The 2015 Endpoint and Mobile Security Buyer's Guide

Version 3.0
Released: July 6, 2014

Securosis, LLC 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051 info@securosis.com www.securosis.com

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

This report is licensed by Lumension Security, whose support allows us to release it for free.

All content was developed independently.

lumension.com

Lumension Security, Inc., a global leader in endpoint management and security, develops, integrates and markets security software solutions that help organizations protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 3,000 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. 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.™

Copyright

This report is licensed under Creative Commons Attribution-Noncommercial-No Derivative Works 3.0.

http://creativecommons.org/licenses/by-nc-nd/3.0/us/

Table of Contents

The Ongoing Challenge of Protecting Endpoints 4

Anti-Malware: Protecting Endpoints from Attack 9

Endpoint Hygiene: Reducing Attack Surface 13

Managing Mobile Endpoint Security 19

Buying Considerations 26

Summary: Key Questions 30

About the Analyst 32

About Securosis 33

The Ongoing Challenge of Protecting Endpoints

Over the past few years Endpoint Security Management offerings — including patching, configuration, device control, and file integrity monitoring — have been bundled into suites to simplify management. Protecting endpoint devices continues to get harder, so the fine folks at Securosis need to continually refine our research. Our goal for this guide is to provide clear, up-to-date buying criteria for those of you looking at procuring these solutions in the near future.

The Ongoing Challenge of Securing Endpoints

Why is protecting endpoint devices hard? It can't be a matter of effort, right? Billions have been spent on research to identify better ways to protect these devices. Organizations have spent tens of billions on endpoint security products and services. But every minute more devices are compromised, more data is stolen, and more security folks need to explain— to senior management, regulators, and ultimately customers— why this keeps happening.

Don't think you are exempt. You have something that someone else wants to steal. You are a target, regardless of the size of your organization.

The lack of demonstrable progress comes down to two intertwined causes. First, devices are built using software with defects that attackers can exploit. Nothing is perfect, especially not software, and every line of code presents the potential for an attack. Second, employees can be fooled into taking action — such as installing software or clicking on a link — that results in a successful attack.

Don't think you are exempt. You have something that someone else wants to steal. You are a target, regardless of the size of your organization. With search engines and other automated tools looking for common vulnerabilities, everyone is a target.

Complicating matters, humans are inherently gullible and flawed. Regardless of any training you provide employees they continue to click links, share information, and fall for simple social engineering attacks. Endpoints remain some of the weakest links in your defenses. Even unsophisticated attacks on endpoints can still succeed, so adversaries do not need serious security Kung Fu to beat your defenses.

The industry has responded, but not quickly enough. A movement to take endpoints out of play is emerging. Whether using isolation technologies at the operating system or application layer, draconian whitelisting approaches, or even virtualized desktops, organizations no longer trust endpoints and have started building complementary defenses in response.

Emerging Attack Vectors

We mentioned the billions of dollars spent on research to protect endpoint devices more effectively. Why hasn't anything come from those investments in time and money? It gets back to attackers innovating faster than defenders. Even if the technology to protect devices more effectively were to emerge, it would take years for it to become widespread enough to blunt the impact of attackers across the broad market.

The reactive nature of traditional malware defenses — finding an attack, profiling it, and developing a signature to block it on device — is too little, too late.

The reactive nature of traditional malware defenses — finding an attack, profiling it, and developing a signature to block it on device — is too little, too late. Attackers now randomly change what their attacks look like using polymorphic malware, so looking for malware files doesn't solve the problem. Additionally, attackers have new and increasingly sophisticated means to contact command and control (C&C) systems and obscure data during exfiltration, making detection even harder.

Attackers do lot more testing than they used to making sure their attacks work before they launch them. Endpoint security technologies are inexpensive, so attackers refine their malware to ensure that it works against a majority of the defenses in use. But keep in mind "advanced attackers" are only as advanced as they need to be. If you leave the front door open, they don't need to sneak in through the ventilation ducts.

