

Lumension Endpoint Protection Solution

Whitelisting Technology Improves Security, Reliability, and Performance via Trusted Change

The Need for Proactive Security

In most organizations, computers, applications, PDAs, smart phones, and data storage peripherals serve as the nervous system of daily business. Applications that track a company's financials, supply chain, and human resources are essential; every employee uses information technology (IT) daily to complete some aspect of their job.

The reliance of people and businesses on IT creates its own challenges. In many organizations, employees can peruse web sites, send and receive email, download software, and install applications whenever they want. On the one hand, such openness helps business flow by empowering workers to use information freely; on the other, it can risk the security and integrity of both computers and data.

Each day hundreds of new security threats emerge via email viruses, website malware, rogue applications, lost and/or stolen storage devices, and malicious attacks. A thumb-size flash drive can siphon gigabytes of business and personal data in seconds. More recently, smart phones – their use often uncontrolled or unauthorized by corporations – make it easier than ever to tap into an organization's information resources. Despite the benefits of information technology, its ubiquity and rapid pace of change can become a security and privacy threat, not to mention a management burden.

As organizations grapple with the advantages and challenges of IT everywhere, they are faced with the choice of locking down an entire infrastructure or continuously defending systems against resourceful hackers, uninformed users, data leakage, and poorly implemented applications.

Anti-virus Programs Are Only the First Step to Security

Often the first defensive step is to turn to anti-virus and anti-malware protection software. At first, these programs perform a thorough cleaning of existing virus and malware infections, returning the systems to a relatively stable state. However, they are typically just behind the hacker curve. Computers are vulnerable to newly released viruses or attacks until the malware code is identified and the anti-virus agents are updated on every machine – a process that can take days if not weeks. Using these methods makes a “zero day attack” almost impossible to prevent using anti-virus software.

In terms of data security, people are often their own worst enemies. They inadvertently circumvent existing barriers by downloading and installing unsanctioned applications which contain malware. Some of the most insidious malware can turn entire departments of computers into zombie machines, running background programs that carry out widespread attacks or tap into business communications and databases. Infected computers must be completely wiped and rebuilt to rid the PC of malware, causing downtime, overloading IT, and diminishing productivity.

Anti-virus software is the best option for keeping systems clear of existing threats. Keeping up with the hacker's most recent threats is more difficult, however. Preventing human error, such as installation of rogue applications, is not the forte of anti-virus software. The alternative – ensuring that only approved and valid applications run on every computer – requires a shift in mindset of IT professionals from playing defense to playing offense with endpoint security.

The Whitelisting Paradigm Shift

Traditional approaches to endpoint protection have become less effective in today's dynamic computing environments. Battling the onslaught of viruses, malware, and poorly designed applications has become a reactive game. To escape this mode of always being one step behind emerging threats, you need a new endpoint security model that includes whitelisting. Whitelisting provides a model to strengthen your endpoint security by making the shift from focusing only on known bad applications (threats) to only permitting what is known to be good.

Identifying what applications you currently have installed and the ones you need to allow is half the battle to a whitelisting deployment. Whitelisting allows you to define and authorize necessary applications for your environment. Any other applications not defined in the whitelist are automatically blocked through a virtual blacklist. Simply stated, any executable – whether a business application, a video driver, or a web browser plug-in – not specified on the whitelist cannot load and run on any

endpoint in your network. Controlling exactly which applications can run on each computer keeps your critical information secure while offering many other benefits. Many organizations are now taking another look at whitelisting as a means to fortify their existing anti-virus deployments and strengthen their overall endpoint security.

Attain Benefits beyond Security

Whitelisting is the best way to prevent direct harm to computers from viruses and malware, but comprehensive application whitelisting – like *Lumension®* Endpoint Protection – offers many more benefits to organizations and the IT environment:

» Increased performance and stability

When only authorized applications can run on a computer there is far less chance that inappropriately installed programs or hardware drivers will corrupt an operating system. Combine Lumension Endpoint Protection with *Lumension®* Vulnerability Management, to ensure that endpoint patches and updates are rolled out in a uniform and approved manner, ensuring that all computers operate on the same release level.

