

Preventing Weaponized Malware Payloads in Advanced Persistent Threats

Strategies for Layered Endpoint Defense Against the APT Kill Chain

Weaponized malware combined with advanced persistent threats pose a daunting security challenge for organizations. Here's how weaponized malware works - and how a defense-in-depth approach to endpoint security can give you the upper hand.

Most security professionals probably don't think of themselves as heroes from Roman mythology. But they just might identify with Hercules, who had to prove himself through 12 nearly insurmountable "labors," or feats of strength and courage.

From polymorphic malware, to botnet attacks, to SQL injections, today's security pros have plenty of their own labors to grapple with. And the emergence of weaponized malware and advanced persistent threats (APTs) adds to those challenges exponentially. In fact, recent attacks such as Stuxnet and Flame—which affected not only specified targets but also many other organizations around the world—combine multiple, sophisticated threats into a single deadly package.

Fortunately, a growing number of forward-thinking organizations are finding a solution through a defense-in-depth approach to endpoint security. They're using defense in depth strategies to strengthen their overall security posture including:

- » Antivirus
- » Device control
- » Hard-drive and media encryption
- » Application control and memory protection
- » Patch and configuration management

Although no single solution—or even combination of solutions—can necessarily guard against every payload, layering multiple technologies with combined best-practice endpoint management is well-suited to decreasing the risk of weaponized

malware and APTs. That's because each layer can block a different aspect of the nefarious, multi-pronged attacks characteristic of this new breed of threat. What one layer misses, another layer is designed to catch. It's all about disrupting the hostile campaign in as many places as possible.

Take, for example, the highly publicized Flame attack. Examining the attack in detail reveals why weaponized malware is such a serious risk. But it also shows how defense in depth can mitigate that risk and ensure the right level of security for your organization.



On-Demand Webcast



Dousing the Flame

How This Tom Clancy-Esque Attack Worked and What You Really Do to Protect Against It

With Randy Franklin Smith
of Ultimate Windows Security



The Barrage Begins

APTs are attacks that follow a disciplined methodology or “kill chain” where the perpetrator is sophisticated, organized and determined – not limited by conventional budgets, capabilities or timeframes.

Weaponized malware are the customized and often sophisticated software payloads being delivered through the use of the APT “kill chain”.

Traditionally the industry has relegated APTs to be carefully aimed presumably at military, government or infrastructure targets. But there’s been a shift towards targeting private corporations in recent months that makes APTs a concern for everyone. Why should the average organization be worried? There are 3 reasons organizations large and small should be concerned about weaponized malware and APTs:

- » **Retaliation** - When one nation cyber-attacks another, it’s only reasonable that the injured party will retaliate. That retaliation may hit military or government targets. But it may well go after private-sector organizations.

A case in point is the Shamoon malware that appeared in August 2012. The Trojan horse, which can steal data and overwrite a computer’s master boot record, hit oil-and-gas companies in Saudi Arabia and Qatar. U.S. intelligence officials reportedly blamed the attack on Iran, which they believe was striking against U.S. allies in response to the Stuxnet and Flame attacks.

Additionally, it has recently been announced that the Chinese government has been staging ongoing APT attacks against the Wall Street Journal and New York Times in retaliation for unfavorable media coverage. In the case of the New York Times attack, 45 customized malware payloads were discovered on endpoints inside of their environment.

- » **Collateral Damage** - Malware spreads. Stuxnet and Flame were carefully targeted at Iranian nuclear facilities. But they were also stealthy enough to go undetected for a long time. That gave them opportunity to circulate to organizations that were outside their intended targets.
- » **Copycat Killings** - Whenever an APT or weaponized malware is discovered, security researchers dissect it and publish the results. Even if opportunistic cyber-criminals don’t get access to the code, they learn how it functioned, and which attack vectors it used, which zero-day vulnerabilities it exploited. In short, they gain new weapons they can use against any organization.

