# Lumension® Endpoint Security

## Targeted Threat Protection for POS Systems

Targeted attacks on retail Point of Sale (POS) networks have entered the scene in a big way recently, ushering in what could be the most damaging cyber-crime opportunities to-date. Balancing business productivity and effective endpoint security has always been a challenge but the remote, Internet-connected POS terminals common place in today's retail environment provide an even bigger dilemma for the IT teams tasked with securing them.

Lumension®
IT Secured. Success Optimized.™

## POS Challenges

Recent attacks against large retailers involving POS systems prompted U.S. CERT to issue an alert. (http://www.us-cert.gov/ncas/alerts/TA14-002A) Even with encrypted communication of credit card holder information, an alarming chink in the armor of credit card processing lies within POS systems themselves.

By installing malicious software onto a POS device, an attacker can capture information that is stored briefly within its memory banks. This "memory scraping" technique captures the data stored on the card's magnetic strip the instant it has been swiped at the terminal and remains in the system's memory. Several malware examples specifically designed to target POS systems have surfaced recently in attacks that have successfully compromised global retailers in high-profile incidents. Though the recent incident involving retailer Target may be top of mind to many in the security industry, the FBI has recently issued a confidential warning to all U.S. retailers titled "Recent Cyber Intrusion Events Directed Toward Retail Firms", after an analysis of twenty similar incidents involving malware that targets many retailers' POS terminals.

Key to stopping these "memory scraping" attacks or any type of malware-based attack on POS systems is ensuring only legitimate and trusted applications are permitted to be installed. While anti-virus, patching and network segmentation play a role in a defense in depth strategy for securing POS systems, only application whitelisting can ensure these systems stay free from new variants of targeted malware.

## Stop Untrusted Change

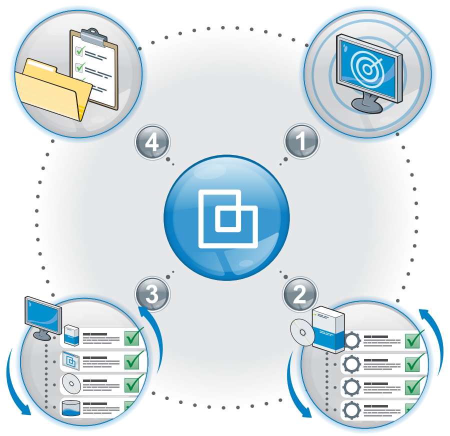
### Neutralize Security Threats, and Prevent Sensitive Data Loss

Lumension® Endpoint Security (L.E.S.) protects retail POS endpoints from both known malware and unknown threats (such as zero-day exploits) while enforcing the use of only authorized software. L.E.S. brings two of Lumension's most advanced security technologies together into one integrated solution. Using Lumension® Application Control, L.E.S delivers advanced application control designed to centrally manage, monitor, and control application installation and use within the POS system environment. Additionally L.E.S. adds an additional layer of protection through Lumension® Device Control that ensures only trusted, externally connected devices such as USB thumb drives can be used, effectively eliminating a commonly used malware attack vector.

Utilizing a centralized whitelist of trusted and approved applications prevents malicious and unintended change without the introduction of operational friction. By scanning a gold image of a single trusted POS system, a centralized application whitelist is created and policies are automatically distributed throughout the POS environment to provide immediate protection. Enforcing trusted change dramatically reduces the risk of targeted attacks against POS systems and improves system performance by reducing unapproved executables. Preventing untrusted, attached storage devices from connecting to endpoints limits the introduction of malware and the accidental or intentional escape of protected data.

Finally, operational management is streamlined by eliminating the unnecessary support calls and performance issues that come with managing unauthorized and unsupported software.

## How Lumension® Endpoint Security Works



**1. Discover:** Scan known gold images to create centralized whitelist images. Verify executables against known hashed provided by application publishers.

**2. Implement:** Assign permissions for applications to run based on executable, user, or user group attributes; use an application whitelist approach to ensure that only authorized and trusted applications can run on endpoints. Block known and unknown malware, targeted attacks, and unauthorized application execution.

**3. Monitor:** Monitor the effectiveness of endpoint security policies in real time and identify potential threats by logging all application execution attempts and recording all policy changes and administrator activities.

**4. Report:** Demonstrate policy compliance and ensure software license compliance by drilling down on suspicious behavior for security or legal follow-up. Report on malware prevention and remediation on behavior of unknown or suspicious code and on current threat levels.

## Take Control of Your POS Environment

Protect your retail organization from threats targeting POS systems starting today. Contact your local Lumension sales representative, reseller or visit us at www.lumension.com.

### Key Features

- Centralized whitelist policy management with global and user/machine specific granularity
- Tamper-resistant, Kernel level agents protect against unauthorized removal
- Proven enterprise-class scalability with load balancing and distributed control
- Attempted attack identification through verbose logging events
- Windows Active Directory and Novell eDirectory support
- Support for Windows POSReady and Embedded Operating Systems XP, 7, and 8

### Key Benefits

- Prevents "memory-scraping" malware from installing
- Disrupts targeted POS attacks from both known and novel malware
- Resists sophisticated, persistent adversaries
- Simplified deployment and maintenance
- Reduce the operational challenges of out-of-bound patches
- Secures removable device use

## Online Resources

- » FREE TRIAL
- » Endpoint Protection Blog
- » Application Scanner
- » Whitelisting Technology Improves Security, Reliability and Performance Via Trusted Change
- » Ogren Group Security Business Analysis - Lumension: A Case Study in Proactively Managing Endpoint Risk
- » Application Security Whitelisting: Keep the Bad Guys Out - Let the Good Guys In

## Contact Lumension

» Global Headquarters
8660 E Hartford Rd
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

**www.lumension.com**

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

Lumension®
IT Secured. Success Optimized.™