» Control of computer and network utilization

Computers have a tendency to become cluttered with junkware, games, and web software that consume computing resources and network bandwidth. Whitelisting offers a way to keep such programs from interfering with business operations.

» Decreased IT support costs

With minimal viral attacks to thwart, malware to hunt down, or incompatible applications to threaten network security, IT can spend more time and resources on improving operations, reliability, and accessibility which results in greater productivity.

» Increased data security and compliance with privacy laws

Preventing unauthorized programs from running on any computer reduces the likelihood for spyware, keyloggers, and hackers to steal passwords, address books, customer files, or other sensitive data from otherwise physically secure computers. Combined with *Lumension*® Data Protection, which prevents sensitive information from leaking out through lost or stolen storage devices, whitelisting creates a stronger infrastructure leading to greater compliance with privacy regulations.

Another side benefit to application whitelisting is a better understanding of your IT environment. A whitelisting deployment requires you to identify what applications your employees are running on their desktops and which ones are really necessary to your operations. You may discover that you buy more bandwidth than is really needed to conduct business. Getting an accurate view of IT application usage is the first step to controlling your information flow and increasing endpoint security.

Understanding Your Application Environment

If a CIO were to envision a perfect IT environment, it would no doubt differ from what most organizations have today. The environment would be controlled with consistent change-control systems. Updates and operating system patches would be rolled out uniformly across a homogenous network. Every computer would have a specific set of applications preinstalled. Users would have no local authority to install, update, or delete applications, drivers, or web plug-ins. Only approved storage devices and media could be used to copy and transport data.

In such a tightly managed computing environment, anti-virus and whitelisting programs might not be needed. However, this scenario represents an environment rarely found in the real world – and not really consistent with actual user needs.

Real-World Challenges

A totally locked down computing environment is not only rare – it is unlikely to meet your business needs. A system with complete top-down control loses the flexibility to quickly add and upgrade applications and business systems. In organizations where communication and creativity fly fast and furious, locked-down systems can frustrate and stifle business. And while such a setup may seem convenient for a security department, it ultimately adds labor-intensive work for system administrators and help-desk operators.

So, what's your environment like today? Small organizations tend to have limited IT departments and often give users local administrative control of individual PCs. Though such a policy lessens the initial burden on IT, as the company grows so do the ranks of new end users. They often install rogue applications – sometimes corrupting files and registries in the process.

Perhaps your organization has evolved to become an infrastructure with uneven change control, resulting in a mishmash of service packs and application versions, sometimes running on the same computer. Unauthorized applications and preloaded junkware clog hard drives and reduce network bandwidth. Malware and viruses continuously creep in through downloads and external website visits. The anti-virus software you installed can't keep up, and you are constantly rebuilding corrupted PCs. Sudden spikes in unauthorized application-generated traffic overload the network at critical times, forcing you to contract for more bandwidth than you really need.

Is this an accurate view of your world? Your scenario may be slightly better, or worse, but the general situation remains the same. You need a way to categorize all the applications on all the computers in your network, and then decide which should be allowed to run.

White Vs. Black – With a Little Bit of Gray

Whitelisting simply means defining what is “good,” then allowing only good programs and processes to load and execute in memory. Every application not on the whitelist – the virtual blacklist – cannot run, period. To increase flexibility, especially at the beginning of a deployment, you can extend the concept of trusted change by implementing a gray-list. This permits safe but potentially undesirable programs to run until you decide whether they are really needed.

Whitelisted applications run without being blocked. Graylisted applications can launch with logging that notifies you when and where they are running. Anything else cannot run at all. Even corrupted or hacked applications on the whitelist are recognized as altered, and are prevented from running. Zero-day attacks orchestrated through malware, worms, and Trojans are automatically prevented from running because they will not be on the whitelist, and therefore never get the chance to launch and corrupt a system.

