

Prevent Malware from Stealing Data; Disrupting Operations

In today's dynamic threat environment, organizations are challenged with increasing volumes of malware - more than 21 million unique samples have been identified through mid-2009¹. 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).

Ensure a Defense-in-Depth Approach

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. By combining the signature-based blacklisting and behavioral malware detection approaches of Lumension AntiVirus with the proactive whitelisting approach of Lumension® Application Control, a continuum of total endpoint protection for your network is achieved.

Lumension AntiVirus provides:

- » Proven technology that incorporates a pioneering and industry-leading proactive anti-malware engine to provide complete protection against all malware such as viruses, Trojans, spyware and adware
- » Breadth of technology via traditional signature matching capabilities as well as innovative DNA Matching, SandBox and Exploit Detection technologies
- » Complementary solution to other Lumension endpoint protection offerings that when combined delivers proactive protection against targeted and blended attacks needed to safeguard Windows-based endpoints

Key Features

- » Full Signature Matching
- » Unique Behavioral Analysis
- » Comprehensive Cleaning Functionality
- » Full Support for Third Party Management Systems
- » Scalable with Small Footprint
- » Automated Detection of All New Endpoints
- » Remote Endpoint Protection
- » Automatic Signature Updates
- » Easy-to-Use Web-Based Management Console

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 operation, including new endpoint detection, signature updates, and easy-to-use web-based management console

1. Avtest.org, cumulative unique malware samples reported through 24-July-2009

Key Features

Full Signature Matching Capabilities:

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

Unique Behavioral Analysis:

Protects against new and unknown malware (zero-day exploits) via the following methods: **DNA Matching** which provides partial signature matching, **SandBox** which delivers behavioral analysis and safe emulation in a virtual environment, and Exploit Detection which detects malware exploiting vulnerabilities used in document types such as OLE2, MDB, WMF, JPEG, RIFF and SWF.

Full Support for Third Party Management Systems:

Supports email, SNMP, SMS, Syslog, Event log with logging, reporting and alerting capabilities to provide necessary visibility into event and status activities and to allow for integration of antivirus information alongside other network security data for further analysis.

Automated Detection of All New Endpoints:

Searches the network to detect and report new and unknown devices in the environment and reports local network traffic with MAC and IP addresses.

Scalable with Small Footprint:

Meets the security requirements of both small businesses (requiring a comprehensive solution which is easy to install, deploy and manage) and enterprises (needing a solution for securing more complex environments). Optimizes system resources to let organizations conduct operations without disruptions.

Easy-to-Use Web-Based Management Console:

Includes powerful policy-based engine for easy endpoint deployment throughout the organization's infrastructure, with a built-in policy tool that lets the administrator keep the desired security state in groups of clients at all times, a dynamic security level indicator and a current status window, giving the IT administrator instant information about the security state of the network, and adjustment and tuning capabilities, enabling the administrator to trigger important and necessary warnings and alarms.

Remote Endpoint Protection:

Ensures that all endpoints are protected regardless of connectivity to network.

Automatic Signature Updates:

Allows for automated, attendant-free operation, reducing administrative overhead and improving TCO.

Comprehensive Cleaning Functionality:

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

Supported Platforms

- » Windows® 2000 Professional
- » Windows XP
- » Windows Vista
- » Windows 7
- » Windows 2000 Server
- » Windows Server 2003
- » Windows Server 2008
- » Windows Server 2008 R2

[Complete Requirements](#)

Online Resources

- » [Endpoint Protection Blog](#)
 - » Moving Beyond AV
[Webcast](#) | [Whitepaper](#)
-

Contact Lumension

- » Global Headquarters
15880 N. Greenway Hayden
Suite 100
Scottsdale, AZ 85260
+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.