And make no mistake: The attacks are increasing. More than 5.5 billion attempted attacks were identified in 2011, an increase of 81 percent over 2010, with an unprecedented 403 million unique malware variants that year, a 41 percent leap.¹

1. Symantec Internet Security Threat Report, 2012

Preventing Weaponized Malware Payloads in Advanced Persistent Threats

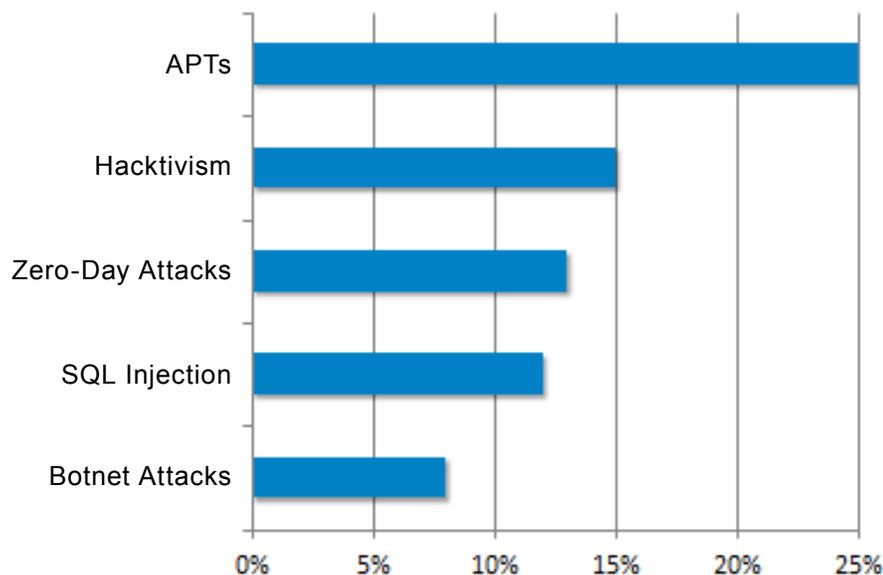
Advanced targeted attacks reached 154 per day by the end of 2011. Those attacks were distributed across large and small organizations. Most of the threats were aimed at government targets, but they also sought out businesses in manufacturing, financial services and other sectors. By job title, executives were most at risk, but employees in sales, R&D and other functions were also in the crosshairs.

In terms of breaches, Verizon tracked 855 cyber-break-ins that resulted in 174 million compromised records in 2011, the second-highest since it began tracking in 2004. Eighty-three percent were linked to organized-crime groups. Overall, 81 percent of

breaches involved hacking, while 69 percent leveraged malware. Verizon reports that for 97 percent of those breaches, could have been thwarted with basic security controls.²

In fact, IT pros are increasingly aware of APTs, according to a December 2012 study by Ponemon Institute, an independent research firm. The study surveyed 671 U.S. IT and data-security practitioners, more than three-fourths of whom worked at companies with more than 1,000 employees. And while zero-day, SQL injection and botnet attacks are all on their minds, their No. 1 headache is now APTs.³ (See Figure 1.)

Figure 1: Top 5 Data-Security Headaches



Source: Ponemon State of the Endpoint, 2013

IT and data-security practitioners cite advanced persistent threats as their biggest security headache.

2. Verizon Data Breach Investigations Report, 2012

3. Ponemon State of the Endpoint, 2013

Breaking the Kill Chain

The “kill chain” of advanced persistent threats (APTs) involves seven links (or steps), according to researchers at global defense company Lockheed Martin Corp.:

1. **Reconnaissance** - Identify targets.
2. **Weaponization** - Combine a remote-access Trojan horse with an exploit into a deliverable payload.
3. **Delivery** - Transmit the malware to the target, typically through an email attachment, website or USB drive.
4. **Exploitation** - Trigger the malicious code, usually to exploit an operating system or application vulnerability.
5. **Installation** - Deploy a remote-access Trojan horse or backdoor so the attacker can persist within the target.
6. **Command and control** - Connect to an Internet server to gain “hands on the keyboard” access to the environment.
7. **Actions on objectives** - Execute toward goals, typically to steal data.

Where can an endpoint defense-in-depth approach to information security break the kill chain? Primarily at Links 3, 4 and 5:

Delivery - Device control can block infected USB devices. File-type filtering from USB to endpoint can also provide protection.

Exploitation - Effective patch and configuration management can eliminate known vulnerabilities. Memory/buffer overflow protection can also offer safeguards.

