

“Out-of-the-box” Application and Device Control for Hardware Manufacturers

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 info or intellectual property, protecting corporate endpoints is of utmost importance¹. Endpoints have become the likeliest entry point for malware and are also targeted by cyber criminals and insiders for data theft. In fact:

- ▣ 75 percent of enterprises will be infected with undetected, financially motivated, targeted malware that evaded traditional perimeter and host defenses²
- ▣ 53 percent of organizations would NEVER know what data was on a lost USB device³

Lumension Security’s Award-Winning Sanctuary® delivers seamless policy-based application and device control to proactively secure PCs from threats, including data leakage, malware and spyware. Protecting against known and unknown threats targeting your enterprise customers, Sanctuary enforces a security posture that allows only the known good applications and devices to execute on your hardware devices.

What is “Out-of-the-box” Application and Device Control?

Lumension Security, the worldwide leader in Unified Protection and Control solutions, including the award-winning and industry-renowned Sanctuary Application and Device Control, is working with hardware manufacturers to offer a higher level of endpoint security to enterprise customers.

Sanctuary enables only authorized applications to execute and only authorized devices to be accessed on corporate endpoints. Any applications or devices that are not known and trusted are automatically denied the ability to execute or be accessed.

A pre-installed Sanctuary agent – the software can be installed as a re-branded and dormant agent – puts comprehensive endpoint protection from unwanted applications and devices at an enterprise’s fingertips. This functionality is optional and transparent with the agent remaining silent until an enterprise’s IT Security Administrator initiates a wakeup command.

“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.”

ROB ISRAEL, CIO, JOHN C. LINCOLN HEALTH NETWORK

Benefits to Hardware Manufacturer

By pre-installing Sanctuary onto PCs shipped to enterprise customers, you can:

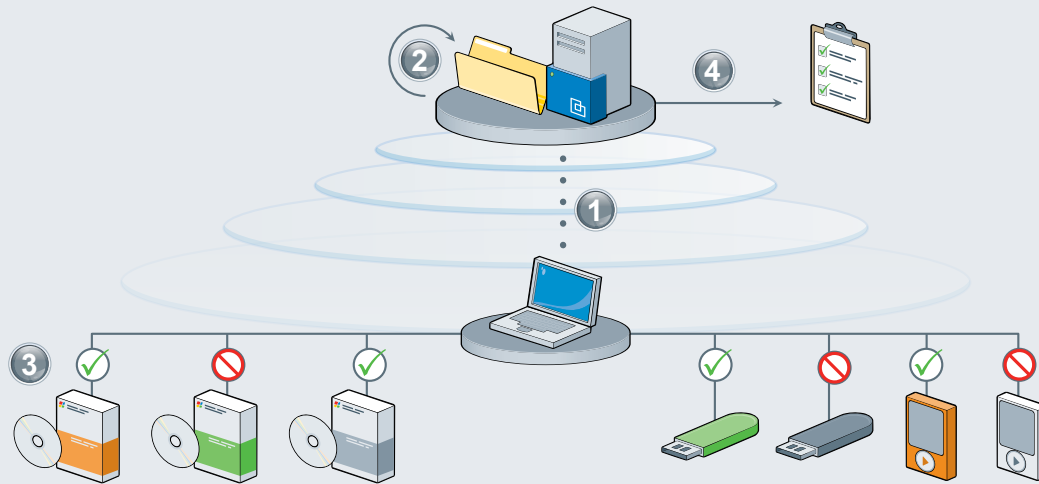
- ▣ **Gain a unique advantage in the market with “out-of-the-box” application and device control for your customers**
Once Sanctuary is turned on by the customer’s administrator, they can seamlessly protect against unwanted applications and targeted malware and they can enforce DLP as it relates to removable media, ensuring that corporate data is properly secured.
- ▣ **Reduce warranty support costs**
With Sanctuary running on your machines, configurations are maintained significantly reducing the amount of machines that must be supported and rebuilt while under warranty. Case in point: With more end users installing non-business related programs and an increased number of threats, 85 percent of corporate machines need to be rebuilt every year.⁴
- ▣ **Enhance perception of your company and products.**
By partnering with an endpoint security leader like Lumension Security, you are standing at the forefront in terms of security for the PC’s that you produce.

1. 2006 CSI/FBI Computer Crime and Security Survey
2. Gartner Research, “Gartner’s Top Predictions for IT Organizations and Users, 2007 and Beyond,” Daryl C. Plummer, December 1, 2006
3. Ponemon Institute, 2006 Cost of Data Breach Study
4. Yankee Group Security Leaders and Laggards Survey, 2005

Top 5 Benefits to Hardware Manufacturer's Customers

1. **Data Leakage Prevention (DLP) Capabilities** – Sanctuary removes the risk of data theft or data leakage as a result of unwanted and unauthorized applications and devices.
2. **Protection Against Malware and Unwanted Applications** – Sanctuary prevents the execution of unknown/malicious code including malware, spyware, zero-day threats and all other destructive viruses.
3. **Compliance with Industry Standards and Government Regulations** – Sanctuary enables your customers to comply with evolving regulations governing privacy and internal controls (i.e., Sarbanes Oxley, HIPAA, GLBA and more).
4. **Maintenance of Enterprise IT System Integrity** – By denying all unknown and unwanted applications and devices, Sanctuary ensures proper configurations and improves IT system performance and network bandwidth.
5. **Employee Productivity Improvements** – Sanctuary enables organizations to allow only the applications or devices that are required for employees to accomplish their daily job requirements.

How It Works



1. Discover: Identify all executable files and devices, collect profiles and organize into pre-defined file groups.

2. Develop: Assign rights to execute based on executable and device attributes as well as user and/or user group attributes.

3. Enforce: When a user wants to execute an application or access a device, the OS request at the kernel level is intercepted by the Sanctuary driver. All of the policy enforcement is completely transparent to the end user.

For applications, the signature generation and verification occurs and is compared with the central or locally authorized list of approved files. If there is no match between the executable file and the central or locally authorized list of approved files, then file execution will be denied. If the file does match the list of approved files it will be allowed to execute.

The same concept applies to devices. The driver checks the user rights in the Access Control List (ACL) for the device class or the specific device. If the user has rights, then access will be granted. If the device is not known or if it is known, but the user does not have rights, then access will be denied.

4. Audit: Sanctuary logs all application execution and device access attempts, logs all administrator actions, and logs all data written to/from a removable device.

How to Participate

To participate in Lumension's Hardware Manufacturer's Endpoint Security Program and deliver additional value to your organization and your customers, contact the Lumension Security Business Development team at BusinessDevelopment@Lumension.com.



Lumension Security

15880 N Greenway-Hayden Loop, Suite 100 / Scottsdale, AZ 85260 / 480.970.1025 / www.lumension.com

© Copyright, 2008 Lumension Security. All rights reserved. Lumension Security, the Lumension Security logo, and the PatchLink and Sanctuary product names and logos are either registered trademarks or trademarks of Lumension Security. In addition, other companies' names and products mentioned in this document, if any, may be either registered trademarks or trademarks of their respective owners.