There is no point sugar-coating anything. Many successful attacks are caused by simple operational failures. Whether due to an inability to patch in a timely fashion or to maintain secure configurations, far too many organizations leave devices vulnerable. But that is not the attackers only path into your organization. They also target users via sleight-of-hand and social engineering. Employees unknowingly open doors for attackers and unwillingly facilitate compromise. Additionally, attackers are starting to target mobile devices since they have access to sensitive data on corporate networks.

Windows XP End of Life

When an operating system is at the end of its life and no longer receiving security updates it's a sitting duck. Attackers have free rein to continue finding exploitable defects with no fear of patches to ruin their plans. Windows XP security updates ended in April 2014. Although Microsoft did issue one patch to address a weaponized exploit, you can't assume that will always be the case. Organizations still using XP need to plan for their luck to run out — like luck has anything to do with it...

We know you're wondering why organizations serious about security — or even those not so serious — still use XP. It's a legitimate question with reasonable answers. For one, some legacy applications only run on XP. It might not be worth the investment (or even possible) to migrate the code to a more recent operating system, so on XP it stays. A similar situation arises with applications that have to be qualified by a government agency. We see this a lot in healthcare, where the OS can't even be patched without going through a lengthy and painful qualification process. That not going to happen, so on XP it stays. Thus, despite Microsoft's best efforts, XP isn't going away any time soon. Unfortunately, all this means that XP will remain a common target, and organizations need a means to protect the devices they cannot upgrade.

Device Sprawl

Remember the good old days, when 'devices' were DOS PCs and a few dumb terminals? The attack surface was the floppy drive. Those days are long gone. Today, we have a range of PC variants running numerous operating systems. They might be virtualized and they may connect in from anywhere in the world — including networks you do not control. Even better, many employees carry smartphones in their pockets, and "smartphones" are really computers. And don't forget tablet computers, each with as much computing power as a 20-year-old mainframe.

Remember the good old days, when 'devices' were DOS PCs and a few dumb terminals? The attack surface was the floppy drive. Those days are long gone.

The recent wave of attacks on retailers has brought Point of Sale (PoS) systems to the forefront of many organizations' thinking. These devices typically use older operating systems, are infrequently patched, and are often used by technologically unsophisticated tellers in stores. Compounding the issue, the retailers don't offer adequate security training. So, PoS systems constitute yet another platform that must be better protected, especially given the sensitive nature of the protected information captured by these devices.

Most attacks start with just one compromised device. More devices mean more complexity, more attack surface, and a higher likelihood of something going wrong. You need to execute your endpoint security strategy flawlessly — but you already knew that.

BYOD and Mobility

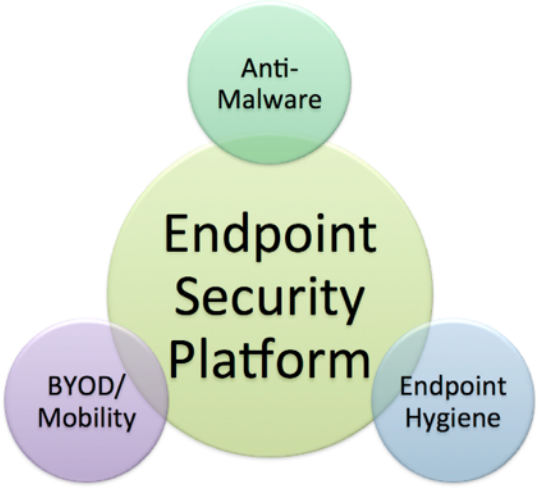
As uplifting as dealing with emerging attack vectors, end-of-life operating systems, and device sprawl is, we're not done complicating things. Now you need to broaden your definition of an endpoint. Many organizations support employee-owned devices, as well as contractor's devices. Moreover, business partners may have authorized third party access to your networks and critical data stores, connecting with devices you don't manage and/or control.

Most folks assume that Bring Your Own Device (BYOD) only applies to those pesky Android phones, iPhones, and iPads. But many finance folks are itching to get all those PCs off the books. That means you will eventually need to support just about any variety of PC or Mac an employee or contractor wants to use.

