

## 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.<sup>1</sup>

### 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 media / devices 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. And the costs for recovery of data and lost business are rapidly rising as well: the total average cost of a data breach incident is estimated to be \$6.6 million or \$202 per compromised record, with the cost of lost business averaging \$4.6 million or \$139 per record.<sup>2</sup>

### Lumension Device Control provides:

- » Enforcement of removable device usage and data encryption policies
- » Central management of devices and data using a whitelist / "default deny" approach
- » Enablement of productivity-enhancing tools while limiting the potential for data leakage and its impact

### Key Features

- » Whitelist / "Default Deny"
- » Policy Enforced Encryption for Removable StorageData Copy Restriction
- » File Type Filtering
- » Temporary / Scheduled Access
- » Context-Sensitive Permissions
- » Centralized Management / Administrators' Roles
- » Role Based Access Control
- » Tamper-proof Agent
- » Flexible / Scalable Architecture

### Key Benefits

- » Protects Data from Loss / Theft
- » Enables Secure Use of Productivity Tools, Like USB Sticks
- » Enhances Security Policy Enforcement
- » Delivers Precise Control with Access Limits
- » Available for both stand-alone and Microsoft System Center Configuration Manager (SCCM) platform 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 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, 2008 Annual Study: Cost of Data Breach Study, February 2009

## How Lumension Device Control Works



1. **Discover:** Identify all removable devices that are currently or have ever been connected to your endpoints.
2. **Assess:** Categorize all “plug and play” devices by class, 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

**Whitelist / “Default Deny”:** Assigns permissions for authorized removable devices and media to individual users or user groups; by default, devices / media and users not explicitly authorized are denied access.

**Policy Enforced Encryption for Removable Storage:** Centrally encrypts removable devices (such as USB flash drives) and media (such as DVDs/CDs), plus enforces encryption policies when copying to devices / media.

**Data Copy Restriction:** Restricts the daily amount of data copied to removable devices and media on a per-user basis; also, limits usage to specific time frames / days.

**File Type Filtering:** Controls file types that may be moved to and from removable devices (such as USB sticks) and media (such as DVDs/CDs) on per-user basis.

**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.

**Temporary / Scheduled Access:** Grants users temporary / scheduled access to removable devices/media; used to grant access “in the future” for a limited period.

**Context-Sensitive Permissions:** Applies different permissions when the endpoint is connected to the network, when it is not, and/or regardless of connection status.

**Role Based Access Control:** Assigns permissions to individual users or user groups based on their Windows Active Directory or Novell eDirectory identity, both of which are fully supported.

**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.

[www.lumension.com](http://www.lumension.com)

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

## System Requirements

- » **Server:** Windows Server 2003, Windows Server 2008, SQL Server 2008
- » **Client:** Windows XP, Windows 2000, Windows 2003, Windows Vista

[Complete Requirements](#)

## Online Resources

- » [FREE TRIAL](#)
- » [Data Protection Blog](#)
- » [Device Scanner](#)
- » [Taking Control of Your Data: Protecting Business Information from Loss or Theft](#)
- » [Webcast: Data on the Edge](#)

## 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 managed within your SCCM infrastructure.

## Contact Lumension

- » Global Headquarters  
15880 N. Greenway Hayden  
Suite 100  
Scottsdale, AZ 85260  
+1.480.970.1025  
[sales@lumension.com](mailto:sales@lumension.com)
- » United Kingdom  
+44.0.1908.357.897  
[sales.uk@lumension.com](mailto:sales.uk@lumension.com)
- » Europe  
+352.265.364.11  
[sales-emea@lumension.com](mailto:sales-emea@lumension.com)
- » Asia & Pacific  
+65.6725.6415  
[sales-apac@lumension.com](mailto:sales-apac@lumension.com)

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