Installation - Application control can prevent unapproved executables (including weaponized payloads) from running on your endpoints.

Defense-in-depth can't stop cyber-criminals from wrongdoing. But if it can interrupt their efforts before they deliver, exploit or install, it can effectively prevent harm to your network.

Deconstructing Flame

By now we've all heard of Stuxnet, DuQu, Flame and, most recently, Gauss. But what differentiates these weaponized attacks from traditional malware? And what lessons can we apply to protecting against future weaponized threats?

By using Flame as a case example, we can understand the nature of weaponized malware and APTs. We can also identify how a defense-in-depth approach to information security can offer meaningful protections.

Flame was designed for cyber-espionage, targeting government organizations and educational institutions in Iran and other Middle Eastern countries. It has been called the "Swiss army knife" of malware and a "new high-water mark" for the complexity of the attack. This malware was uncovered in May 2012 but had been operating in the wild since at least February 2010.

The weaponizers started by using stolen credit cards to register 84 domain names to fake individuals and addresses. They registered innocuous-sounding names such as traffic-spot.com, quick-net.info and smart-access.net to establish 24 command-and-control servers.

The actual malware appears to have been originally delivered on a USB drive. Once Flame reached an endpoint, it spread through the network by spoofing a Windows Update server. It then captured keystrokes, network logs, text documents and other data, and transmitted that information to the command-and-control servers through the LAN's Internet connection and through Bluetooth devices.

The Flame attack ingeniously combined high-tech and low-tech. It hacked the MD5 hash algorithm to serve up an authentic Microsoft digital certificate, yet its initial attack vector was a simple USB drive. The malware was antivirus-aware and, in the presence of AV software, would turn off detectable features. In fact, it packed 20 MB of robust, stable payload. Here are just a few of its more notable capabilities:

- » **USB delivery vector** - Flame's preferred delivery method was a USB drive. That was low-tech but effective, because it relies on human behavior, the weakest link in the security chain. Someone can carry an infected USB stick into an organization. They can share it with another person, who can walk it through a locked door and into a secure area. That person can then share it with someone else, who can plug it into a privileged or mission-critical machine. And that's possibly what happened with Flame.
- » **USB beacon** - If Flame infected a computer running Bluetooth, it turned the system into a Bluetooth beacon. It could then download data from any nearby Bluetooth-enabled mobile device. It could also jump from one Bluetooth device to another. If those devices had a wireless connection to the Internet, they became alternate routes to the command-and-control servers—a path that bypassed any security protections on the LAN.

- » **Keystroke logging** - Flame could capture keystrokes as well as network activity. So in addition to usernames and passwords it could figure out who was logged on, what they were sending, where they were in the network, and where other systems were located. Before long, it could map out and move around the network.

Text summary, data compression, trickle uploader—Flame was intended to gather information, a capability it had in spades. In addition to capturing screenshots, audio files and Skype conversations, it could scan large documents and generate a text summary. That avoided the need to exfiltrate large files. It also had the ability to compress files. And it featured a trickle uploader that transmitted data in inconspicuous 8-KB packets that would go undetected.

- » **Command and control** - To capture data, Flame needed to communicate with its command-and-control servers. The 84 domain names associated with Flame were an effective way to achieve that, because they weren't dependent on a specific IP address. Instead, the domain names pointed to 24 IP addresses, which were the command-and-control servers. In addition to allowing data collection, such servers can also upload new payload to the malware—for example, altering its mission from data collection to data destruction.
- » **Extendible architecture** - Flame wasn't a crude piece of malware. It was sophisticated and well-developed. It had an extendible modular architecture, with each module

loaded up as a separate dynamic link library (DLL) or Object Linking and Embedding custom control (OCX). And connected through the command-and-control servers, the weaponizers could upload new modules to active Flame deployments.

- » **Windows Update proxy server** - One of the more pernicious aspects of Flame was that it could make itself appear to be a proxy Windows Update server. An infected computer would pose as a Windows Update site, to which other Windows computers could connect and download a “patch” that was actually Flame. Flame signed the bogus patch with a certificate that appeared to be from Microsoft. Any site that relied on Windows Update would have been completely vulnerable to this means of infection.

