

Unified PROTECTION & CONTROL

Lumension Security provides proactive endpoint protection and control through best-of-breed policy-based solutions.

putting security in a positive light



putting security in a positive light

Traditional security models are reactive in nature and are constantly working to resolve threats after the fact. One AV vendor has reported that 70,000 unique malware fingerprints were created in the last two months of 2006. This figure does not cover all threats 'in the wild' today as cyber criminals leverage financially motivated and targeted 'boutique' malware to gain access to sensitive data.

Lumension Security, formerly PatchLink, is maximizing the synergies between three best-of-breed, policy-based solutions and brands to deliver definitive protection and control of your corporate endpoints:

- ▣ **PatchLink®** – Since 1991, the market share leader in Patch and Remediation Management
- ▣ **Harris® Corporation's STAT®** – Vulnerability Assessment solution of choice for large government and commercial organizations
- ▣ **SecureWave Sanctuary®** – Since 2000, the market leader in Endpoint Policy Enforcement solutions with integrated Application and Device Control

Lumension's Positive Security Model leverages proven security methodologies, practices and technologies to help organizations simplify the entire security management lifecycle. By putting security in a positive light, Lumension is shifting the security paradigm from a reactive model to a proactive approach, providing definitive protection of enterprise data and IT assets, improving operational efficiencies, reducing costs and accelerating business results.



Say Goodbye to Security Management Challenges

Managing Risk at the Endpoint

Managing risk throughout an enterprise can feel like an insurmountable issue as new vulnerabilities are exposed regularly and as other threats targeting IT assets and sensitive data come not only from external sources, but also from within. Threats come from virtually anywhere, from curious hackers to malicious code writers to professional criminal organizations to corporate or government espionage to employees who accidentally or intentionally click on a malicious web link or disclose sensitive data.

A key concern for organizations is understanding what is in your network and managing the risk from exploited vulnerabilities, malware and data leakage - all while enabling your end users to achieve desired business results.

New Vulnerabilities Exposed and Targeted

Vulnerabilities continue to rapidly increase, many of which must be addressed immediately:

- ▣ 24 vulnerabilities are identified every day, of which 12.5 are considered serious enough for IT staff to address each day¹
- ▣ Hackers are using automation to identify and exploit vulnerabilities - 8,064 reported in 2006²
- ▣ 75 percent of enterprises will be infected with financially motivated, targeted malware that evaded traditional perimeter and host defenses³

Data Leakage

Protecting data continues to confound organizations:

- ▣ 75 percent of Fortune 1000 companies fell victim to data leakage⁴
- ▣ 53 percent of organizations would never know what data was lost on a USB device⁵
- ▣ Companies spend on average \$5 million dollars per year to recover lost or stolen data⁵

The Insider Threat

Endpoints have become a major source of disclosure. Oftentimes the threat comes from within the organization:

- ▣ 70 percent of all serious incidents are sparked by insiders⁶
- ▣ 56 percent of CISOs noted employee misuse of corporate data as the most serious IT challenge⁷

Bringing Disparate Groups Together

IT, security and business groups rarely work together to solve business challenges such as:

- ▣ Managing corporate risk
 - ▣ Complying with federal and industry regulations
- ▣ The rising value and security of data transmission and storage
- ▣ The increasing sophistication of attackers

Each organization within the enterprise has its own measurements and goals, but there must be interaction at a policy level among these disparate groups in order to successfully manage risk and improve efficiencies.

Developing Security Policy and Regulatory Controls, and Responding to Audits

Many organizations have a false sense of security because they do not have comprehensive visibility into their network and do not have effective endpoint protection controls. Enterprises must enforce proper controls and must be able to prove policy compliance as:

- ▣ Regulatory compliance related to IT security is seen as a critical security issue⁴
- ▣ The majority of enterprises - 66 percent - are subject to regulatory compliance⁸
- ▣ 27 percent of all software on business computers is unlicensed, the average fine for which is \$91,000 if caught⁹

Reducing Costs and Complexity, Consolidating IT and Improving Productivity

To address security management challenges, enterprises have come to rely upon many different security and configuration management vendors and solutions. Reliance on many point solutions forces organizations to manage silos, which produce inconsistent security approaches, fragmented policy enforcement and reporting, and ultimately a more complex network to manage and secure. As such, organizations cannot achieve economies of scale across people, processes and technologies.

Taking the Next Step

The ineffectiveness of silo endpoint solutions has sparked demand for a shift in the security paradigm to a more holistic approach to unified security management. Enterprises are clamoring for definitive protection of their endpoints.

