Lumension® Endpoint Management and Security Suite

AntiVirus

Prevent Malware from Stealing Data and Disrupting Operations

In today's dynamic threat environment, organizations are challenged with increasing volumes of malware - more than 2 million unique samples are identified each month. Much of today's malware is fueled by financially-motivated cyber criminals trying to gain access to valuable corporate, consumer and/or personal data.

With the enormous variety of malware in the wild today, organizations need an antivirus solution that provides fast and accurate identification of the vast amount of known malware. And with the sophistication of malware continuing to increase daily, organizations need an antivirus solution that employs multiple detection techniques to identify and block unknown malware (e.g. zero-day threats).

Use in Combination with Application Whitelisting to Ensure Defense-in-Depth Endpoint Protection

To prevent these threats from disrupting operations and potentially stealing data, organizations need strong and comprehensive endpoint protection using complementary solutions on different endpoints depending on their security requirements. *Lumension*® AntiVirus provides advanced protection via traditional signature-matching capabilities as well as innovative DNA Matching, SandBox and Exploit Detection technologies which provide proactive protection against zero-day threats. *Lumension*® AntiVirus is available as a stand-alone product or as a module within the *Lumension*® Intelligent Whitelisting™ solution and is delivered on the *Lumension*® Endpoint Management and Security Suite.

Lumension® AntiVirus provides:

- Proven technology that incorporates a pioneering and industry-leading proactive anti-malware engine to block malware such as viruses, Trojans, worms, spyware and more from wreaking havoc on endpoints.
- Removal of identified malware to ensure that any detected malware is not allowed to remain on network assets.
- A complementary offering to other Lumension endpoint security modules that when combined delivers effective defense-in-depth security against targeted and blended attacks

Key Features

- Full Signature Matching Capabilities
- Variant and Exploit Detection
- Behavioral Analysis Detection
- Real-time Scanning
- Scheduled Scanning
- On-Demand Scanning
- Comprehensive Malware Removal
- Automatic Signature Updates
- Integration with *Lumension*® Endpoint Management and Security Suite

Datasheet

Key Benefits

- Complements application whitelisting technology for an effective defense-in-depth approach
- Combines traditional signature-based protection with unique behavioral analysis
- Prevents known and unknown malicious threats (zero-day exploits) from gaining unauthorized access to systems and data
- Ensures comprehensive clean-up, including rootkit removal
- Fully automated detection of endpoints and signature updates
- Integrates with *Lumension*® Application Control and *Lumension*® Patch and Remediation to deliver a unified endpoint security workflow

Detects 100%
of Wildlist Malware with
No False Positives

Key Features

Full Signature Matching Capabilities: Recognizes, blocks, and removes viruses, worms, Trojans and other types of malware such as keyloggers, hijackers and rootkits. Anti-malware capabilities protect your network, endpoints and organization from malicious code which compromises security, privacy and/or performance.

Variant and Exploit Detection: Protects against new and unknown malware (zero-day exploits) via DNA Matching or partial signature matching that detects components of malware that have been re-used from previous attacks and via Exploit Detection, which detects and stops hidden malware that has been injected into otherwise benign file types such as PDFs.

Unique Behavioral Analysis: Delivers another layer of protection via SandBox behavioral analysis which runs suspect executables in a safe emulation to look for malicious behavior and identify sophisticated zero-day malware.

Real-time Scanning: Ensures protection against common malware entryways by enabling malware scanning of files as they are being opened for reading, writing or execution.

Scheduled Scanning: Provides in-depth protection against malware by scanning entire endpoints on a predetermined schedule.

On-demand Scanning: Delivers targeted in-depth assessment and protection by scanning malware on specific endpoints as needed.

Comprehensive Malware Removal: Ensures that any detected malware is removed or quarantined and not allowed to remain on network assets.

Automatic Signature Updates: Allows for automated, attendant-free operation, reducing administrative overhead and improving TCO.

Integration with Lumension® Endpoint Management and Security Suite: Integrates with other Lumension product modules to streamline and improve IT operations and security, reduce agent bloat and improve endpoint visibility.

Supported Platforms

- **Server**: Windows Server 2003, 2003 R2, 2008, and 2008 R2
- **Client**: Windows XP Pro, Windows Vista, Windows 7, and Windows Server 2003, 2003 R2, 2008, and 2008 R2

Complete Requirements

Online Resources

- Lumension® Application Scanner Tool
- Intelligent Whitelisting: An Introduction to More Effective and Efficient Endpoint Security
- Key Strategies to Address Rising Application Risk in Your Enterprise

Contact Lumension

- Global Headquarters
  8660 E Hartford Dr.
  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.™

LAV-DS-EN-07-11-2011