

Say Hello to

## **PROACTIVE ENDPOINT SECURITY**

Protect Against IT Security Threats that Evade  
Traditional and “Best Guess” Defenses

## Today's Endpoint Security Challenges

With 74 percent of an enterprise's overall financial losses the result of virus attacks, unauthorized access to networks, lost/stolen laptops and mobile hardware, theft of proprietary information or intellectual property, protecting your endpoints is of utmost importance<sup>1</sup>. The threat landscape has undergone a shift from widespread attacks to those that target specific sources of endpoint risk, such as zero-day threats, missing patches and system mis-configurations.

According to Gartner Inc., 75 percent of enterprises will be infected with undetected, financially motivated, targeted malware that evaded traditional perimeter and host defenses<sup>2</sup>. It is clear that the traditional, reactive approaches to security have been unable to stem the tide of these ever-increasing threats because they were not designed to address today's challenges:

**75% of enterprises will be infected with undetected and targeted malware.<sup>2</sup>**

Gartner Inc.

**Borderless Enterprise** : More employees work remotely than ever before and the increased usage of mobile technology pushes data further from the network.

**70% of all security incidents are sparked by insiders.<sup>4</sup>**

IDC

**Increasing OS and Application Vulnerabilities** : 20 new software and configuration vulnerabilities are released per day and are being exploited by cyber criminals faster than ever before<sup>3</sup>.

**Insider Threats** : 70 percent of all serious incidents are sparked by insiders who are privy to sensitive data and know the value of it<sup>4</sup>.

**Well-funded Adversaries Target Organizations** : Cyber criminals target specific organizations and environments with methods that are more advanced, more varied and much harder to detect.

**53% of companies would never know what information was lost or stolen with USB devices.<sup>5</sup>**

Ponemon Institute

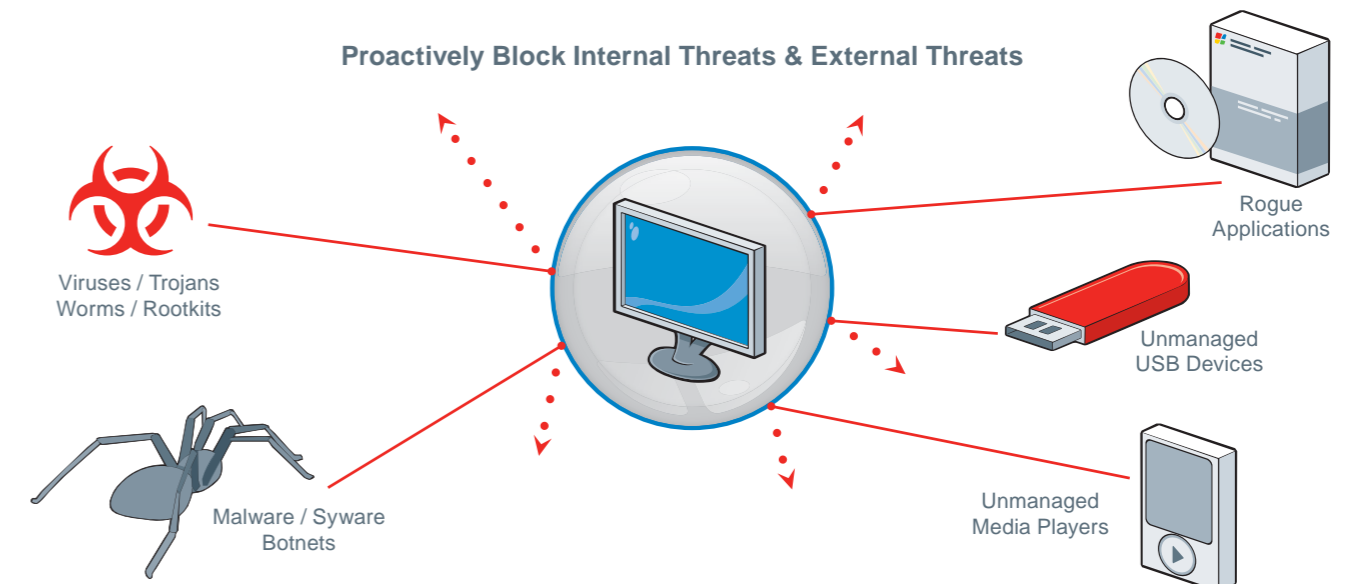
## Lumension's Proactive Endpoint Security Approach

95 percent of attacks exploit mis-configured or un-patched endpoints, with the final five percent coming from zero-day attacks<sup>6</sup>. By proactively remediating these sources of endpoint risk before they can be exploited, Lumension Security takes the guesswork out of securing corporate endpoints.