Four Phases of Implementing a Whitelisting Solution

Now that you understand the benefits whitelisting, let's look at how a whitelisting solution can work in your organization. The deployment process consists of four phases:

1. Discover and control the application ecosystem
2. Roll out pilot clients
3. Enforce protection
4. Fine-tune the application ecosystem

Whitelisting Phase 1: Discover and Control the Application Ecosystem

To begin a whitelisting project, you must first understand your application environment by discovering and defining the set of applications required for your business to run. These applications, with supporting files and drivers, represent the contents of your “gold standard” PC and your initial whitelist.

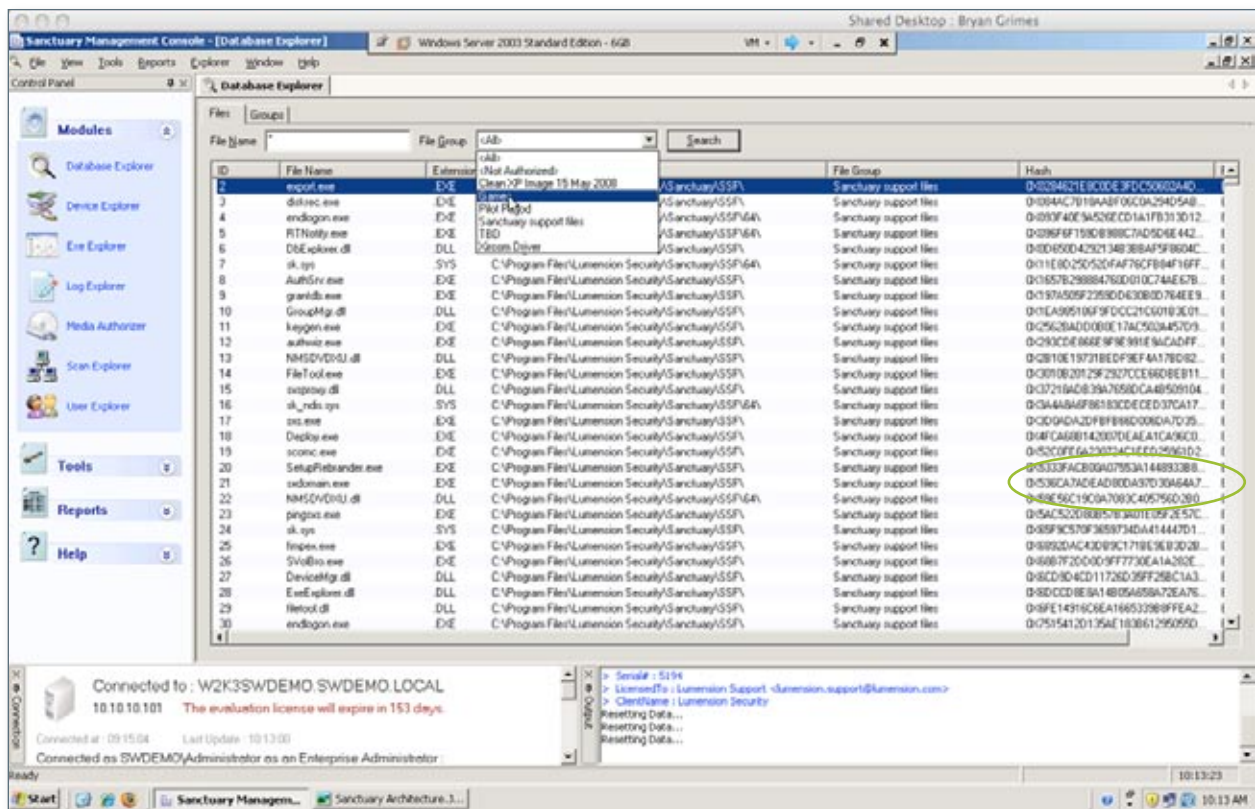
Typically, the gold-standard PC represents a “clean machine,” one never used for business or connected to the Internet but loaded with all applications normally deployed to employees. It includes the operating system, patches, service packs, and third-party applications such as Microsoft Office, Acrobat Reader, WinZip, Explorer, and any anti-virus or communication software (e.g., WebEx)

that employees use on a regular basis. Also, a gold standard PC will contain applications used by specific departments, such as accounting or CAD software. If your organization uses next-generation web-based applications such as Salesforce.com, you must also include any client agents that plug in to the browser.

