

# Lumension® Data Protection



## Prevent Data Loss and Theft by Enforcing Removable Device Usage and Data Encryption Policies

In today's global 24x7 business environment, organizations need real-time access to information - balancing this with the associated risks is key to ensuring data is not lost or stolen and business productivity is not diminished. Lumension Data Protection automates the enforcement of data and device usage policies across the entire network and enforces encryption policies for sensitive data being copied to removable devices.

## Data Protection Business Drivers and Challenges

Data breaches resulting in the loss/theft of sensitive data remain a major concern. In fact, more than 85% of companies surveyed had at least one reportable breach and 63% experienced multiple (between 6 and 20) reportable breaches.<sup>1</sup> It is expensive to recover from a data breach; not only the hard costs (e.g., notification, free credit checks, etc.), but also in terms of lost customer trust and brand equity resulting in lost business. In fact, recent statistics put the average total cost of a corporate data breach at \$6.6 million, with lost business accounting for 69% of breach costs.<sup>2</sup>

This concern over data loss/theft has spawned a myriad of regulations, including pan-national (e.g., EU directive 45/2001), national (e.g., SOX, GLBA and HIPAA), state (e.g., CA SB 1361) and even industry-specific standards (e.g., PCI DSS), which apply to almost all public and private organizations no matter where they operate. For instance, in 2010 Massachusetts will require businesses that collect information about that state's residents to follow comprehensive information security requirements; these apply to both in-state and out-of-state companies with operations or customers in Massachusetts.

Ensuring compliance with all of these regulations adds another layer of risk to your organization. Failure to comply can result in very real economic damage, both directly in terms of cost and indirectly in terms of lost customers and business.



“By rolling out Lumension Data Protection to all of our desktops, we were able to set policies based on either a user's role or a user's identity. A user could get full thumb drive access, just keyboard access or access to read from a thumb drive or CD-ROM, but not be able to save anything to the machine.”

Rob Israel, CIO, John C. Lincoln Health Network

## Put an End to Lost Data and Business with Lumension Data Protection

As an IT professional charged with protecting your organization's vital information, you are well aware of the issues:

- » **Borderless enterprise** - The growth of “borderless enterprises” means data is less centralized than ever before: disaggregated supply chains, outsourcing, and a mobile workforce all contribute to increased collaboration and productivity, but also opens the door to data loss or theft.
- » **Increased insider risks** - Innocent mistakes, malicious intent and increased opportunity all lead to an increased internal threat. Some studies suggest that well over half of all serious data breach incidents are sparked by insiders<sup>3</sup> and almost 60% of insiders admitted they have taken company data when they leave their employer.<sup>4</sup>

1. Deloitte & Touche and Ponemon Institute, [Enterprise@Risk: 2007 Privacy & Data Protection Survey](#), December 2007
2. Ponemon Institute, [2008 Annual Study: Cost of a Data Breach](#), February 2009
3. Data Monitor, [Mitigating the Risks of Data Loss](#), August 2007
4. Ponemon Institute, [Data Loss Risks During Downsizing](#), February 2009

- » **Organized external threats** - Gone are the days of pranksters and script kiddies. Today, the attacks are highly targeted, launched by increasingly sophisticated criminals who exploit online forums to buy and sell tools, services and stolen data. These organized cyber criminals supply a black market recently estimated at \$276M.
- » **Consumerization of IT** - Users are increasingly defining the IT environment by bringing their productivity tools, both hardware (like USB flash drives) and software (like IM), into work. This too facilitates collaboration and productivity, but also exposes the organization to malware (e.g., Trojans).

“Deploying Lumension has given us peace of mind that our commercially sensitive data is secure, meaning that the risk of our directors being liable for any information leaks is minimal. The decision to invest in Lumension was an easy one - we simply compared the cost of purchasing and deploying the software with the financial and reputational risk to the business of being a victim of a security breach”.

Kevin Gregory, Senior Business and IT Manager, Savills Hamilton Osborne King

When developing your data protection strategy in this increasingly difficult environment, it is important to balance the rewards of accessible data (and the collaboration / productivity it enables) with the risks (and costs) of losing your data. Lumension Data Protection enables you to effectively balance that risk/reward to enable productivity without putting sensitive information at risk.



## How Lumension Data Protection Works

### Key Benefits

- » Protects Data from Loss/Theft
- » Ensures Compliance with Security Policies, Regulations and Industry Standards
- » Enforces Encryption on Removable Devices
- » Enables Secure Use of Productivity Tools like USB Sticks
- » Available for both stand-alone and Microsoft System Center Configuration Manager (SCCM) platform implementations

# Take Control of Your Vital Information

Ensure your data is protected. Contact your local Lumension sales representative or reseller today or visit us at [www.lumension.com](http://www.lumension.com).



“Consumers’ personal financial information is highly-targeted by identity thieves and we are obligated to take all precautions necessary to protect this data. With Lumension, I can stay ahead of potential challenges, providing peace of mind for the bank’s executives and auditors, and ultimately, our customers.”

Brent Rickels, VP Technology, First National Bank of Bosque County

## Key Features

- » Identifies all endpoints on the network and all devices ever connected to these endpoints (servers, desktops, laptops, etc.).
- » Automatically forces encryption of sensitive data being moved to removable devices and media, ensuring it is protected.
- » Installs tamper-proof agents on every endpoint on the network and protects against unauthorized removal – even by local administrators.
- » Logs all network events related to your Data Protection policy automatically, including endpoint status, device connection, user activity, and file tracking, providing visibility into policy compliance and violations.
- » Assesses device and data usage, including what device, on what machine, by which user, and when.
- » Provides organization-wide control and enforcement using scalable client-server architecture with a central database that is optimized for performance. Supports virtualized server configurations.
- » Defines security policy with global and user- and/or machine-specific rules based on specific organizational needs using a “whitelist” approach.
- » Fully supports both Windows Active Directory and Novell eDirectory / NDS structure.
- » Enforces your data and device usage policies automatically across your entire network.

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

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

## Online Resources

- » [FREE TRIAL](#)
- » [Data Protection Blog](#)
- » [Device Scanner](#)
- » [Webcast: Data on the Edge](#)
- » [Taking Control of Your Data: Protecting Business Information from Loss or Theft](#)
- » [Compliance with Data Handling Procedures in UK Government](#)
- » [ROI Case Study with John C. Lincoln Health Network](#)
- » [Minimizing Security-Related Total Cost of Ownership](#)

OTIKA

Phone: 01 71 11 31 45

[lumension@otika.fr](mailto:lumension@otika.fr)

[www.otika.fr](http://www.otika.fr)

LDP-SB-EN-10-02-09