of data copied daily 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).

In-Depth Reporting: Automatic logging of all network events related to your security policy – provides visibility into policy compliance and violations via reports, email and dashboard widgets.

Centralized Management / Administrators' Roles: Centrally defines and manages user, user groups, computer and computer groups access to authorized removable devices / media on the network; once in 'enforcement mode' only explicitly authorized devices / media / users are allowed access by default.

Integration with Lumension® Endpoint Management and Security Suite: Integrates with other Lumension product modules to streamline and improve IT operations and security, reduce agent bloat and improve endpoint visibility.

System Requirements

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

[Complete Requirements](#)

Online Resources

- » [FREE TRIAL](#)
- » [Device Scanner](#)
- » [Data Protection Blog](#)
- » [Whitepaper: Three Ways to Prevent USB Insecurity](#)
- » [Webcast: Endpoint Device Control in Windows 7 and Beyond](#)

Contact Lumension

- » Global Headquarters
8660 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.