To help build your definitive whitelist, Lumension Endpoint Protection includes several tools. Scan Explorer and Authorization Wizard help you scan and catalog your gold-standard PC and any future configurations you may add to the whitelist, including:

- » Installation CDs, DVDs, and file servers
- » Local and network hard drives for all executable binary files
- » Hardware (video, printer, media storage) drivers

Continued »



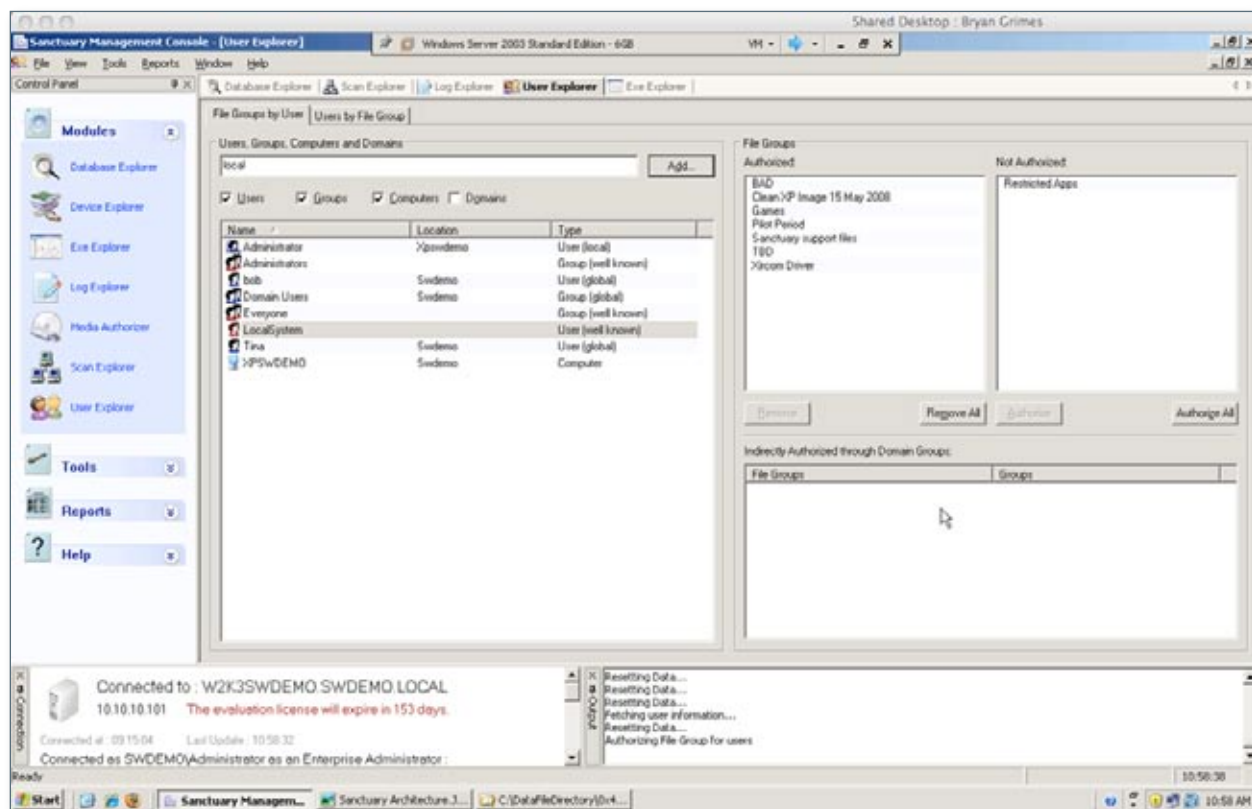
A unique SHA-1 signature is calculated for each binary file, together with the filename, path, size, and product version. This information is recorded on the Lumension server whitelist, defining what programs can run on all selected computers.