- » **MD5 collision attack** - To pull off the Windows Update spoof, the weaponizers had to first create Microsoft digital certificates. They did this by achieving a “collision attack” on the MD5 hash algorithm that Microsoft used to produce digital certificates.

Hash algorithms are designed to produce a unique cryptographic hash for each input. In a collision attack, the attacker manages to use two separate inputs that produce the same hash value. In short, rather than try to create a fake digital certificate, the Flame weaponizers attacked the hash algorithm itself and generated a fraudulent but “mathematically authentic” Microsoft certificate.

What Have We Learned?

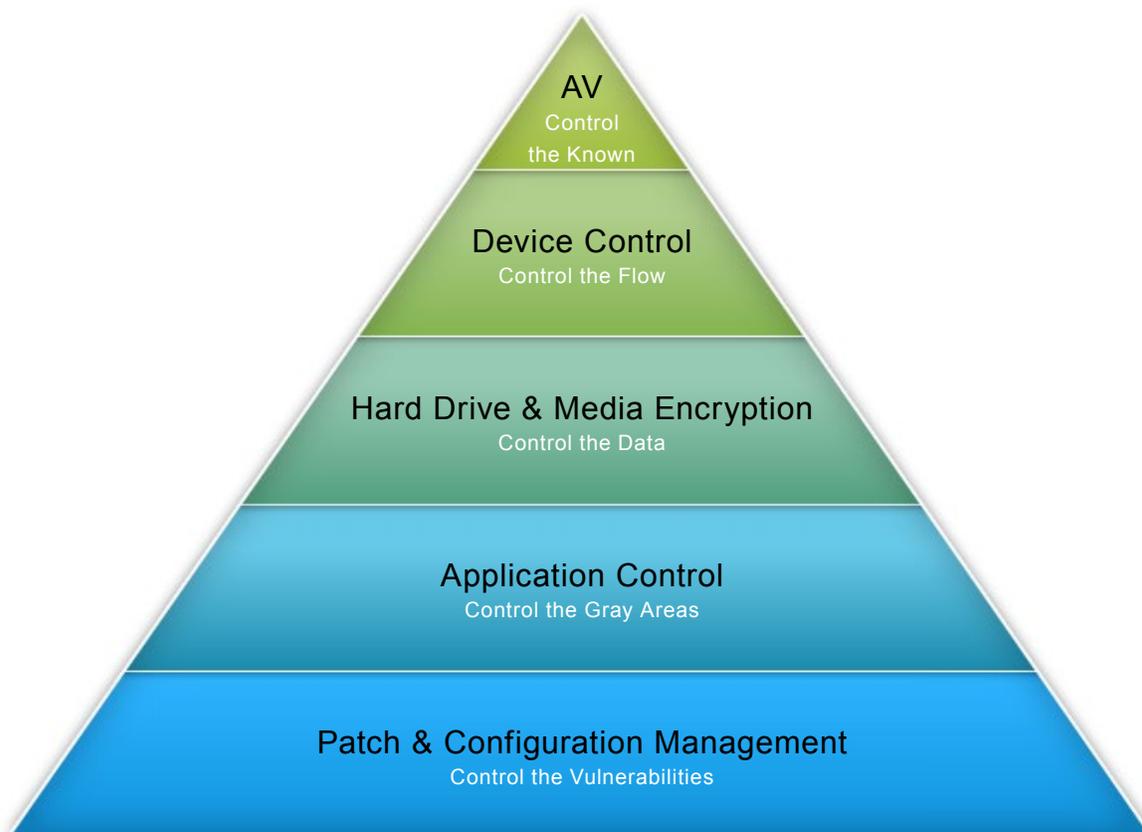
No single data-security solution would have stopped Flame. In fact, given its sophisticated and multifaceted payload, it's unlikely any combination of security technologies could have thwarted every aspect of the malware.

But information security has never been about 100 percent protection. Rather, it's about identifying the level of risk appropriate for your organization and implementing the safeguards that keep you on the right side of that risk threshold.

That's exactly the intention and advantage of defense-in-depth. Defense-in-depths gives you layers of protection that reduce your overall risk. It helps slow perimeter attacks so you have time to respond. And, it gives you multiple defenses working in tandem so you have the tools to respond.

