

Putting Security in a Positive Light

A Guide to Proactively Managing Endpoint Risk

In this whitepaper, Patrick Clawson, Chairman & CEO of Lumension Security, will outline the importance of adopting a Positive Security Model that combines the power of vulnerability management, automated remediation, and whitelist application and device control to eliminate the risk of the unknown threat.

September 10th, 2007



Putting Security in a Positive Light

Information security managers have always had a healthy fear of the unknown threat. But over the last two years that fear has developed into a paranoia, an obsession that keeps them up at night sweating over thoughts of financially-motivated malware that may be slipping past their traditional anti-malware defenses without a blip on the radar. They spend all of their time trying to find better ways to block the threats, and yet most of their efforts end in futility anyway.

This is because the threats keep multiplying. The past several years have brought a wave of unending zero-day attacks designed specifically to silently steal information. Organizations are not receiving the necessary back-up from their traditional vendors, because these security companies are drowning in the flood of malware issued by crooks that are specifically programming malware to evade blacklist signatures. Anti-virus vendors have admitted as much to the media.

“We’re losing this game with computer criminals,” Eugene Kaspersky, the founder of Kaspersky Labs, told eWEEK in a December 2006 interview. “There are just too many criminals active on the Internet underground.”

His thoughts were echoed by Mikko Hypponen, F-Secure’s director of anti-virus research, who in March was quoted by MSNBC as saying, “It’s getting harder and harder for us just to keep up with the amount of new malware coming in. Right now on a typical day we receive more than two a minute. There are thousands every day. The increase in three years has been tenfold.”

Compounding the near-constant barrage by the criminals is the fact that rogue users are increasingly opening up the enterprise to countless more risks by introducing applications and technologies with exploitable flaws. One big example is the proliferation of social networking sites whose users have become low-hanging fruit to attackers. Personal applications such as peer-to-peer file sharing applications expose enterprises to software licensing and copyright violations. The same goes for the unfettered use of removable storage devices, which brings the added risk of data leakage.

Sleepless security managers are left spinning their wheels in response to all of this, trying to reduce risks by responding to this attack here,

that new exposure there. But this negative security model is just spinning them into a spiral of reactivity. IT resources are drained while security plays catch-up and never quite catches up.

“When a zero-day comes, you’re behind the eight ball if you’re just relying on reactive defenses,” says Charles Kolodgy of IDC.

The numbers prove this to be true. Even though 99 percent of all enterprises had antivirus installed by 2005, 62 percent still suffered from an infection.

Clearly, the model is flawed. Analysts like Kolodgy believe that the only way organizations today will crawl from under the weight of unknown threats to their systems is to change the way they practice security. They must shift from the negative to the positive security model.

Allowing the Known Good

The principle of positive security is simple. Rather than chasing every risk and threat in the environment with blocks and denials, the positive security practitioner blocks everything by default. Only the known good applications are allowed to run. The unknown threat loses its power when it is blocked from systems automatically.

“If you’re proactive you don’t need to worry about what new thing is going to pop up tomorrow because you’ve already dealt with it,” Kolodgy says. “There isn’t a gotcha.”

Network managers are already familiar with this positive approach—they’ve been practicing it with firewalls for years.

“In network security there is no question that a default-deny scheme is the best policy,” says William Bell, director of security at ECSuite.com. “The funny thing is that when you take that into the systems protection arena many people have failed to apply that same policy.”

Progressive security practitioners like Bell agree that traditional systems protections such as anti-virus and anti-malware are too reactive to rely on alone.

Hackers and other malcontents can easily take

advantage of the fact that these outmoded technologies must know about a particular type of attack before they can protect against it. This is the reactive approach's Achilles heel, one that is being assaulted daily by malicious "boutique" attacks designed specifically to evade traditional defenses by sneaking in with new and unknown approaches.

"My philosophy is that our security should be able to stay ahead of emerging threats rather than just reacting to them," Bell says.

He uses a combination of Lumension solutions such as Sanctuary endpoint security and PatchLink Update and PatchLink Developers Kit to develop and enforce a proactive security approach at CWIE that only allows the execution of approved and updated applications and ensures proper security configurations on an ongoing basis.

Not only does such a comprehensive line of defense help mitigate risks at the endpoint through proactive remediation, it protects against unknown attacks and also cuts off other risks such as data leakage through unauthorized devices or illegal downloading to corporate endpoints through peer-to-peer networking applications.

"This positive stance keeps our digital assets safe from both internal and external threats," he says.