During the scanning process, each application file is defined with a unique hash number that enables the system to detect when corrupted or hacked, or when different versions of programs attempt to execute. The master whitelist is stored on a secure server, with an encrypted copy stored locally on each PC. Each time an application is launched, the local whitelist is checked for permission to execute. When there is no need to search internet databases to verify application use, performance overhead is undetectable and checks may be made even when the computer is offline.

Assign User Access

After initial scans using Scan Explorer, the whitelist should include 70 to 90 percent of all valid binaries found on all end-user computers. These files are added to the approved “Corporate” file group on the whitelist.

Next, employ the User Explorer module to define groups of users and add permissions. The scanned files are initially added to the “Everyone Group.” At this stage, everyone can run all applications contained in the whitelist. Later, you can fine-tune which groups can run specific applications.



The User Explorer module lets you use the Microsoft Active Directory to map users and groups to the whitelist.

Lumension Endpoint Protection offers granular control of the processes authorized to execute on managed devices. Whitelisting can be deployed with different levels of blocking modes. You can choose to extend trust to applications based on several factors including:

- » Known approved applications
- » Source and signature
- » Who (local or admin) or what agent (WebEx update, Norton AV agent) is trying to install them
- » Who created them: Microsoft=always allow; Microsoft=always deny
- » Trusted scripts and macros allowed to run with user permission

If you enable this high level of control, the best approach is to integrate whitelisting management with IT change management processes that can update files on managed PCs and servers. From this phase on, do not deploy or install any new or updated applications, drivers, OS patches, or other executables onto endpoint computers without first adding them to the whitelist. You can either add the updates and patches to a clean image build that is then rescanned, or use the Authorization Wizard tool to scan the patch sources. This integrates Lumension Endpoint Protection Solution into your overall change management process.

Whitelisting Phase 2: Roll Out Pilot Clients

Once your gold-standard whitelist is populated with approved applications, drivers, and plug-ins, you are ready to deploy the Lumension Endpoint Protection Agent to a group of PCs of similar purpose and build. This is the pilot and precursor to the wider rollout of all PCs and servers.

Define Your Pilot Group

The pilot group will test the completeness and accuracy of your gold-standard whitelist. Choose a department or group of similar users for your pilot. Avoid IT and development PCs for now, as they often use non-standard configurations and code development constantly changes runtimes that would be blocked by the standard whitelist.