Of course the security controls you put in place need to be consistent whether a device belongs to your organization or the employee. The difference is granularity of management. If a corporate device is compromised, you just nuke it from orbit, as they say. That involves wiping the machine down to bare metal to ensure no vestiges of malware remain. But nuking devices you don't own can be problematic. What about those pictures of Grandma on an employee's device? What about their personal email and address book? How do you think a contractor will react when you nuke information related to other clients? Blow those away, and you're likely to meet with a louder uproar than if you'd just idled someone for a few hours while they waited to get their work desktop back.

Defining Endpoint Security

Before we jump into specifics let's consider what we mean by "endpoint security":



- **Anti-Malware:** Security researchers write entire books about how to detect today's modern attacks and malware. In this paper, we'll just cover the highlights of how anti-malware is packaged and what to look for. We'll also mention some advanced detection techniques emerging to stop the relentless tide of attacks. For a more thorough discussion, see our papers on Evolving Endpoint Malware Detection and Malware Analysis Quant.

- **Endpoint Hygiene:** The operational aspects of reducing device attack surface are an integral part of an endpoint security strategy. You do that by ensuring you have sufficient capabilities to manage patches and enforce security configuration policies. You need to lock down device ports — typically called "device control." We covered the issues in deploying these technologies in Implementing and Managing Patch and Configuration Management.

- **BYOD and Mobility:** Finally, you need to think about employee-owned devices and those that don't fit the traditional definition of a PC. So we will briefly discuss how tools such as Mobile Device Management (MDM), Mobile Application Management (MAM), and other security controls (including device containers) have emerged to provide simple management of these devices.

- **The Endpoint Security Platform:** The centerpiece of the endpoint security platform is an asset management capability and console to define policies, analyze data, and generate reports. Platforms should include advanced capabilities for asset management and discovery, policy management and alerting, analytics, and reporting. This is the glue that makes a comprehensive endpoint security strategy work.

Anti-Malware: Protecting Endpoints from Attack

Now let's turn our attention to the anchor feature of any endpoint security offering: anti-malware. Anti-malware technologies have been maligned because malware attacks are still largely successful despite widespread deployment of the technology. So we need some perspective — not only on where anti-malware has been, but also on where the technology is going, and how that impacts endpoint security buying decisions.

History Lesson: Reacting No Bueno

Historically, anti-malware technologies have utilized virus signatures to recognize bad files: a blacklist. It is ancient history now. As we reached tens of thousands of new malware samples per day, this model broke. Vendors could neither keep pace with the explosion of files to analyze nor update their hundreds of millions of deployed AV agents with gigabytes of signatures every couple of minutes. So vendors started looking at new technologies to address the limitations of blacklists, including heuristics to identify attack behavior within endpoints and reputation services to identify malicious IP addresses and malware characteristics.

> In light of modern randomly mutating polymorphic malware, expecting to reliably match identifiable patterns has become unrealistic — no matter how big a signature repository you build in the Cloud.

But the technology is still inherently reactive. Anti-malware vendors cannot protect against any attack until they see and analyze it. They need either a specific file, recognizable and identifiable tactics, or indicators to watch for. They need to profile each attack and push updated rules down to each protected endpoint. "Big data" signature repositories in the Cloud, cataloging known files both safe and malicious, have helped alleviate the issues that come with distributing billions of file hashes to each AV agent. If an agent sees a file it does not recognize, it consults the Cloud repository for a verdict. But that is still a short-term workaround for a fundamental issue with blacklists.

In light of modern randomly mutating polymorphic malware, expecting to reliably match identifiable patterns has become unrealistic — no matter how big a signature repository you build in the Cloud. Blacklists can block simple attacks using common techniques, but are completely ineffective against advanced malware attacks from sophisticated adversaries. Anti-malware technology needs to evolve, and it cannot rely purely on file hashes. We described the early stages of this evolution in Evolving Endpoint Malware Detection, so we will summarize here.