Five Steps to Positive Security

The beauty of the Positive Security Model is that it can be extended far beyond a whitelisting augmentation of anti-virus. In an ideal setting, this model will establish the "known good" across the entire IT infrastructure. When organizations establish what they want their systems and configurations to look like at any given point in time, they gain proactive control of their infrastructure.

A holistic positive model will ensure a desired security posture by settling in advance on matters such as patch levels and vulnerability remediation, port settings and accepted networking equipment, along with accepted devices and applications. By doing so, IT administrators gain the visibility and the capacity to manage the infrastructure securely without ever worrying about

reacting to new threats.

- 1. Discover Assets:** Organizations must first understand what they're up against before they can harness the power of positive security. They must learn what the operational inventory encompasses and why each component is in place before establishing and enforcing the "known good." The first step of discovery includes every part of the infrastructure, including hardware, software and configuration.

From a hardware perspective, this means surveying servers, desktops, printers and all devices down to the stray USB thumbstick or external CD burner. Similarly, every application needs to be detected, from server apps to user-installed shareware. Configurations of all of these items also need to be cataloged. Those in charge of discovery will need to find rogue networks, usernames without passwords, and other configuration risks that have previously gone undetected.

Organizations will also need to figure out why each part of the infrastructure is installed or configured in its current set-up. This will give them a better understanding of business needs in relation to the risks presented by each. Some unconventional applications or devices may have been installed by users to address critical business needs. Others could just be there to satisfy users' personal whims. Some riskier configurations might be intentionally set to improve business efficiencies. Others might simply be overlooked mistakes. Uncovering the reasons behind each installation and configuration will enable management to decide how much risk it is willing to assume based on operational requirements.

In the past this discovery process has been a seemingly impossible task, but the development of automated tools such as the Lumension line of whitelisting, vulnerability and patch management tools has eased this pain point. Automation can take care of the heavy lifting required to shed light on system contents. From there, it is up to administrators to assess which applications and devices are crucial to core business practices and which are frivolous or too risky to run.

Putting Security in a Positive Light

- 2. Develop Policy:** At this point, the organization will need to focus its efforts on one of the most critical elements of positive security: policy development. A sound collection of policies will set the “known good” for an organization.

The policy statements developed in this step should not imitate the broad IT “shelfware” policies of old. They should be systematic, actionable rules that balance accepted risk with business needs.

Both comprehensive and detailed, these policies will establish which hardware, software and configurations will be accepted in the environment. They should specify which models of servers, laptops, desktops and networking equipment are allowed on the network. They’ll also detail which applications are allowed to run and which peripheral devices are allowed to connect on the equipment. From the endpoint perspective these policies might ban the use of personal applications or limit the connection of removable storage to certain times of day.

Configuration settings should also be spelled out. This will mean describing specific versions of accepted applications that are permitted and laying out the levels of patching required for each. It will mean requiring passwords for all accounts and stating what types of critical vulnerabilities will trigger blocking of applications or configurations once considered safe.

Many IT security professionals have avoided developing such detailed rule sets in the past because there was no easy way to enforce them. Today’s mature solutions make this a non-issue. IT organizations can now develop policies based on how they’d like to mitigate risks rather than on what they think they can feasibly enforce.

- 3. Eliminate Risks and Threats:** Before getting to the stage of ongoing enforcement, of the current environment must be remediated appropriately. Organizations should start by eliminating risks and threats that are already present in the environment so that they can start enforcement from a clean slate.

During this remediation phase, organizations will update configurations, prevent ex-

ecution of unacceptable applications and devices, patch old versions of acceptable software and ensure that there is no malware or spyware lurking on any of their systems.

Once this is done the infrastructure and configuration set-up should match the policies established during step two. This is the “baseline” which IT practitioners can update and maintain in order to comply with policies from there on out.

- 4. Enforce Policy:** Now it is time to put actions behind words and enforce the corporate policy that has been established. Many organizations are able to eliminate risks and threats in fits and starts, but few are able to continually enforce policy on a real-time and ongoing basis. This programmatic enforcement truly is the benchmark of a well-executed Positive Security Model.

A comprehensive set of tools is critical to carry out this step of real-time enforcement. Lumension’s vulnerability management solution will not allow the resetting of a compliant configuration into a riskier non-compliant configuration will remediate vulnerabilities as they crop up and will patch applications as soon as vendors make fixes available. And Lumension’s Sanctuary endpoint security solution provides administrators with the capability to enforce application and device use on the endpoints and when. Rather than relying on users to comply, these tools don’t even give them a chance to break the rules.