**95% of attacks target mis-configured or un-patched endpoints.<sup>6</sup>**

Gartner Inc.

Lumension Security enables organizations to improve their endpoint security and operations from a cost, effectiveness and productivity standpoint. Continuous monitoring and enforcement of endpoint security policies across platforms, users and data ensures that organizations are protected from both internal and external threats.



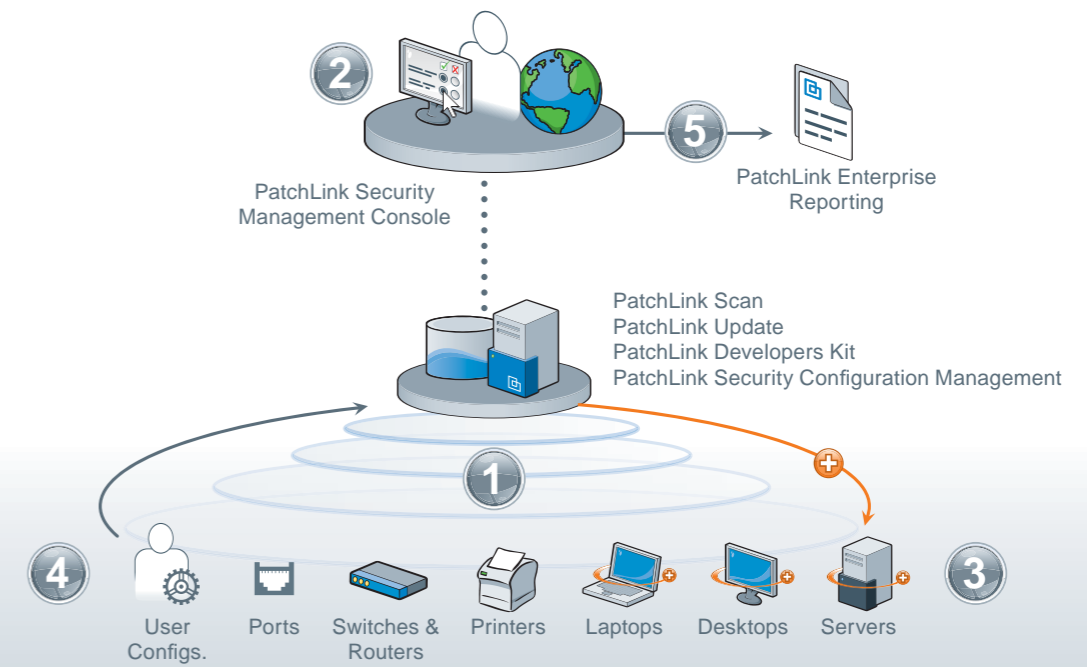
Platform Security	User Security	Data Security
Enforce policies regarding patches, configurations and authorized applications.	Enforce policies to enable only authorized users to access certain applications and removable devices.	Enforce policies to secure and audit the transfer of data to removable devices.
<ul style="list-style-type: none"> <li>Vulnerability Management</li> <li>Application Control</li> </ul>	<ul style="list-style-type: none"> <li>Application Control</li> <li>Data Protection</li> </ul>	<ul style="list-style-type: none"> <li>Data Protection</li> </ul>

## Vulnerability Management Solution

Lumension's Vulnerability Management solution simplifies control of the entire vulnerability life-cycle through a market-validated process that includes comprehensive asset discovery and inventory, thorough vulnerability assessments based upon network and agent-based scans, intelligent, automated remediation and ongoing policy compliance audits - all from a single, seamlessly integrated solution with enterprise reporting.

