

# Lumension Security Endpoint Protection Solution

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

September 2008



### 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; almost every employee uses information technology (IT) daily.

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 targeted malicious attacks. A thumb-size flash drive can siphon gigabytes of business and personal data in seconds. Most recently, smart phones – their use 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 code is identified and the anti-virus agents are updated on every machine – a process that can take weeks. Using these methods makes a “zero day attack” almost impossible to prevent.

In terms of data security, people are often their own worst enemies. They inadvertently circumvent existing barriers by downloading and installing infected applications, or 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 tapping into business communications and databases. Infected computers must be completely wiped and rebuilt to rid the operating system of the malware, causing downtime, overloading IT, and killing productivity.

Anti-virus software is the best option for keeping systems clear of existing threats. Keeping up with the hackers is more difficult, however; preventing human error, such as incorrect installation of rogue applications, is not its forte. The alternative – ensuring that only approved and valid applications run on every computer – requires a shift in mindset from defense to offense.

### The Whitelisting Paradigm Shift

Traditional approaches to endpoint protection have become ineffective in today's dynamic computing environments. Battling the onslaught of viruses, malware, and plain old poorly designed applications has become a reactive game with a losing proposition. To escape this mode of always falling one step behind emerging threats, you need a new endpoint security model. The whitelist provides the means to take charge of your information environment by making the shift from focusing only on what you know is bad to allowing only what you know to be good.

Knowing what applications you have, and which you need, is half the battle. By defining the necessary applications in a whitelist and authorizing them to run on the appropriate computers, you automatically place everything else on a virtual blacklist. Simply put, any executable – whether a business application, a video driver, or a web browser plug-in – not specified on the whitelist cannot load and run. Controlling exactly which applications can run on each computer keeps information secure while offering many other benefits.

## 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 Security Endpoint Protection Solution – 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. Combined with Lumension Security Vulnerability Management Solution, 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 an unfortunate 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 no viral attacks to thwart, malware to hunt down, or incompatible applications to invoke the blue screen of death, IT can spend more time and resources on improving operations instead of constantly fixing computers.
- **Increased data security and compliance with privacy laws.** Preventing programs not on the whitelist from running on any computer obviates the chance for spyware, keyloggers, and sniffers to steal passwords, address books, customer files, or other sensitive data from otherwise physically secure computers. Combined with Lumension Security Data Protection Solution, which prevents sensitive information from leaking out through lost or stolen storage devices, a whitelist creates a strong infrastructure that makes it possible to comply with privacy regulations.

Yet another benefit to application whitelisting is the ability – and the opportunity – to better understand your IT environment. What applications are your people really running? Which are necessary to your operations? Are you buying more bandwidth than you really need to conduct business? Getting an accurate view of IT usage is the first step in controlling your information and your business.

Lumension Security can give you the answers you need. Take the first step.

## Understanding Your Application Environment

If a CIO were to dream up a perfect IT environment, it would no doubt be very different from what most organizations have today. It would be a controlled environment 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 regulated computing environment, anti-virus and whitelisting programs might not be needed. But this scenario represents an environment seldom found in the real world – albeit perhaps one that is not as desirable as it may first seem.

### Real-World Challenges

A totally locked down computing environment is not only rare – it is unlikely to best 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 the flow of business. And while such a setup may at first seem convenient for the CIO's department, it ultimately adds labor-intensive work for system administrators and help-desk operators.

So, what do you live with today? Organizations that start out small, with even smaller IT teams, often by default give users local administrative control of individual PCs. Though such a choice lessens the initial burden on IT, as a company grows those few savvy users are joined by well-meaning neophytes installing rogue applications – sometimes incorrectly – corrupting files and registries in the process.

Or maybe your organization has inherited an infrastructure with a history of 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 networks. Malware and viruses continuously creep in through downloads and 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 a snapshot of your world? Though your scenario may be slightly better, or worse, the general situation remains the same. You need a way to categorize all the applications on all the computers on 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. Everything not on the whitelist – the virtual blacklist – cannot run. Period. To increase flexibility, especially in the beginning, you can extend the concept of trusted change by implementing a graylist. This permits safe but potentially undesirable programs to run until you decide whether they are really needed.

Whitelisted applications run. 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 prevented from running. Zero-day attacks through malware, worms, and Trojans are automatically prevented from running because they are not on the whitelist, and therefore never get the chance to launch and corrupt.