Organizations that are worried about backlash from users and executives should be allowed to slowly ease into this process. Good enforcement tools will enable security professionals to run them in monitor mode and observe how the solution would react to certain policy events. This gives them the opportunity to tweak configurations and gain confidence that critical business applications will remain unaffected once enforcement is enabled.

- 5. Audit and Report:** The final step in the positive security progression is to audit and report on activities based on the policy that has been set. Automated auditing and reporting functions give security personnel the flexibility to conditionally allow certain

devices, applications or configurations while still keeping a close eye on their use. For example, say an organization has decided to allow the use of removable media in order to facilitate business operations. Security needs to have the ability to know when an employee downloads important intellectual property onto a device so that it can circle back with that individual to double-check that this was done for legitimate purposes.

In a way, the auditing and reporting process is like an extension of that first discovery and assessment step. Because the known good is a moving target, organizations need to be constantly surveying the environment and updating policy based on the information gathered from auditing and reporting.

Reaping the Benefits

Clearly, it takes more foresight and effort to replace a reactive model with a more effective proactive security approach. In large part this is why many organizations still persist in relying on traditional techniques or other point solutions.

“They see it as an unaccomplishable task,” Bell says of his counterparts who have not yet adopted positive security methodologies.

This is how he’s convinced upper management to give him the resources to enable his company’s positive approach. The outcome has certainly justified the decision, he says.

“We have replaced 72 percent fewer computers than we did before,” he says. “Usually those replacements were due to spyware, malware, whatever. We don’t see that anymore because it can’t run.”

Best of all, he can rest easy at night because he doesn’t have to worry about the unknown. “The risks have dramatically decreased,” he says. “I don’t go to sleep at night worrying about the latest, greatest Trojan that has come out. I don’t go through that. I did before.”

By combining the power of vulnerability management, automated patching, and whitelist application and device control, any organization can similarly eliminate the risk of the unknown threat. The chaos of reactivity can be replaced by the

order of the known good. This is the true potential of a fully-realized Positive Security Model. And that means a good night’s sleep for everyone.

Positive Security Model in Action: ECSuite.com Case Study

One of the biggest challenges William Bell faced when transitioning ECSuite.com to a positive security model adjusting with a diverse endpoint environment. As director of security for this Tempe, Ariz.-based e-commerce solutions provider, Bell is tasked with protecting wildly divergent systems.

With multiple companies under the ECSuite. umbrella and just 320 people on staff, there are no large departments with homogeneous system configurations here. And yet, with the help of Lumension’s vulnerability management and endpoint security solutions, Bell and his staff were still able to construct a system that worked across the organization.

“We’re a dynamic organization,” Bell says. “I would say that we are one of the harder kinds of organizations out there for this kind of solution. Everybody and their brother has 50 different kinds of software. Some of our departments were harder than others. Development was hard, so was the graphics department. They use a lot of software products.”

The key, Bell says, was taking the time and care to ensure that these products all worked once all the tools were installed. The other critical action that ensured success of the program was a refresh of the organization’s change management process, which brought some order to the already chaotic system environment.

“We didn’t have a very sound change management process,” he says. “Users would ask for it and if it cost money it would go to be processed for price approval, if not it would go on their computer. Now we’ve modified that.”

The new process now requires approval from the security department before an application is loaded.

“We’re in the loop now, looking to see if an application is dangerous, whether it is already authorized to the whitelist and whether it is updated.”

Putting Security in a Positive Light

he says. “It was one of those things that we’ve had to overcome, but we’re there and now we can keep moving forward.”

In addition to Lumension’s Sanctuary whitelisting tools, Bell takes advantage of Lumension vulnerability management to only allow systems to operate applications and devices that are approved, updated and configured correctly.

“We believe in defense in diversity,” Bell says. “Sanctuary is our security blanket against any possible zero-day attacks, but on top of that, patching is the best way to eliminate vulnerabilities. This multi-layered approach helps us identify and remove vulnerabilities while maintaining a consistent baseline of security.”

Bell also uses PatchLink Update to rapidly test and deploy patches, and he uses PatchLink Developer Kit to code his own patches. This is especially useful when a critical vulnerability is discovered for which a patch has yet to be released.

“This positive stance keeps our digital assets safe from both internal and external threats,” Bell says. “In large organizations, it may take a month to roll out every necessary patch. With PatchLink Update and Sanctuary in place, I can rapidly deploy patches—including those I script myself—with the insurance of ‘big brother’ protecting our patch cycle.”

Lumension Security™, Inc.
15580 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260

www.lumension.com