### Comprehensive Vulnerability Management Solution delivers:

- ☒ Thorough and accurate discovery of network assets using both network and agent-based scans of all resources to ensure maximum coverage
- ☒ In-depth assessment of vulnerabilities
- ☒ Automatic deployment of agents and remediation of configuration and software vulnerabilities
- ☒ Flexible, open support for all major platforms and applications
- ☒ Advanced vulnerability, configuration and policy compliance reporting



### PatchLink Update™

PatchLink Update proactively remediates threats through the accurate and automated collection, analysis and delivery of security and operational patches for all major operating systems and applications across heterogeneous networks. PatchLink Update's scalable, agent-based patch management provides the capabilities and context to effectively act on information. Flexible, role-based administration with Active Directory integration enables the delegation of agent/group management, assessment and remediation activities to improve productivity while maintaining security. Ongoing audits of applied patches ensure continuous policy compliance. PatchLink Update:

- ☒ Minimizes risk through immediate discovery of assets and vulnerabilities
- ☒ Eliminates software vulnerability flaws through the rapid deployment of patches and continuous enforcement of mandatory baselines
- ☒ Simplifies management of the remediation process with one solution for all major operating systems and applications
- ☒ Reduces the cost and time required between the detection and remediation of vulnerabilities
- ☒ Demonstrates IT policy and regulatory compliance with comprehensive auditing and reporting of patch deployments

### PatchLink Scan™

PatchLink Scan provides accurate, rapid and actionable network-based vulnerability assessments using safe, flexible scanning techniques based on access levels including credentialed and null-based scans. The network-based scanner identifies all software threats, including missing patches, out-of-date anti-virus signatures, worms, Trojans, and more, and conducts detailed configuration checks on ports, users, shares, groups, agents and services. Once threats are identified, PatchLink Scan prioritizes them for remediation based upon vulnerability scoring and asset criticality, leveraging common industry tracking standards such as SANS, BugTraq, CVE, IAVA, CERT and many more. PatchLink Scan:

- ☒ Delivers visibility of network environment, identifying all network devices and vulnerabilities including: servers, desktops, laptops, printers, routers, switches, wireless access points and more
- ☒ Provides detailed and accurate assessments of vulnerabilities for orderly remediation
  - Description of the vulnerability and potential exploits
  - Exploit categorization and severity
  - Reference links and sources of vulnerability information
  - Tested remediation instructions
  - Impacted executable files or DLLs
  - Registry and file reference for the vulnerability

### PatchLink Security Configuration Management™

PatchLink Security Configuration Management delivers out-of-the-box regulatory and standards-based assessment to ensure endpoints are properly configured. Based on best practices as defined by NIST, NSA and DoD, PatchLink Security Configuration Management prevents configuration drift and identifies risk via proactive and continuous monitoring and reporting of the endpoint configuration status. By fortifying the configuration of operating systems and applications, PatchLink Security Configuration Management:

- ☒ Eliminates endpoint risk through proactive and automated configuration issue identification and correction
- ☒ Simplifies regulatory or policy compliance by leveraging Security Content Automation Protocol (SCAP) to automate and standardize technical controls
- ☒ Reduces IT operations and support costs by integrating with PatchLink Update and PatchLink Scan to manage all vulnerability activities from one single solution

Assesses hundreds of pre-defined security configuration checks, including:

- Event Log Policy Settings
- File Permission Settings
- Local Policies Group
- System Services Group
- Network Settings
- System Settings
- Windows Components
- Local User Policy Settings
- Security Patches
- Firewall Settings
- IE Settings
- Application Settings (i.e. Office, Symantec, IIS, Apache, etc.)

### Ancillary Vulnerability Mgmt. Products

#### PatchLink Developers Kit™

PatchLink Developers Kit enables administrators to enforce and automate configuration policies and tasks, develop and deploy custom remediation content, distribute software applications, files and data and respond to zero-day vulnerabilities.

#### PatchLink Security Management Console™

PatchLink Security Management Console provides centralized command and control over the entire vulnerability management process and a single, unified view of the IT infrastructure and risk profile.

