Lumension® Data Protection

Prevent Data Loss and Theft by Enforcing Data Encryption and Removable Device Usage 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 encryption and removable device usage policies across the entire network.

Lumension
IT Secured. Success Optimized.™

Data Protection Business Drivers and Challenges

Data breaches resulting in the loss/theft of sensitive data remain a major concern. In fact, in 2010 more than 90% of companies surveyed had at least one reportable breach and 59% experienced two or more reportable breaches.[1] 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 $7.2 million, with breaches involving lost or stolen laptops or other removable storage devices costing significantly (as much as 20%) more.[2]

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, since 2010 Massachusetts has required all organizations that collect information about that state's residents to follow comprehensive information security requirements; this applies to both in-state and out-of-state organizations with operations or customers in Massachusetts.

Ensuring compliance with all of these personal information protection 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

And yet the loss of so-called toxic customer data might pale in comparison to the loss of vital, revenue-generating intellectual property (IP) such as designs for the next generation chip, marketing forecasts, customer lists and other trade secrets. In fact, a recent report concluded that proprietary knowledge and company secrets are twice as valuable as the custodial data.[3]

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.

- **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).

1. Ponemon Institute, Perceptions About Network Security, Jun 2011
2. Ponemon Institute, 2010 Annual Study: Cost of a Data Breach, Mar 2011
3. Forrester Research, The Value Of Corporate Secrets, Mar 2010
4. Securosis, 2010 Data Security Survey, Sep 2010
5. Ponemon Institute, Data Loss Risks During Downsizing, Feb 2009
6. Ponemon Institute, The Billion Dollar Lost Laptop Problem, Sep 2010
7. IDC, Laptop Theft- The Internal and External Threats, Sep 2010
8. Ponemon Institute, The State of USB Drive Security, Jul 2011

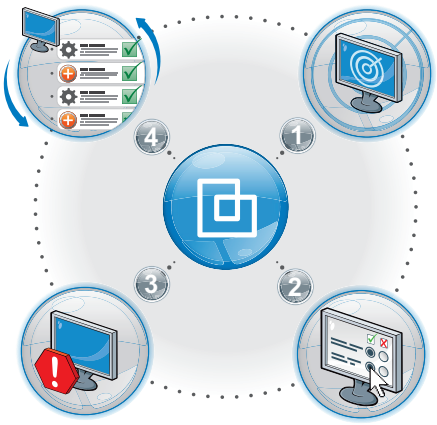
» **Increased Insider Risks** - Innocent mistakes, malicious intent and increased opportunity all lead to an increased internal threat. Studies suggest that over 70% of all data breach incidents are sparked by insiders (either intentionally or accidentally)[4] and almost 60% of insiders admitted they have taken company data when they leave their employer.[5]

» **Lost / Stolen Laptops / Devices** - Surveys indicate that 86% of organizations have had a laptop lost or stolen, and 56% report that it resulted in a data breach.[6] And an astonishing 58% of these laptop losses happened at work.[7] And while hard statistics on lost or stolen removable devices (like USB sticks) and media (like CDs / DVDs) are difficult to come by (given the price point, it's easier to replace than to report), 70% of organizations link their loss of sensitive or confidential information to USB flash memory sticks.[8]

» **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.

"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 portable and 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.



1. **Discover:** Find all the endpoints in your network, and who is using what removable devices / media on those endpoints; use "audit mode" to collect the information without disrupting productivity.

2. **Define:** Centrally create and manage encryption of endpoint hard drives and removable devices / media. Use whitelisting approach to create rules at both default and machine-specific levels for groups and individual users; this proactive approach limits your burden to defining what is allowed instead of trying to keep up with the ever changing list of what is bad.

3. **Enforce:** Implement data encryption and USB security policies to ensure sensitive information is secured by encrypting hard drives and removable devices / media, controlling file transfers (e.g., copy limits by amount and/or time of day, type filtering), and more.

4. **Manage:** Generate reports which show how your data protection policies safeguard critical business information, prevent unauthorized data access via lost or stolen laptops or removable devices / media, and demonstrate compliance with internal security policies and external government and industry regulations.

How Lumension Data Protection Works

Key Benefits

» Protects Data from Loss/Theft
» Ensures Compliance with Security Policies, Regulations and Industry Standards
» Enforces Encryption on Hard Drives and Removable Devices / Media
» Enables Secure Use of Productivity Tools like USB Sticks
» Reduces Impact / Cost of Lost or Stolen Laptop, Devices or Media Containing Sensitive Data 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.

"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 connected to these endpoints (servers, desktops, laptops, etc.).
- Assesses device and data usage, including what device, on what machine, by which user, and when.
- Defines security policy with global and user- and/or machine-specific rules based on specific organizational needs using a "whitelist" approach.
- Enforces your data encryption and device usage policies automatically across your entire network, even when the endpoint is offline.
- Automatically forces FIPS 140-2 validated encryption of sensitive data on endpoint hard drives and removable devices / media, ensuring it is protected.
- Logs all endpoint 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.
- Provides organization-wide control and enforcement using scalable client-server architecture with a central database that is optimized for performance. Supports virtualized server configurations.
- Integrates with *Lumension*® Endpoint Management and Security Suite to improve endpoint security and to reduce operational complexity.
- Utilizes a tamper-proof, modular agent architecture to simplify deployment / upgrades, eliminate agent bloat and improve operational security.

www.lumension.com

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

Online Resources

- FREE TRIAL
- Data Protection Blog
- FREE Device Scanner
- Webcast: Data on the Edge
- Whitepaper: Taking Control of Your Data
- Whitepaper: Compliance with Data Handling Procedures in UK Government
- ROI Case Study with John C. Lincoln Health Network
- Whitepaper: Minimizing Security-Related Total Cost of Ownership

Contact Lumension

- Global Headquarters
  8660 East 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

Lumension
IT Secured. Success Optimized.™

LDP-SB-EN-10-18-11