With greater awareness of how defense-in-depth can offer protection against weaponized malware and APTs, you're better equipped to identify the security solutions that will best meet your needs:

Figure 2: Defense-in-Depth Architecture



A defense-in-depth approach to endpoint security can effectively protect against weaponized malware and advanced persistent threats.

- » **Antivirus** - AV would have automatically constrained Flame's capabilities. Because Flame was AV-aware, it shut down some of its payload in the presence of AV. Plus, because AV removes all known malware, it lets you focus on unfamiliar attacks like Flame.

Effective AV quickly and accurately identifies all known viruses, worms, Trojan horses, rootkits, keyloggers, spyware and adware. It also employs multiple detection techniques to identify and block zero-day exploits.

AV should combine traditional signature-matching capabilities with newer heuristic based approaches such as partial pattern matching, behavioral analysis and general exploit detection to provide the most proactive protection. It should also enable granular policy management, with the ability to schedule multiple AV scans per endpoint with various scan settings and times.

- » **Device control** - Flame's primary means of infection was a USB drive. Device control lets you set rules about what kinds of devices can be plugged into an endpoint. Those rules can be granular, addressing type, brand, and even individual USB drive. So anyone with a nonstandard USB device is unable to load it on an endpoint.

Device control would also have protected against Flame's Bluetooth capability. Device

control lets you turn Bluetooth beacons on or off, and set connections with other Bluetooth device as allowed or not allowed.

An effective device-control solution centrally automates the discovery and management of removable devices. It defines and enforces device use and data encryption policies by group and by user, with flexible exception management. By centrally applying encryption, it also ensures that lost or stolen devices or media can't be accessed. It should also capture detailed forensic information to track data transfer events.

- » **Hard-drive and media encryption** -

Encryption wouldn't have stopped a Flame infection. But it would have prevented Flame from scanning text documents on lateral endpoints, which were then summarized and uploaded to its command-and-control servers. And even if Flame exfiltrated files, the attackers would have had to decrypt them to gain any benefit.

- » Effective hard-drive and media encryption secures all data on endpoint hard drives. IT also provides single sign-on to Windows and enforces secure, user-friendly pre-boot authentication. It quickly recovers forgotten passwords and data. And it enables automated deployment, management and auditing.

» **Application control & memory protection**

- With application control, you don't let any executable run unless it's been established that they came from a trusted source. So effectively managed application control could have blocked Flame payloads. Even if malware gets through the perimeter, if it can't execute, you've protected the endpoints on the network.

Flame teaches another lesson about application control. Because Flame was able to spoof Windows Update, any security configuration that implicitly trusted Microsoft was left vulnerable - potentially including application control policies that extended trust based on "known software publishers".

An effective whitelisting solution is built around a trust engine that lets you define criteria for trusted applications. You can define trusted publishers, updaters, paths or locations. You can specify trusted authorizers, so certain users can run software that would otherwise be blocked. You can approve or deny globally, for groups of users or for individual endpoints.

Additionally, you can maintain a blacklist of denied applications. The blacklist can override the whitelist to block specific applications, regardless of publisher or path, for example. Though application control or "whitelisting" is a very effective defense against unknown threats, it's important to protect the most critical of endpoints with more stringent security policies

rather than with open flexible policies that could be "duped" by APT attackers. This is particularly important for servers and essentially enforces change control policies that are already established by most organizations.

In addition to application control, it's important to protect the memory space of trusted applications. This prevents attacks from exploiting trusted applications that are already installed on endpoints.

