

Say Goodbye to DATA LEAKAGE & MALWARE

Protect Against Data Leakage and Malware
with Policy-Based Endpoint Security



Endpoint Security Solution

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 your endpoints is of utmost importance¹.

Fortunately, there is a way. Lumension Security's Common Criteria EAL2 Certified Endpoint Security Solution delivers policy-based application and device control that proactively secures your organization from data threats, including data leakage, malware and spyware.

Lumension's Sanctuary® enforces a security posture that allows only the known good applications and devices to execute on network servers, terminal services servers, thin clients, laptops or desktops:

- ☒ Removing the risk of data theft or data leakage as a result of unauthorized applications and devices
- ☒ Preventing the execution of unknown/malicious code including malware, spyware, zero-day threats and all other destructive viruses
- ☒ Enabling compliance with evolving regulations governing privacy and internal controls (i.e., Sarbanes Oxley, HIPAA, GLBA and more)
- ☒ Maintaining IT system integrity and improving IT system performance and network bandwidth
- ☒ Reducing endpoint security TCO
- ☒ Improving end user productivity

Application and Device Control for Your Endpoints

Enterprises today are constantly challenged with security and support issues arising from endpoint users and their laptops and PCs. Sanctuary provides endpoint security with a simple and unique Positive Security approach that enables only authorized applications to run and only authorized devices to connect to a network server, terminal services server, thin client, laptop or PC. Offering the best of both worlds, Sanctuary facilitates security and systems management and provides necessary flexibility to the organization.

Protecting against known and unknown threats targeting your enterprise, Sanctuary combines the proven capabilities of its application and device control modules, providing organizations with the only endpoint security solution to centrally manage, monitor and control applications and devices on the corporate network.

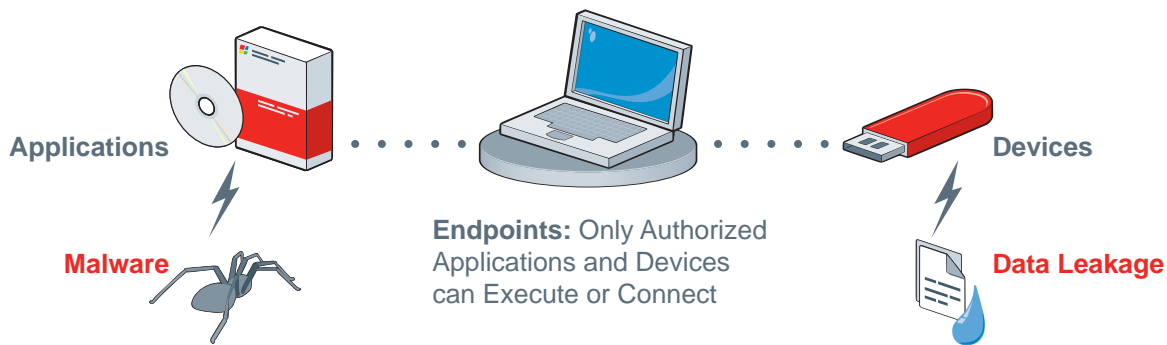
Solution Overview

Removes the risk of data leakage, malware and spyware, improving IT security and network bandwidth. Reduce the effort and cost associated with supporting endpoint technologies and assure regulatory compliance.

☒ Total Control of all Removable Media, Endpoint Peripheral Devices and Port Access

☒ Complete Prevention of Malware and Unwanted Applications

☒ Comprehensive Policy Enforcement of Application and Device Use



Sanctuary® Application Control

Provides policy-based enforcement of application use to secure endpoints from threats, such as malware and spyware, as well as unwanted or unlicensed software.

Sanctuary® Device Control

Provides policy-based enforcement of removable device use to control the flow of inbound and outbound data from your endpoints.

The Endpoint Security Challenge

The security landscape is shifting from large, widespread attacks at the enterprise perimeter, to targeted threats focusing on corporate endpoints, which are traditionally less secure. Most data leaks and security threats – inadvertent or intentional – occur at the endpoint and many of these are generated internally.