Better Heuristics

You cannot depend on reliably matching what a file looks like — you need to pay much more attention to what it does. This is the concept behind the heuristics that anti-malware offerings have begun using more frequently in recent years. Early heuristics didn't provide enough contextual information to know whether an executable was taking a legitimate action. Malicious actions were defined generically for each device, generally based on operating system characteristics, so false positives (blocking a legitimate action) and false negatives (failing to block an attack) were both common.

By understanding all the legitimate functions within a constrained universe of frequently targeted applications, you can eliminate a significant chunk of attack surface.

Heuristics have evolved to encompass authorized application behavior. This advancement has dramatically improved accuracy because rules are built and maintained for each application. Well, not every application, but at least the "big 7" applications targeted most often by attackers: browsers, Java, Adobe Reader, Word, Excel, PowerPoint, and Outlook. With new heuristics methods, these applications have been profiled to identify authorized behavior, and anything unauthorized is blocked. This is a type of whitelisting: only authorized activities are allowed.

By understanding all the legitimate functions within a constrained universe of frequently targeted applications, you can eliminate a significant chunk of attack surface. Here's a simple example: There really aren't any good reasons for a key-logger to capture keystrokes while filling out a form on a bank website. And it is decidedly fishy to take a screen capture of a form with PII on it. Previous detection technologies would have missed these activities — since both screen captures and reading keyboard input are legitimate functions in specific scenarios — but context enables us to recognize these behaviors as suspicious and stop them.

That doesn't mean attackers won't continue targeting operating system vulnerabilities, applications, and employees with social engineering. But these advanced heuristics have made a big difference in the efficacy of anti-malware technology.

Better Isolation

The next area of innovation on endpoints is the sandbox. We talked about sandboxing malware within a Network-based Malware Detection Device, which enables you to focus on what the file does before it executes on a vulnerable system. But isolation zones for detecting malicious code are appearing on endpoints as well. The idea is to spin up a walled garden in which to run a limited set of applications — the big 7, for example — shielding the rest of the device from applications that may be compromised.

Many security-aware individuals have been using virtual machines on endpoints to run these risky applications for years. But this approach only worked for the technically savvy and never saw broad usage within enterprises. To achieve market success isolation products must maintain a consistent user experience. It is still early for isolation technologies, but the approach — even down to virtualizing different processes within the OS — shows promise. Of course, it is important to keep in mind that sandboxes are not a panacea. If the isolation technology utilizes any base operating system services (network stacks, printer drivers, etc.), the device is still vulnerable to attacks on those services, even while running in an isolated environment. Isolation technology doesn't exempt machines from the need for hygiene (patching and configuration), the details of which we will discuss later in this paper.

Of course, it is important to keep in mind that sandboxes are not a panacea. If the isolation technology utilizes any base operating system services (network stacks, printer drivers, etc.), the device is still vulnerable to attacks on those services, even while running in an isolated environment.

As we extend the discussion to mobile endpoints, keep in mind that mobile device operating systems (predominately iOS and Android) are isolated by design. One of the key architectural constructs of these operating systems is that each app runs in its own space with limited access to the rest of the device. So does that mean you don't have to worry about anti-malware on smartphones and tablets? Well, that depends on what you consider anti-malware technology. These operating systems don't support the same level of executable inspection as traditional PCs. But it does make sense to scrutinize applications allowed to run on the devices, which we will discuss later in this paper.

Total Lockdown

Finally, there is the total lockdown option: defining an authorized set of applications or executables that can run on the device and blocking everything else. This Application Whitelisting (AWL) approach has been around for over 10 years, but remains a niche model for endpoint protection. It never became mainstream because it impacts the end-user experience too much. If an employee wants to run an unauthorized application they are out of business — unless either IT manages a quick authorization process (rare) or they get a "grace period" where the application can run for 24 or 48 hours until

administrators approve or reject it. The grace period model addresses the user experience challenges, but opens a hole in the security model. Though some organizations are willing to make this compromise in order to protect against unauthorized (and undesired) executables more effectively than traditional anti-malware technologies.

The user impact of AWL is much less of a problem on servers, because servers infrequently call the help desk to ask why they cannot install iTunes, so AWL can effectively these devices. Additionally, AWL is well suited to protect fixed-function devices (including kiosks) from malware, given the infrequently changing applications running on those devices. Organizations also tend to accept AWL on high-value endpoints, which need stronger protection from targeted malware.