#### PatchLink Enterprise Reporting™

PatchLink Enterprise Reporting delivers centralized business intelligence that enables organizations to consolidate security data from across the enterprise, assess business risk through powerful data mining analysis, and demonstrate security policy and regulatory compliance status through flexible, customized reporting.

## Data Protection Solution

Lumension's Data Protection Solution delivers best-of-breed technologies to secure data-in-motion and data-at-rest:

**Device Control** – Protects against data theft and data loss with comprehensive auditing of all data movement and device access attempts

**Whole Disk Encryption (WDE)** - Enforces disk and file encryption to protect against data loss

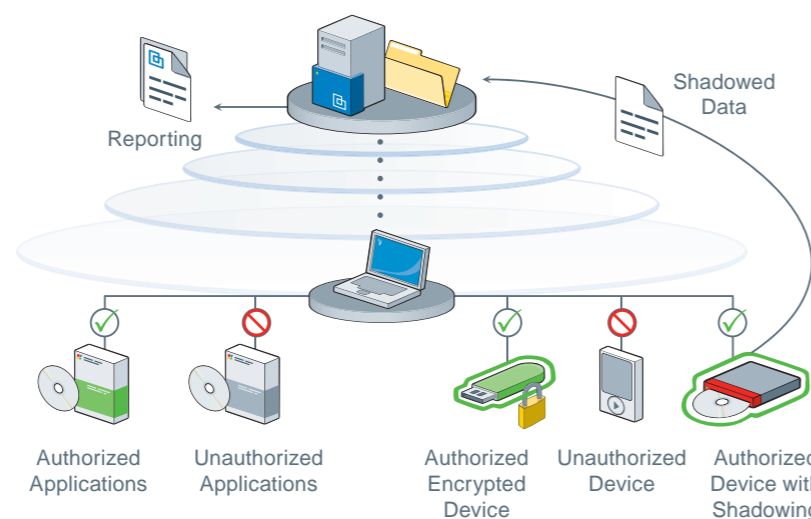
**Content Monitoring and Filtering** - Provides visibility as to the sensitivity of data that is transferred onto removable media

### Sanctuary Device Control

Sanctuary Device Control delivers policy-based enforcement of removable device use to control the flow of inbound and outbound data from enterprise endpoints. With Sanctuary, only authorized devices are allowed to be accessible on endpoints - all unauthorized device access is prohibited by default. Sanctuary Device Control:

- ☑ Reduces risk of data leakage through any ports or removable media including USB, FireWire, WiFi, Bluetooth, CD/DVD, etc.
- ☑ Enables the enforcement of flexible and granular policies to ensure maximum data protection and user productivity
- ☑ Delivers and enforces 256 AES encryption for data transferred onto removable devices
- ☑ Ensures policy compliance through detailed audit capabilities, including the tracking of all data written to/from a removable device as well as all administrator actions and access attempts
- ☑ Prevents malware introduction via unauthorized removable media

Additionally, Lumension Security has extended its data protection capabilities through best-of-breed partnerships with some of the leading endpoint encryption and data leakage prevention vendors, to deliver total data protection at the endpoint.



## Application Control Solution

Lumension's Application Control Solution enforces what can run on an endpoint and prevents anything that is not explicitly trusted to load in memory.