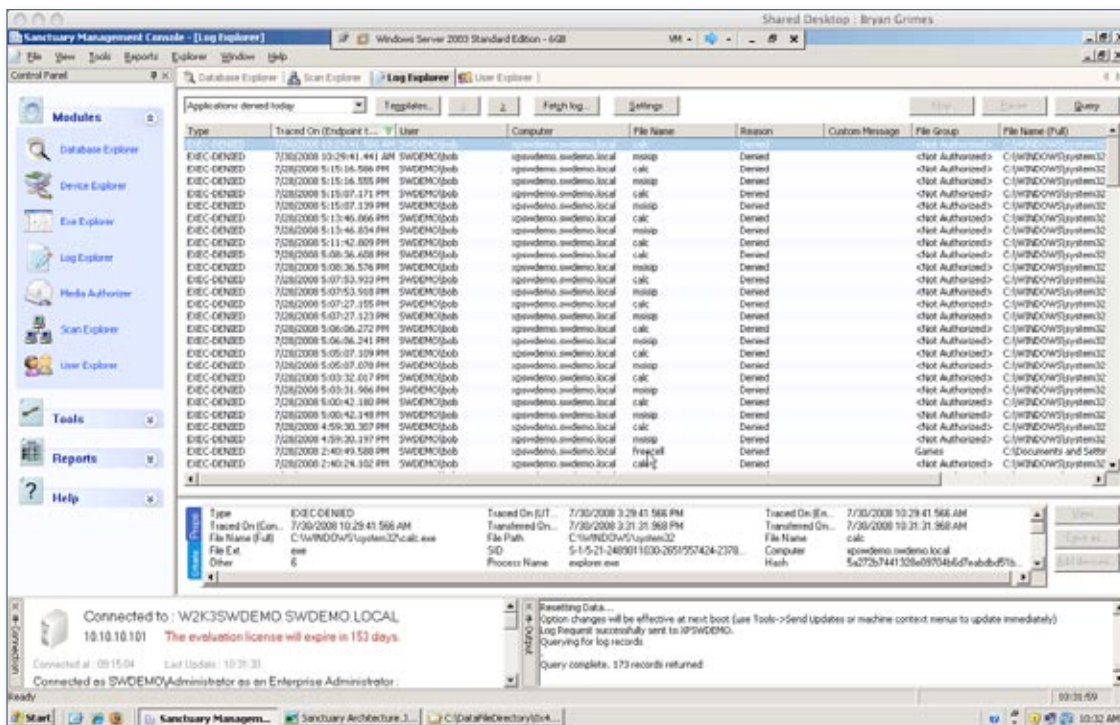
To prevent abrupt interference of operations, deploy the Endpoint Protection Agent in non-block-

ing mode. In the Endpoint Protection Management Console, enable the Execution Logging and Access Denied Logging functions.

Monitor the Exception Logs

During the first one to two weeks of the pilot phase, review the exception logs daily to identify active applications not currently on the whitelist. Be sure to include logging times when periodic applications – for example, month-end accounting programs – are run.

As the system finds and logs applications not on the whitelist, decide which to add and which to deny once full blocking mode is turned on. Make note of multiple versions of applications (e.g., Acrobat Reader 8 and 9) that must be added separately to your whitelist. For files that aren't readily identifiable, the file path displayed in the log results can often help identify the parent application.



Exception logs show what applications are running that are not on the whitelist.

Define a Graylist

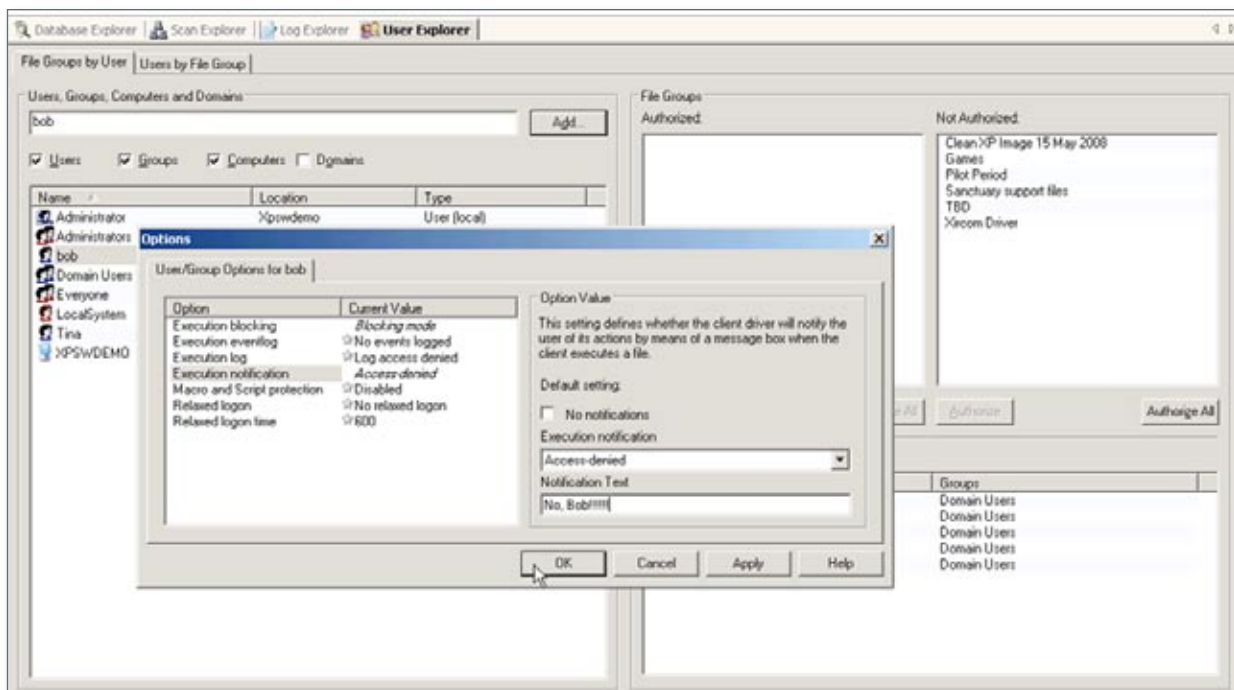
Depending on the size of your pilot and how long the PCs have been in the hands of users, there will be exceptions that are difficult to identify. For files that require additional research or need to be approved for use, place them on a graylist (a separate group) assigned to the “Everyone Group.” This prevents interruptions when blocking mode is turned on. Once you determine whether a graylisted application is needed or desired, either move it to the whitelist or remove it from the graylist, ending its ability to run.