The Future: Endpoint Activity Monitoring

These techniques are all designed to stop malware from executing on a device or to block malicious activity during execution. But that is not enough. Dormant malware may look like a harmless file today, but it might be detected as malicious tomorrow with new information and you'll want to know what's happened with that file. Given the endless supply of 0-day attacks and the wide variation in attack kits, you need to be prepared to will miss something. Then you will need to respond as quickly as possible, and it will be helpful to know on which devices the bad file was downloaded and on which it ran.

With the ability to search all devices for indicators you can move beyond the whack-a-mole approach of finding and fixing one device at a time. Instead, you can identify all devices impacted by a specific attack and then remediate in one fell swoop.

So the objective is to keep track of what happens on each endpoint at a very granular level at all times. We call that Endpoint Activity Monitoring — at least until the industry comes up with a better term. Yes, it imposes a heavy compute burden and can generate a large amount of data, but fortunately we have fancy big data and cloud analytics technologies to soak it up. For this approach you need to know what files were downloaded onto each device, which were executed, and what changes were made on each device — in great detail. Moreover, if you can profile malware as described in Malware Analysis Quant, you can query your endpoint activity monitoring platform for devices which show indications of that specific infection — regardless of when they were infected.

Protecting endpoints successfully still depends on reacting faster and more effectively. By shortening the window between infection and detection, you can remediate faster and contain damage with greater success. With the ability to search all devices for indicators you can move beyond the whack-a-mole approach of finding and fixing one device at a time. Instead, you can identify all devices impacted by a specific attack and then remediate in one fell swoop. We expect this to become a key capability of endpoint anti-malware technology over the next few years.

Endpoint Hygiene: Reducing Attack Surface

As we've already mentioned, anti-malware tends to be the anchor in endpoint security protection suites. Today's typical attacks justify that pattern. But too many organizations forget the importance of keeping devices up-to-date and configured securely. Even "advanced attackers" don't burn 0-day attacks when they don't need to. Leaving long-patched vulnerabilities exposed or keeping unnecessary services active on endpoints makes it easy for attackers to own your devices. In almost every attack, regardless of the attacker's sophistication, the attacker will compromise a device, gain a foothold, and then systematically move toward the target.

By ensuring proper hygiene on devices, you reduce the attack surface — if attackers want to get in, make them work for it. When we refer to "hygiene," that encompasses three main functions: patch management, configuration management, and device control.

When we refer to "hygiene," that encompasses three main functions: patch management, configuration management, and device control.

Patch Management

Patch managers install fixes from software vendors to address vulnerabilities. The most well-known patching process is Microsoft's monthly Patch Tuesday, when the company issues a variety of software fixes to address defects in its products — many of which could result in system exploitation. Other vendors have adopted similar approaches, with a periodic patch cycle and out-of-cycle patches for more serious issues.

Once a patch is issued, your organization needs to assess it, figure out which devices need to be patched, and install the patch within the window specified by policy — typically a few days. A patch management product scans devices, installs patches, and reports on the success or failure of the process. Our Patch Management Quant research provides a detailed view of the patching process, so refer to it for more information.

Patch Management Technology Considerations

- **Coverage (OS and applications):** Your patch management offering needs to accurately support the operating systems and applications you need to keep current. Top priority is ensuring the big 7 vulnerable applications (browsers, Java, Adobe Reader, Word, Excel, PowerPoint, and Outlook) are well covered. Keep in mind that the word "supported" on a vendor's data sheet doesn't necessarily convey the quality of the support. Be sure to test their patch library and the timeliness of their updates.

- **Discovery:** You can't manage devices you don't know about, so you need a way to identify new devices via a built-in discovery capability, bidirectional integration with vulnerability management (for active and passive monitoring of new devices), asset management and inventory software, or, more likely, all of the above.

- **Reliable deployment of patches:** If patches don't install consistently, that means more work for you. Faulty installation of patches can easily make a tool more trouble than it's worth.