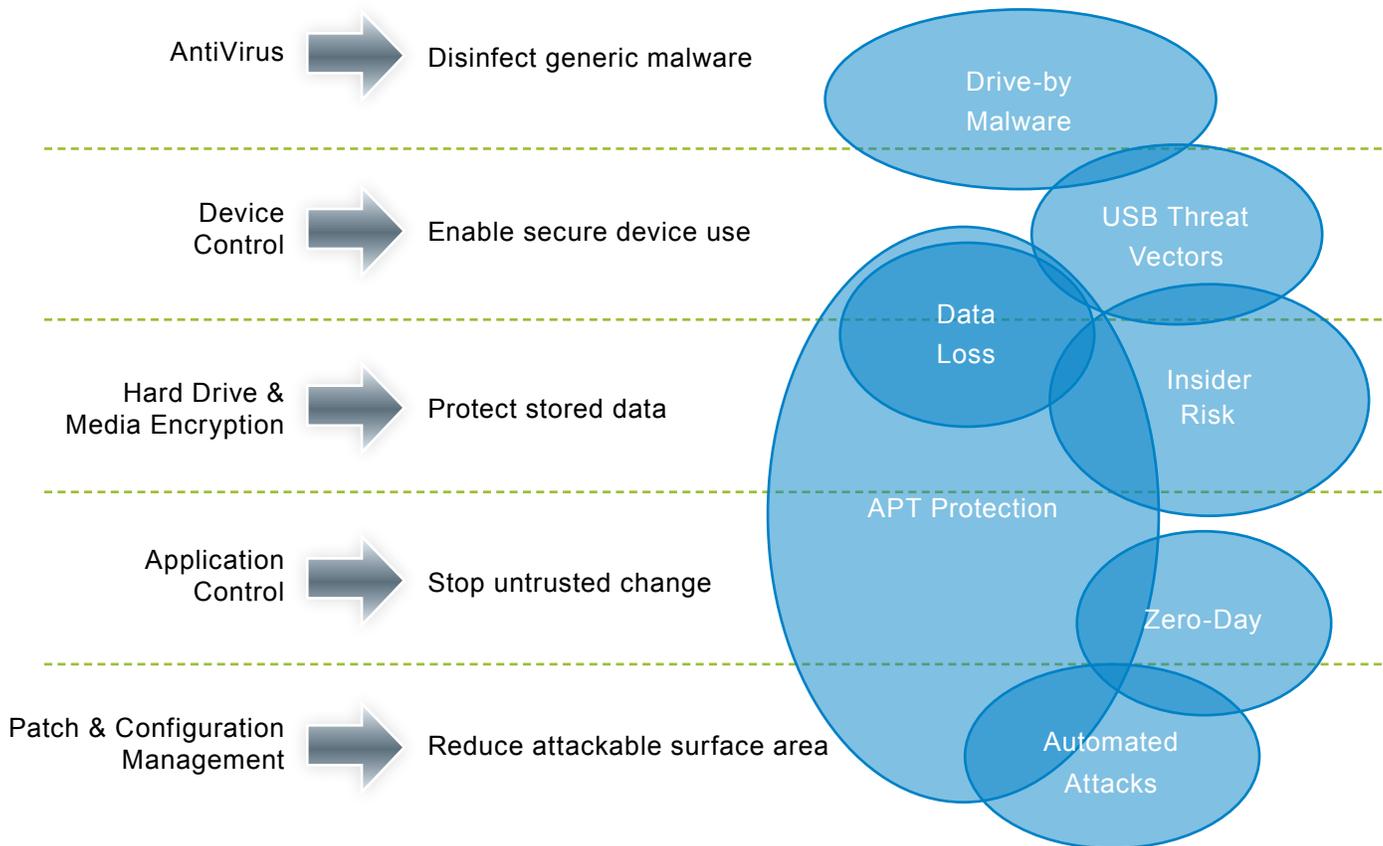
» **Patch and configuration management** - Patch Management is still one of the most effective layers in preventing attacks that we have today. The premise is simple – reduce the known vulnerabilities in your environment to minimize the exploitable surface area that attackers have to target. While Patch management cannot protect against zero-day vulnerabilities (other layers of the defense-in-depth approach, such as application control and memory protection address this), most attacks today actually target older vulnerabilities and not the newer or un-disclosed.

Likewise, good configuration management would have turned off unnecessary features such as Bluetooth and Web Proxy Auto-Discovery Protocol (WPAD) on computers that didn't need it. Establishing a baseline configuration and applying it to every endpoint can go a long way in reducing exploitable targets.

An effective patch and configuration solution enables patching of all versions of Microsoft and other operating systems, as well as Microsoft, third-party and custom applications. It should also support patching based on the Common Vulnerabilities and Exposures (CVE) database.