### Four Phases of Implementing a Whitelisting Solution

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

- Discovering and monitoring your application ecosystem
- Rolling out pilots and clients
- Enforcing protection
- Fine-tuning your application ecosystem

## Whitelisting Phase 1: Discovering Your 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 loaded with all applications normally deployed to employees but never used for business or connected to the Internet. 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

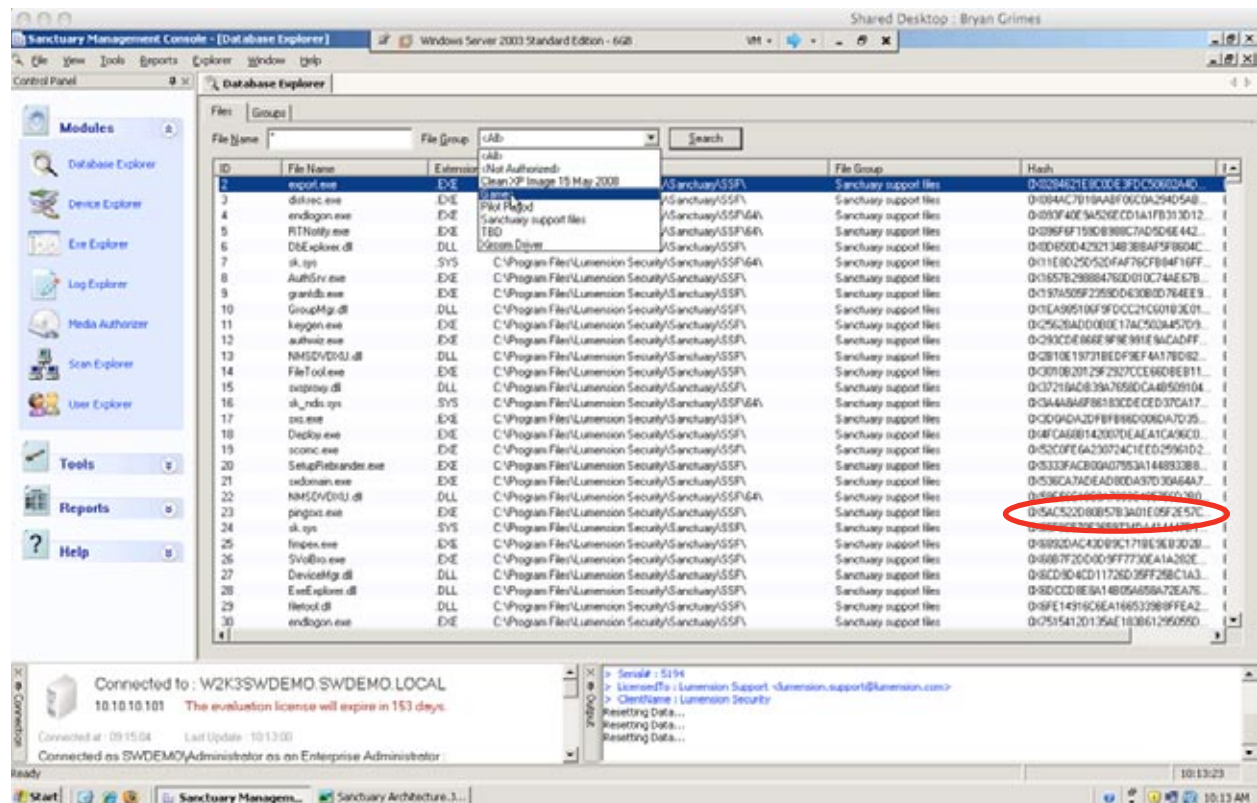
# Lumension Security Endpoint Protection Solution

regular basis. Also consider 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, the Lumension Security Endpoint Protection Solution 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

During the scanning process, each application file is defined with a unique hash number that enables the system to detect when corrupted, hacked, or simply 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, any performance overhead is undetectable and checks may be made even when the computer is offline.



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.