### Sanctuary Application Control

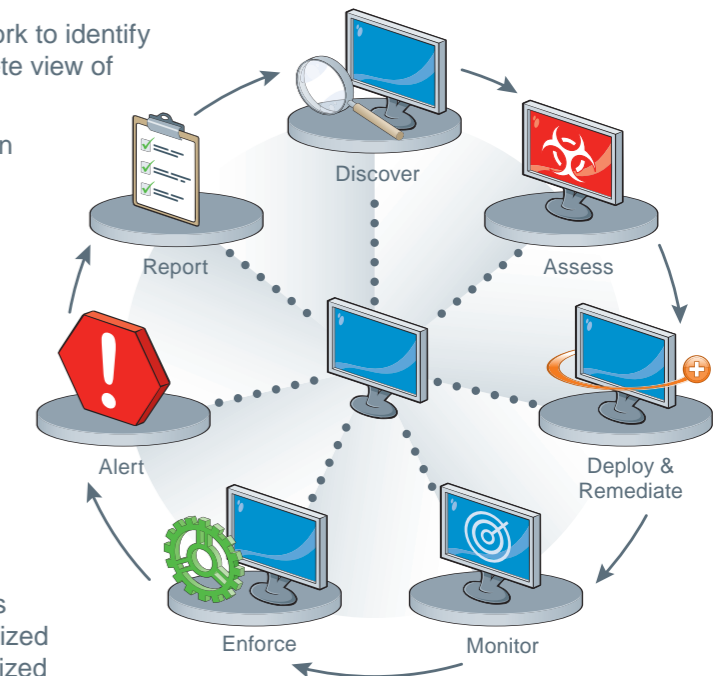
Sanctuary Application Control provides granular, policy-based enforcement of application use to secure your endpoints from malware, spyware and unwanted or unlicensed software. By employing a whitelist approach, Sanctuary Application Control enables only authorized applications to execute on a network server, terminal services server, thin client, laptop or desktop. Unauthorized applications are prohibited from executing. Malware is virtually eliminated and control is given to administrators over unwanted and unauthorized applications, including bandwidth stealing P2P applications. Sanctuary Application Control:

- ☑ Stops attack payloads from executing – targeted attacks, zero day threats, malware, spyware, rootkits, keyloggers, Trojans, worms and viruses
- ☑ Manages and enforces authorized software for the organization
- ☑ Catalogs all applications in the environment
- ☑ Improves user productivity by ensuring only business-appropriate applications are available to staff
- ☑ Reduces IT costs by minimizing the amount of endpoints that need to be rebuilt due to unwanted or malicious executables

## Continuous Endpoint Security

Lumension Security's proactive endpoint security approach is delivered via a comprehensive set of solutions including Vulnerability Management, Data Protection, Application Control, which enable organizations to achieve and maintain their desired security posture.

- 1. Discover** – Discover all assets on the network to identify unmanaged and rogue devices for a complete view of your risk profile.
- 2. Assess** – Assess software and configuration vulnerabilities and the criticality of these issues through network and agent-based scanning and assessment against security best practices policy templates.
- 3. Deploy and Remediate** – Automatically deploy agents to rapidly remediate software and configuration issues based on criticality.
- 4. Monitor** – Continuously monitor endpoints to ensure that your desired security posture is maintained over time.
- 5. Enforce** – Enforce your desired security posture by establishing mandatory baselines for software versions, configurations, authorized applications and devices. Block all unauthorized applications and devices and ensure that only trusted users have access to appropriate technology.
- 6. Alert** – Notify administrators of un-patched or mis-configured endpoints and unauthorized application or removable device access attempts. Deliver notifications to end-users so they understand why they were denied access.
- 7. Report** – Report policy compliance of all endpoints within your enterprise at a summary or detailed level, as it relates to regulatory guidelines, industry standards or corporate governance.



## About Lumension Security

Lumension Security is the recognized, global leader in security management, providing Unified Protection and Control of all enterprise endpoints, applications and devices to more than 5,100 customers and 14 million nodes worldwide. Lumension Security enables organizations to proactively manage risk at the endpoint by delivering best-of-breed, policy-based solutions, including vulnerability management, endpoint policy enforcement and extensive policy compliance reporting.

## Take Control of Your Endpoints

See how you can proactively secure your enterprise endpoints and safeguard data by contacting your local Lumension Security sales representative or reseller by visiting us at [www.lumension.com](http://www.lumension.com).

### Sources:

1. 2006 CSI/FBI Computer Crime and Security Survey
2. "Gartner's Top Predictions for IT Organizations and Users, 2007 and Beyond" Daryl C. Plummer, December 1, 2006
3. National Vulnerability Database, March 11, 2008
4. IDC Worldwide Security Products and Services 2007 Top 10 Predictions
5. Ponemon Institute, 2006 Cost of Data Breach Study
6. John Pescatore, Vice President Gartner Fellow, Gartner Inc.

Best-of-Breed

## PROACTIVE SOLUTIONS TO SECURE ENDPOINTS

- Combined Network and Agent-Based Vulnerability Scanning
- Vulnerability Management
- Security Configuration Management
- Data Protection
- Application Control
- Policy Compliance Reporting