Educate Your Users

As you expand beyond the first pilot rollout, which most likely involved a small group of savvy users,

you must start educating personnel on which applications are approved for use and which are not. This is a continuous process, especially if employees are used to managing their own PCs – that is, if they have local administrator control – and therefore have been able to add programs as they please. Unauthorized programs will stop running when the system is in full effect.

If you have not prepared your employees for this change, your help desk will soon let you know about it. Use the Lumension Endpoint Protection Manager to design explanatory alerts that display when users try to run prohibited applications. This reduces the immediate desire to call for help when a favorite – but now banned – application won't launch.



Use warning messages to explain why applications won't run after blocking is turned on – perhaps with more information than “No, Bob!”

Roll Out to New Groups

As the exception log for the initial pilot group shrinks, you can roll out the client to an expanded group. Monitor the exception list daily for errant applications, adding to the whitelist or graylist as needed.

The exception log should grow shorter with each expansion of the pilot. Repeat the expansion until all PCs have Lumension Endpoint Protection Agent installed, and all exceptions have been logged and added to either the whitelist or graylist.

The volume of the logs from each new group will give you an indication of how many machines to add at a time. The fewer the exceptions, the larger the group you can add. The process of ferreting out exceptions should grow easier each time you expand the pilot.

Whitelisting Phase 3:

Enforce Protection with Blocking Mode

Once all clients are deployed and exception logging has largely subsided, begin to turn on blocking mode in phases, in the order that you first rolled out the solution.

This is where your education efforts will pay off – users will expect specific applications not to run. They will know to call the help desk if important but perhaps overlooked applications do not work properly, perhaps because all components were not fully included on the whitelist.

After you turn on blocking mode, there may be an occasional denial of an application not previously encountered, such as a seldom-run process. When this happens, use the log from those affected machine(s) and assign the application binaries to the whitelist or graylist as in the pilot deployment.

Most PCs will now be running only the applications on the whitelist. Applications on the graylist should be researched and added to the whitelist if prudent. All other unapproved applications – including malware, junkware, and viral programs – are on the virtual blacklist and cannot run.

Congratulations. You have control of your IT resources again.