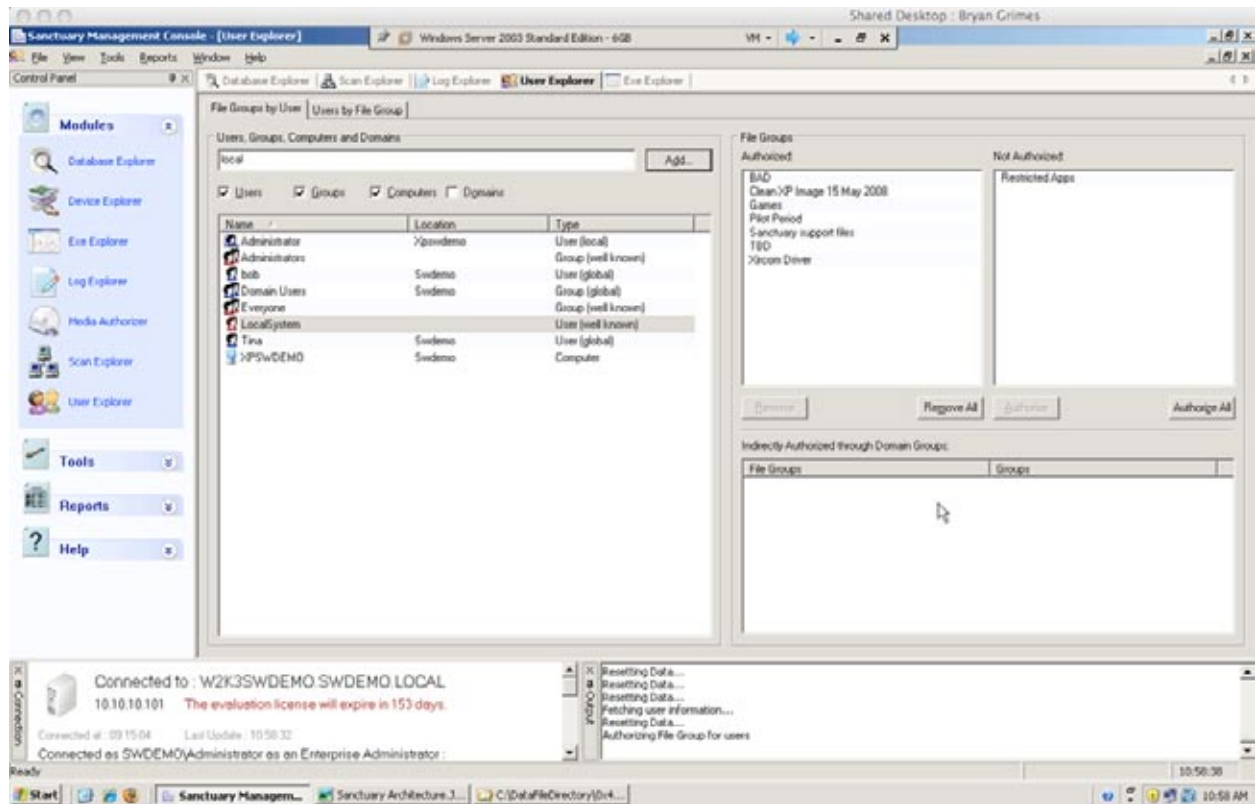
## Assign User Access

After initial scans, 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, use the User Explorer module to define groups of users and add permissions. These files are added

# Lumension Security Endpoint Protection Solution

to the “Everyone Group.” At this stage, everyone can run all applications that are on the whitelist. Later, you can fine-tune as necessary which groups can run which applications.



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

Lumension Security Endpoint Protection offers granular control of which processes are 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:

- 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; Microserf=always deny
- Trusted scripts and macros can be allowed to run with user permission

With this level of control, it is best 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. 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 the Lumension Security Endpoint Protection Solution into your overall change management process.

## Whitelisting Phase 2: Pilot Rollout

Once your gold-standard whitelist is populated with approved applications, drivers, and plug-ins, you are ready to deploy the Lumension Security Endpoint Protection Solution Agent to a group of PCs of similar purpose and build. This is the pilot for the wider rollout to 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; code development constantly changes runtimes that would be blocked by the standard whitelist.

To prevent abrupt interference of operations, deploy the Endpoint Protection Solution Agent in non-blocking mode. In the Endpoint Protection Management Console, enable the Execution Logging and Access Denied Logs 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 on the whitelist. Be sure to include times when periodic applications – for example, month-end accounting programs – are run.