The solution should also let you establish patch baselines. That way, if a user installs an earlier version of an application or reverts to an earlier state, the application will automatically be patched, without reporting a new problem and requiring manual intervention.

Figure 3: Defense-in-Depth Protections



Defense-in-Depth protections address the multi-pronged attacks that typify weaponized malware.

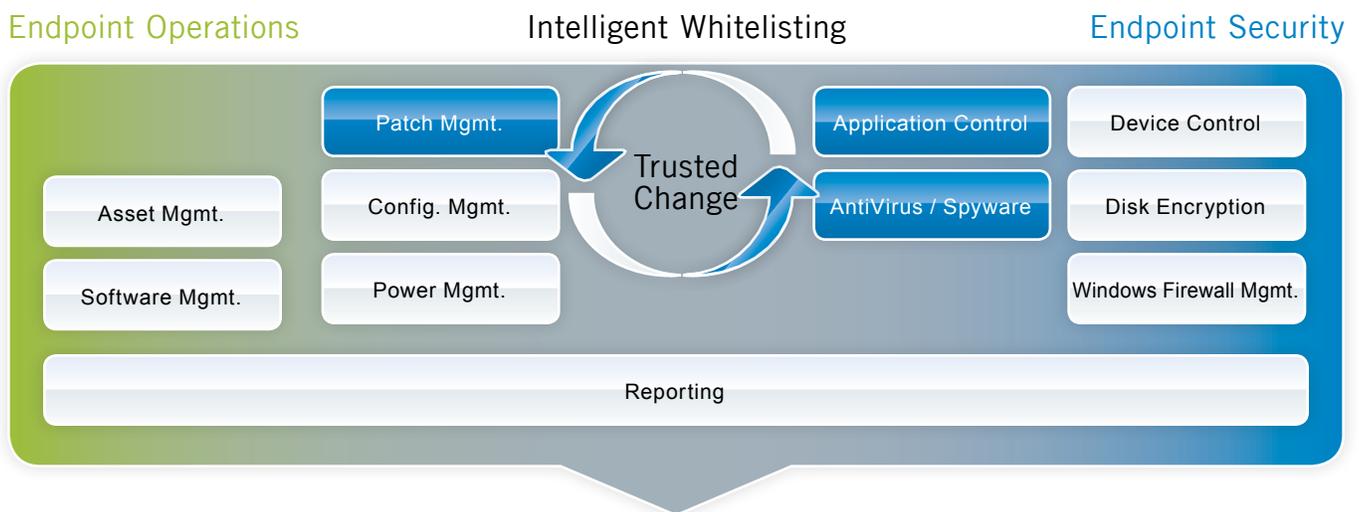
Integrate and Conquer

Fundamental to good defense-in-depth is seamless integration among layers. Siloed security solutions will be less effective, will place a greater administrative burden on your security staff, and will result in a performance hit on your endpoints.

An integrated security suite ensures a flexible, modular approach to endpoint security. It gives you one management console, for a single view of the enterprise. And it provides interlocking defenses that enable true risk mitigation.

Sophisticated attacks and advanced persistent threats are likely to become more common. But you don't need to be a mythological hero to reduce the risk of weaponized malware and APTs. Effective defense-in-depth, thoughtfully deployed and integrated, can relieve your security labors while tangibly improving your security profile. For today's security pros, that's heroic enough.

Figure 4: Integrated Defense-in-Depth



- » Comprehensive security
- » Proactive target hardening
- » Reduced overall IT cost

The crux of effective endpoint security is that all safeguarding technology be integrated to achieve truly layered, defense-in-depth security.

About Lumension Security, Inc.

Lumension Security, Inc., a global leader in endpoint management and 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, Antivirus 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 Texas, Florida, Washington D.C., Ireland, Luxembourg, Singapore, the United Kingdom, and Australia. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Lumension, Lumension Device Control, “IT Secured. Success Optimized.”, and the Lumension logo are trademarks or registered trademarks of Lumension Security, Inc. All other trademarks are the property of their respective owners.



Global Headquarters

8660 East Hartford Drive, Suite 300

Scottsdale, AZ 85255 USA

phone: +1.480.970.1025

fax: +1.480.970.6323

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Compliance and IT Risk Management