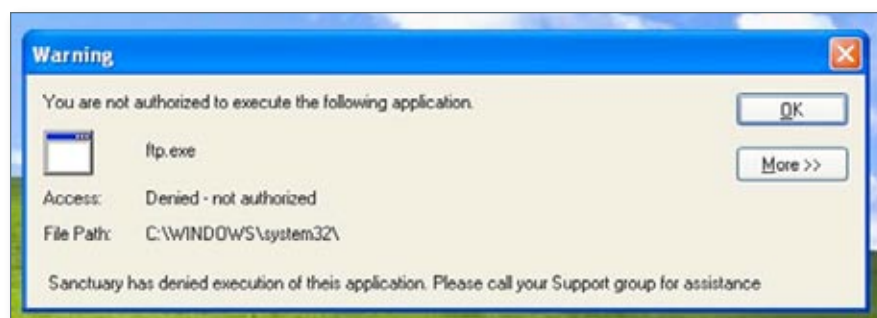
Whitelisting Phase 4: Fine-Tune the Application Ecosystem

Once you have regained control of your PCs through application whitelisting, you're ready to begin fine-tuning and optimizing the whitelist. Lumension Endpoint Protection offers a very high degree of control over user access, system-level executions, and auto-updates.

User Access Control

You can group applications by role or user group to limit the use of certain applications to specific personnel. First identify executables and reassign them to new groups. This could be as simple as assigning the Windows game executables to a group such as "Holiday." Or you could reassign the top-level executable for a third-party application, such as Skype, to only specific users and/or user groups. (The child process DLLs and sublevel executables can remain in the main file group.)

When users try to launch an application not on the whitelist or graylist, they will see a visual notification on their screen that explains why the application cannot run. The attempt to run an unauthorized application will also be logged at the security console.



You can write custom warning messages for users when they attempt to launch an application that is not on the whitelist.

System-Level Access Control

You can restrict the ability of the Local System account to execute valid OS binaries – such as telnet, ftp, CMD, or control panel applets – without the local user giving secondary permission. For example, if a Trojan virus previously on the machine tried to run an FTP connection in the background, the local user would receive a warning message. If there is no user response, the process is blocked and logged in the management console. Alternately, if the user has a reason for running the process, he or she can allow it with permission.

Path Rule Exceptions for Auto-Updating Services

Some legitimate applications attempt to auto-update online following their own schedules. For example, WebEx updates its Meeting Manager, or an anti-virus agent updates the AV engine files, using the web. To allow such updates, define a path rule to the source files that is exempt from blocking. For applications that are called from a file server but changed frequently, a path rule can permit access to applications or specified files called from a predefined file path.

Lumension works continuously in the background to give you control over your application ecosystem.

As you become more experienced with Lumension Endpoint Protection, you will be able to hone your system to maximize efficiency of blocking or permissions while maintaining the flexibility of your IT infrastructure and your business processes.

Expand Your Control with Lumension

With Lumension Endpoint Protection, whitelisting guards your systems by allowing only approved processes and applications to run on the endpoint. Whitelisting protects your systems against malware and viral programs while improving total data security and overall system performance.

Adding Lumension Data Protection for device control lets you manage removable storage devices and stop leakage of sensitive information. Though malware is a significant cause of data theft, data can also be lost, misplaced, or intentionally stolen while at rest on physical storage devices. The ease and speed with which gigabytes of data can be copied to a thumb drive, for example, requires a security solution that controls not only what devices can

be attached to a computer but how much data can be copied at a time and whether it is encrypted. Lumension Data Protection provides that control, and offers detailed forensics of who is moving data and where. It's a perfect complement to application whitelisting.

Organizations are realizing that anti-virus and anti-malware software can protect their networks from known threats. But keeping pace with emerging threats is not possible in today's Internet-driven business environment. The next step in fighting cyber threats and enhancing endpoint security is to deploy a whitelisting technology only allowing known good applications to run. Lumension Endpoint Protection delivers the whitelisting solution enterprises need to securely and comprehensively manage their threat landscape.

Continued »

About Lumension

Lumension, a global leader in operational endpoint security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets.

Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Reporting and Compliance offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year.

Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, India, Hong Kong and Singapore. Lumension: IT Secured. Success Optimized. More information can be found at www.preventia.co.uk