The screenshot displays the Lumension Security Endpoint Protection Management Console. The main window is titled "Log Explorer" and shows a list of denied applications. The table below represents the data shown in the log:

Type	Traced On (Endpoint...)	User	Computer	File Name	Reason	Custom Message	File Group	File Name (Full)
EIEC-DENIED	7/30/2008 10:29:41.441 AM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 5:15:16.506 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 5:15:16.595 PM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 5:15:07.171 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 5:15:07.139 PM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 5:13:46.864 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 5:13:46.834 PM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 5:11:42.609 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 5:00:36.600 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 5:00:36.576 PM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 5:07:53.903 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 5:07:53.918 PM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 5:07:27.185 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 5:07:27.123 PM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 5:06:06.272 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 5:06:06.241 PM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 5:05:07.109 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 5:05:07.076 PM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 5:03:32.017 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 5:03:32.006 PM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 5:00:42.180 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 5:00:42.148 PM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 4:59:30.307 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe
EIEC-DENIED	7/30/2008 4:59:30.197 PM	SWDEMO\bob	spwdemo.swdemo.local	msosp	Denied	<Not Authorized>	C:\WINDOWS\system32	msosp.exe
EIEC-DENIED	7/30/2008 2:40:49.588 PM	SWDEMO\bob	spwdemo.swdemo.local	fragspl	Denied	<Not Authorized>	C:\Documents and Settings	fragspl.exe
EIEC-DENIED	7/30/2008 2:40:24.102 PM	SWDEMO\bob	spwdemo.swdemo.local	calc	Denied	<Not Authorized>	C:\WINDOWS\system32	calc.exe

The screenshot also shows a detailed view of a denied application at the bottom, including fields for Type (EIEC-DENIED), Traced On (Icon...), File Name (Full), File Ext, Other, Traced On (UT...), Transferred On..., File Path, SID, Process Name, Traced On (En...), Transferred On..., File Name, Computer, Hash, and buttons for View, Details, and Add Events.

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

As the system finds and logs applications not on the whitelist, decide which to add and which to deny when 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. For files that aren't readily identifiable, the file path displayed in the log results can often help identify the parent application.

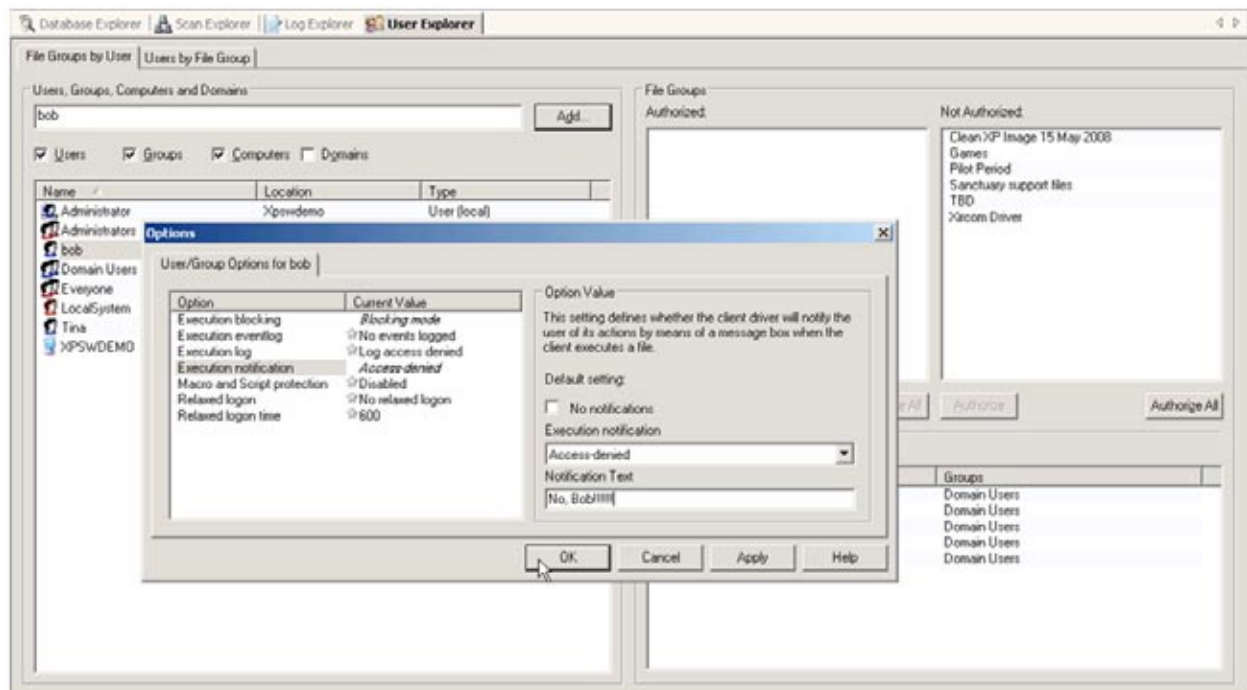
## Define a Graylist

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 staff for this change, your help desk will soon let you know about it. Use the Lumension Security Endpoint Protection Manager to design explanatory alerts that display when users try to run forbidden 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, 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 the Lumension Security Endpoint Protection Solution 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: Enforcing 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 they were not included fully 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. They are effectively deadware.