Only through policy-driven security solutions can enterprises proactively manage risk, work across disparate groups, comply with security policies and regulations, consolidate IT resources, and ultimately reduce costs and improve productivity.

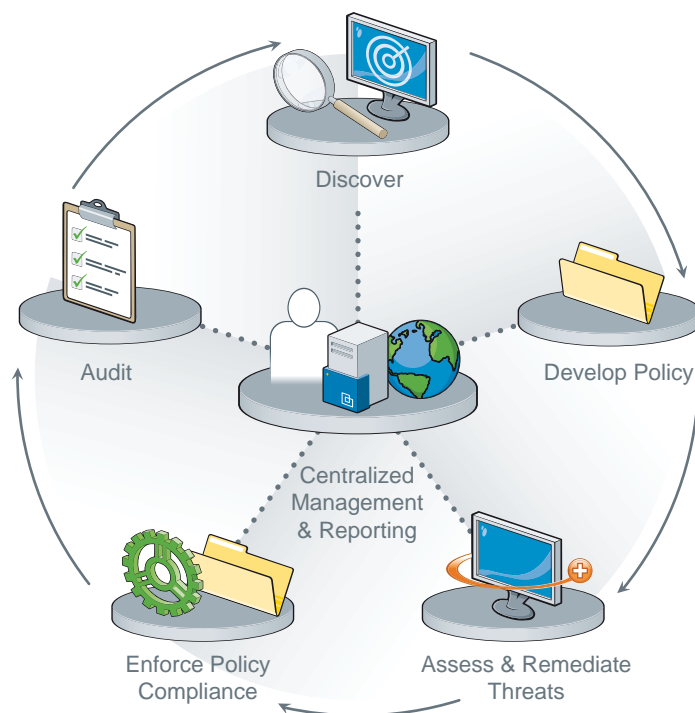
Say Hello to A Secure Environment

Unified Protection and Control

Lumension Security is a leading global security management company, providing unified protection and control of all enterprise endpoints, applications and devices to more than 5,100 customers and 14 million nodes worldwide. Lumension enables organizations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions, including:

- ▣ Unified Vulnerability Management – Automated Discovery, Assessment, Remediation and Validation
- ▣ Unified Endpoint Policy Enforcement – Application and Device Control
- ▣ Integration with Leading Network Access Control Solutions
- ▣ Extensive Policy Compliance Reporting

Employing a policy-based framework that mitigates non-compliant behavior or vulnerabilities *before* problems occur, Lumension solutions assure that desired security levels are consistently and continuously enforced throughout the enterprise.



1. Discover – Discover all assets on the network to identify unmanaged and rogue devices for a complete view of your risk profile.

2. Develop Policy – Create a policy framework that establishes an enterprise security posture and enables the business and technical sides of the organization to work together to manage risk. This includes setting mandatory baselines for software vulnerabilities and hardware configurations, determining user behavior with specific applications and peripheral devices and developing auditing and reporting processes.

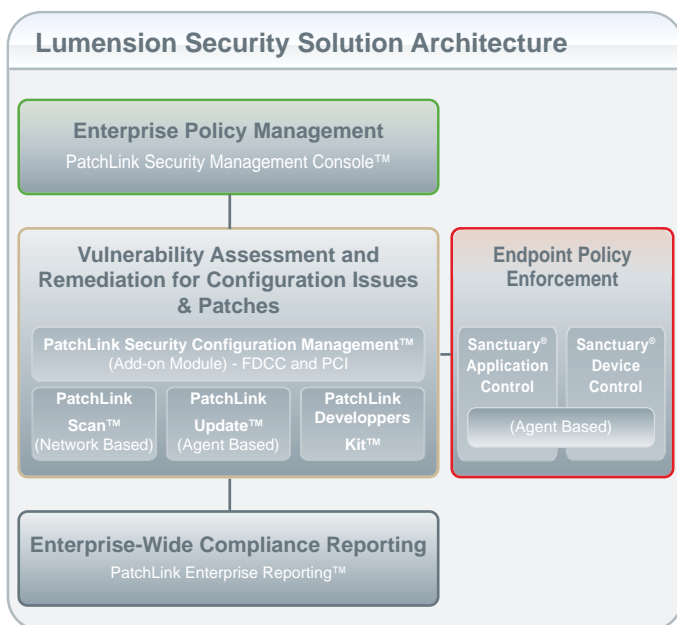
3. Assess and Remediate Vulnerabilities – Assess asset and vulnerability criticality through network and agent-based scanning and remediate all known vulnerabilities.

