

## Lumension Device Control™

### 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 data, corporate data and intellectual property 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 \$6.3 million or \$197 per compromised record, with the cost of lost business averaging \$4.1 million or \$128 per record.<sup>2</sup>

#### Lumension Device Control provides:

- » Enforcement of removable device and data usage 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

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

1) Deloitte & Touche and Ponemon Institute, Enterprise@Risk: 2007 Privacy & Data Protection Survey, December 2007

2) Ponemon Institute, 2007 Cost of Data Breach Study, November 2007

#### Datasheet

#### Key Benefits

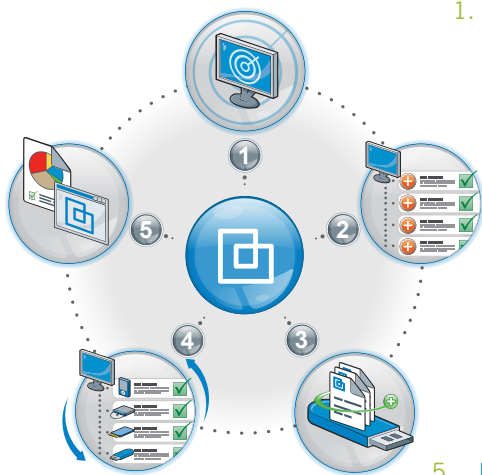
- » Protects Data from Loss / Theft
- » Enables Secure Use of Productivity Tools
- » Enhances Security Policy Enforcement
- » Delivers Precise Control with Access Limits

*"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



## How Lumension Device Control Works



1. **Discover:** all removable devices that are currently or have ever been connected to your end-points.
2. **Assess:** all “plug and play” devices by class, model and/or specific ID and define policy through a whitelist approach.
3. **Implement:** file copy limitations, file type filtering and forced encryption policies for data moved onto removable devices.
4. **Monitor:** all policy changes, administrator activities and file transfers to ensure continuous policy enforcement.
5. **Report:** on device and data usage to show proof of compliance with corporate and/or regulatory policies.

## Key Features

**Policy Enforced Encryption for Removable Storage:** Centrally encrypts removable devices (such as USB memory 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, limit usage to specific time frames / days.

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

**Whitelist / “Default Deny”:** Assigns permissions for authorized removable devices and media to individual users or user groups; by default, devices / media / people 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 con-

nected to the network, when it is not, and/or regardless of connection status.

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

**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:** Agents are installed on every endpoint on the network, and are protected against unauthorized removal – even by authorized (local) administrators. Only (enterprise) Administrators may deactivate this protection.

**Flexible / Scalable Architecture:** Provides organization-wide control and enforcement using scalable client-server architecture with a central database.

## System Requirements

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

## Other Lumension Products

- » Lumension Device Control
- » Lumension Application Control
- » Lumension Patch & Remediation
- » Lumension Scan
- » Lumension Vulnerability Management
- » Lumension Enterprise Reporting
- » Lumension NAC Integrator



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

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance



LDC-DS-EN-01-29-09