Unmanaged removable media and applications that reside on endpoints can easily bypass traditional security methods and open the floodgates for data to escape into the wrong hands. Traditional security solutions have been unable to stem the tide of these ever-increasing endpoint security threats because they react to symptoms after a threat has propagated, as opposed to proactively stopping it in its tracks.

In fact, 62 percent of enterprises which rely on anti-virus solutions, suffered an infection². Furthermore, 70 percent of all computer attacks, IT security breaches and data thefts are generated from within the firewall², proving that endpoints are the likeliest entry point for malware. Today, security threats such as malware can also be introduced via removable media at the endpoint.

By enforcing application and device use policies, you can secure endpoints from becoming a doorway for sensitive data to escape and for security threats such as malware to enter. It is easy to block known security threats from your network - it is the hidden threats lurking on the endpoints that require a different approach.

Comprehensive Policy Enforcement

Sanctuary validates applications and removable devices as they are used within an enterprise. By employing a positive model approach, Sanctuary enables only authorized applications to run and only authorized devices to connect to laptops, PCs, servers, terminal services servers and thin clients. By default, unauthorized applications

cannot execute and unauthorized device access is prohibited. Sanctuary policies are managed per user or user group as well as per computer.

Simple, Fast, Flexible Administration and Management

Through a central console, application and device control policies are quickly established and enforced through two simple steps. Sanctuary enables the administrator to rapidly identify devices and applications and then assign permissions at a high level or all the way down to device class, specific device or application to users, user groups or a particular computer. Sanctuary links application and device policies to user and user-group information stored in Microsoft® Windows® Active Directory™ or Novell® eDirectory™, dramatically simplifying the management of endpoint application and device resources.

Automated Discovery of Applications and Devices

Sanctuary enables discovery of applications and devices in use through a non-blocking audit option, as well as through a variety of scanning tools to assess the current state and simplify policy definition and management.

Granular Device Control Permission Settings

To eliminate the risk of unauthorized devices from connecting to the network, device policies are enforced by time constraints, encryption, volume of data, data transfer and more. Sanctuary also controls the types of files moved to and from removable devices to reduce the risk of unwanted files from entering and sensitive files from leaving the network. Separate policies can be defined and enforced when the user is online or offline.

Enforced Encryption

Removable media can be encrypted for safe use and transportation without the fear of exposing your confidential data to unauthorized users. Users can have access to

their encrypted data even on computers that do not have Sanctuary client software installed. Centralized and decentralized encryption schemas provide the flexibility to centrally encrypt removable media or enable users to encrypt removable media on their own and, more importantly, enforce the use of that encrypted media.

Flexible Authorization Rules

Administrators can allow trusted users to authorize their own applications. This option provides ultimate flexibility, while alerts keep the administrator informed.

Detailed Audit Capabilities

Sanctuary's patent-pending I/O bi-directional Shadowing tracks filenames or file content as it is read from or written to floppy, CD/DVD and removable devices. All application execution and device access attempts can be logged and reviewed with flexible filter, sort and display options and stored custom query templates. Administrator actions,

including changes in policy settings, are logged ensuring a full audit trail of policy enforcement.

Proven Security

Sanctuary is impenetrable because it is deployed at the kernel driver level. Users cannot turn off Sanctuary or bypass it in any way.