4. Enforce Policy – Enable and promote acceptable use of resources while preventing and reporting unacceptable ones that could put the enterprise at risk, such as the deliberate or accidental execution of malware and unknown or unwanted applications; reading and writing company-confidential or private data to personal removable media; attaching a PC to the corporate network that may have back-level, vulnerable software installed.

5. Audit - Develop routine, comprehensive reports to inform all policy stakeholders of the enterprise's security state on a continuous basis, escalating high risk violations, and providing a constant audit trail.

Through development and enforcement of endpoint policies that cut across all products, disparate groups and users, enterprises can truly take charge of their security posture and shift the security paradigm from a reactive security approach to a positive one.

Lumension Security Solution Architecture



Proven Policy-Based Process

Lumension Security's proven policy-driven process enables organizations to achieve a desired security posture with centralized management and reporting to ease administration and interaction among disparate groups. The process includes five key steps:

Best-of-Breed Solutions & Brands Coming Together



PatchLink Security Management Console™

Centralized command and control over the entire vulnerability management process and a single, unified view of the IT infrastructure and risk profile.

PatchLink Security Configuration Management™

Out-of-the-box regulatory and best security configuration practices templates to ensure corporate endpoints and applications are properly configured.

PatchLink Scan™

Complete network-based scanning solution enables assessment and analysis of threats impacting all network devices.

PatchLink Update™

Proactive management of threats through automated collection, analysis, and delivery of patches (all major operating systems and applications) across heterogeneous networks.

PatchLink Developers Kit™

Create custom remediation packages to address configuration issues, remove unauthorized files and applications, address zero-day threats, patch custom software and more.

PatchLink Enterprise Reporting™

Robust data warehouse that enables easy creation and sharing of reports on all aspects of your remediation efforts in support of policy compliance.



Sanctuary® Application Control

Policy-based enforcement of application use to secure your endpoints from malware, spyware and unwanted or unlicensed software.

Sanctuary® Device Control

Policy-based enforcement of removable device use to control the flow of inbound and outbound data from your endpoints.

Lumension Security At A Glance

- ☒ Ranked #14 on Inc. 500 List of Fast Growing Companies for 2006
- ☒ Ranked #1 in Patch and Remediation Market Share for Third Consecutive Year
- ☒ More than 5,100 Customers and 14 Million Nodes Deployed Worldwide
- ☒ Highly Experienced Team of Security Market Professionals
- ☒ Backed by Some of the World's Leading High-Tech Venture Firms

What Our Customers Are Saying

"Before PatchLink, securing our mobile devices was an organized free-for-all. Without a centralized patching process, we couldn't keep up with vulnerability patching and software upgrades. Now we have comprehensive, automated vulnerability management for our very mobile organization."

Booz Allen Hamilton

"Sanctuary provides a single, seamless view of everything accessing or attempting to access your network through corporate endpoints from a device and application perspective, providing a new level of visibility into your network then was previously possible."

John C. Lincoln Health Network

"Sanctuary Device Control ensures that no device, unless authorized, can ever be used, no matter how it gets plugged in. Device Control is a really strong, easy to use product which is why Barclays chose this solution."

Barclays

"Once we saw what PatchLink could do we were knocked out by its flexibility and its ability to remotely provide subcategories for different systems. PatchLink was the only vendor that could do this effectively providing us with the visibility and added security protection we needed."

Australian Defense Force Academy

Sources

1. National Vulnerability Database - May 9, 2007
2. www.cert.org
3. Gartner Research, "Gartner's Top Predictions for IT Organizations and Users, 2007 and Beyond," Daryl C. Plummer, December 1, 2006
4. 2006 CSI/FBI Computer Crime and Security Survey
5. Ponemon Institute, 2006 Cost of Data Breach Study
6. IDC Worldwide Security Products and Services 2007 Top 10 Predictions
7. Merrill Lynch Security Software CISO survey, June 27, 2007
8. Yankee Group
9. UK Business Software Alliance





Lumension Security - Worldwide Headquarters

15880 N. Greenway-Hayden Loop Suite 100 Scottsdale, AZ 85260
phone: +1 (480) 970 1025

Lumension Security - United Kingdom

Unit C1, Windsor Place Faraday Road, Crawley West Sussex RH10 9TF United Kingdom
phone: +44 (0) 1908 357 897

Lumension Security - Continental Europe

Atrium Business Park Z.A. Bourmicht 23 rue du Puits Romain L-8070 Bertrange Luxembourg
phone: +352 265 364 11

Lumension Security - Asia Pacific

Level 27 Prudential Tower 30 Cecil Street Singapore 049712
phone: +65 6725 6415