

Lumension Application Control™ (FORMERLY SANCTUARY)

Prevent Unauthorized Software and Reduce Endpoint Security TCO with Application Whitelisting

The battle to protect the IT assets from malware and unauthorized software is a costly, ongoing struggle taking up valuable resources and time.

Each time a new malware threat appears or unsupported software causes a compatibility conflict, IT has to stop what they're doing to resolve the issue. Whether that's updating antivirus signatures to ensure that systems and information are protected or re-imaging laptops due to software conflict blue-screens, the end result is an increased support burden and lower operational efficiency.

Secure Endpoints, Servers, Kiosks and POS Systems from Malware

The threats aren't going to stop and antivirus software alone cannot control the problem as malware threats are being developed faster than the necessary fixes. Malware has grown over 500% with more than 5.49 million unique samples of malicious software in 2007¹ and 2008 has seen the rise of targeted attacks, which are now being designed to specifically bypass antivirus solutions.

Lumension Application Control enables you to prevent the execution of malicious code utilizing application whitelisting. This approach allows only authorized applications to run on laptops, PCs, servers, terminal services servers and thin clients without relying on antivirus signature-updates, freeing up network bandwidth and IT resources.

With no viral attacks to thwart, malware to hunt down, or incompatible applications to invoke the blue screen of death, you can spend more time on more strategic activities instead of constantly fixing computers.

Lumension Application Control provides:

- » Endpoint protection from malware without relying on signature updates
- » Optimized IT support with decreased helpdesk calls to support unauthorized software
- » Improved system availability and service levels by preventing known and unknown threats
- » Audit-readiness with detailed tracking of all application execution attempts and policy changes

Key Features

- » Application Whitelisting
- » Automated Application Discovery
- » Standard File Definitions
- » Automatic Authorization of Software Updates
- » Script / Macro Protection
- » Flexible File Authorization
- » Local Authorization
- » Spread Check
- » Offline Computer Protection
- » Active Directory and eDirectory Support

Datasheet

Key Benefits

- » Prevents Known and Unknown Threats
- » Blocks Targeted Malware and Zero-Day Attacks
- » Enforces Trusted Application Environment
- » Improves Server Availability
- » Reduces Endpoint Security TCO

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

Brent Rickels, VP Technology,
First National Bank of Bosque County