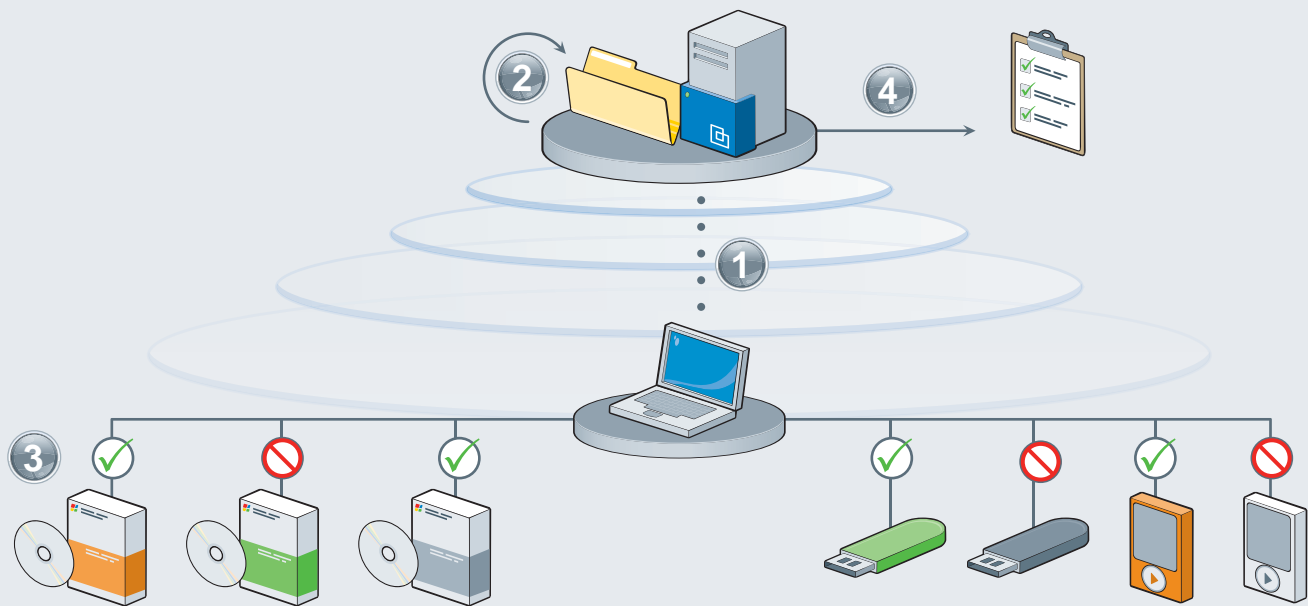
Enterprise Scalability

Designed to scale to large and complex environments, Sanctuary employs a three-tier architecture with database, application server(s) and client.

Common Criteria EAL2 Certified

The Common Criteria Evaluation and Validation Scheme (CCEVS) has asserted that Lumension's Endpoint Security solution complies with the specified security 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.

Add-on Products

Sanctuary® Application Control: Server Edition

Provides server security software that enforces application use policies to secure mission-critical servers (i.e. mail servers, CRM applications, web and other critical database servers) from unauthorized, illegal or unwanted applications by default and preventing any interruption to the flow of your business.

Sanctuary® Application Control: Terminal Services Edition

Enforces application use policies to secure business-critical Windows or Citrix terminal services environments from unauthorized, illegal or unwanted applications by default.

Sanctuary® for Embedded Devices

Enabling simple and effective control of an organization's entire Windows embedded devices network configuration from one central location. Sanctuary offers advanced device and application policy enforcement solutions for thin client devices based on Windows Embedded for Point of Services (WEPOS) and Windows XP Embedded platforms, such as Retail Point-of-Sale Terminals, ATMs, Gaming Devices, Thin Clients and other Network Connected Systems.

Also available from Lumension

Lumension's Vulnerability Management Solution enables organizations to effectively manage the entire vulnerability lifecycle through an actionable, enterprise-wide Vulnerability Assessment scanner and the #1 ranked Patch and Remediation solution, all unified under a central management and reporting console.

About Lumension

Lumension Security is a leading global security management company, providing unified protection and control of all enterprise endpoints, applications and devices to more than 5,100 customers and 14 million nodes worldwide. Lumension enables organizations to effectively 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 enforce acceptable application and device use throughout your enterprise by contacting your local Lumension sales representative, reseller or by visiting us at www.lumension.com.

What Our Customers Are Saying

"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."

John C. Lincoln Health Network

"Sanctuary Device Control ensures that no device, unless authorized, can ever be used, no matter how it gets plugged in. Device Control is a really strong, easy to use product which is why Barclays chose this solution."

Barclays

"Sanctuary enables me to explicitly list the applications that are allowed to run on our bank's machines. All other executables - including any malicious code - simply will not run. With Sanctuary, I can stay ahead of potential challenges, providing peace of mind for the bank's executives and auditors, and ultimately, our customers."

First National Bank Bosque County

Sources:

1. 2006 CSI/FBI Computer Crime and Security Survey
2. 2005 Yankee Group Security Leaders and Laggards Survey



Lumension Security
15880 N Greenway-Hayden, Suite 100
Scottsdale, AZ 85260
480.970.1025 \ www.lumension.com

©2007 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.