Congratulations. You have control of your IT resources again.

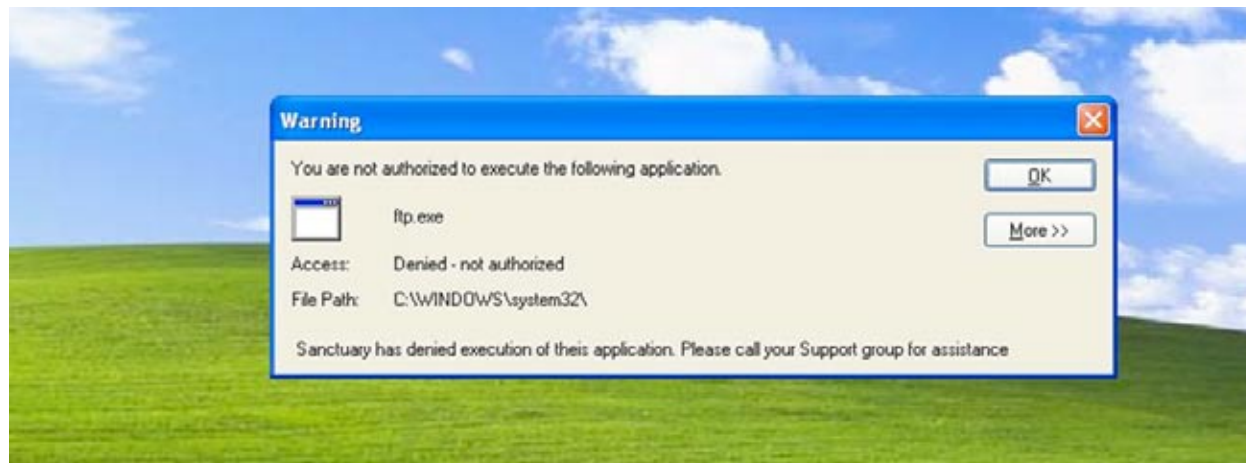
### Whitelisting Phase 4: Fine-Tune Your Application Ecosystem

Once you have regained control of your PCs, begin fine-tuning and optimizing the whitelist. The Lumension Security Endpoint Protection Solution 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 a valid executable and reassign it to a new group. This could be as simple as assigning the Windows game executables to a group such as “Holiday.” Or 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 to give you more control over your application ecosystem. As you become more experienced with the Lumension Security Endpoint Protection Solution, 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 Security Endpoint Protection, whitelisting guards your systems by allowing only approved processes and applications to run. It automatically protects your systems against malware and viral programs while improving total data security and overall system performance.

Adding Lumension Security Data Protection Solution 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. The Lumension Security Data Protection Solution provides that control, and offers detailed forensics of who is moving data and where. It's a perfect complement to application whitelisting.

Lumension Security delivers the only Vulnerability Management solution that fully integrates network scanning and agent-based assessment and remediation in a single management console that enables businesses to detect risks, deploy patches and defend their business information across a distributed environment with greater efficiency and no impact on productivity.

Lumension Security gives you control over your IT resources – today.

For more information, contact Lumension at [www.lumension.com](http://www.lumension.com) or +1 888 725 7828.

### About Lumension Security

Lumension Security™, formed by the combination of PatchLink® Corporation and SecureWave® S.A., is a recognized, global security software solution company, providing optimal protection and control of enterprise endpoints for more than 5,100 customers and 14 million nodes worldwide. Leveraging its proven Proactive Security Model, Lumension Security enables organizations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions that simplify the entire security management lifecycle. This includes [Vulnerability Management](#), [Endpoint Protection](#), [Data Protection](#) and [Reporting & Compliance](#). Headquartered in Scottsdale, Arizona, Lumension has offices worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, Hong Kong and Singapore. PatchLink, now Lumension, was founded in 1991 by Sean Moshir.

#### Global Headquarters

15880 North Greenway Hayden Loop, Suite 100  
Scottsdale, AZ 85260 / United States of America  
phone: +1 888 725 7828 / fax: +1 480 970 6323