- **Agent vs. agentless:** Does the patch vendor assess devices with an agent, or does it perform "agentless" scanning (typically using a non-persistent or "dissolvable" agent). In either situation, how do they deploy patches? While advocates for both strategies argue about which is better, fortunately, both models are proven to work. If the patch manager requires an agent, it should be integrated with any other endpoint agents (anti-malware, device control, etc.) to minimize the number of agents per endpoint.

- **Remote devices:** How does the patching process work for remote and disconnected devices? This category includes field employees' laptops as well as devices in remote locations with limited bandwidth. What features are built in to ensure that the right patches are deployed, regardless of location? Can you be alerted when a device has not updated within a configurable window — perhaps because it's been off the network?

- **Deployment architecture:** Some patches are gigabytes in size so patch distribution flexibility is important — especially for remote devices and locations. Architectures may include intermediate patch distribution points to minimize network bandwidth, as well as intelligent packaging to install only appropriate patches on each device.

- **Scheduling flexibility:** Of course, disruptive patching must not impair productivity, so you should be able to schedule patches during off hours and when machines are idle.

- **Value-add:** As you consider a patch management tool, make sure you fully understand the value it adds — what distinguishes it from low-end and free or low-cost operating system-based tools such as Microsoft's WSUS. Make sure the tool supports your process and provides the capabilities you need.

Configuration Management

Configuration management enables an organization to define an authorized set of configurations for devices. These configurations control applications installed, device settings, running services, and on-device security controls. Another aspect of configuration management is the ability to assess configurations and identify changes, which is important because unauthorized configuration changes often indicate malware manipulation or potentially exploitable operational error. Additionally, configuration management can help ease the provisioning burden of setting up and reimaging devices in case of infection.

Configuration Management Technology Considerations

- **Coverage (OS and applications):** Your configuration management offering needs to support your systems.
- **Discovery:** As mentioned above, you cannot manage devices you don't know about, so you need a way to identify new devices — otherwise this process will fail. You can achieve this with a built-in discovery capability, bidirectional integration with vulnerability management (for active and passive monitoring for new devices), asset management and inventory software, or more likely all of the above.
- **Supported standards and benchmarks:** The more built-in standards and/or configuration benchmarks offered by the tool, the more likely you'll find something you can easily adapt to your own requirements. This is especially important for highly regulated environments, which need to support and report on multiple regulatory hierarchies.
- **Policy editing:** Policies generally require customization to satisfy requirements. Your configuration management tool should offer a flexible policy editor to define policies and add new baseline configurations and benchmarks.
- **Scalability:** Scanning each device for configuration changes can be demanding on both endpoints and the network, so understand how to distribute scanners effectively and ensure that scanning frequency is flexible to ensure you can scale to the size of your environment.
- **Remote devices:** How do assessment and management work for remote and disconnected devices? This includes field employees' laptops as well as devices in remote locations with limited bandwidth. What kind of recovery features are built in to ensure devices are assessed in a timely fashion and remediated correctly, regardless of location? Can you be alerted when a device has not updated within a configurable window — perhaps because it is not on the network?
- **Agent vs. agentless:** Does the configuration management vendor assess devices with an agent, or do they perform 'agentless' scanning (typically using a non-persistent 'dissolvable' agent), and if so how do they apply changes? This is almost a religious dispute but fortunately both models work. If the configuration manager requires an agent it should be integrated with any other endpoint agents (anti-malware, device control, etc.) to minimize the number of agents per endpoint.

- **Integration with operational process:** Make sure any identified configuration issues are reported to the central help desk system to close the operational loop, ensuring a proper process for authorizing and applying changes. You can take care of this within the endpoint security platform but integrating with enterprise systems can make things easier.

- **Exception management:** As mentioned above, there may be situations where a configuration change represents an authorized exception. To make things more fun, authorization is often granted *after* configuration management detects (and perhaps reverses) the change. You must be able to handle these situations without bogus alerts every time the device is assessed.

- **Value-add:** As you consider a configuration management tool, make sure you fully understand the value it adds — what distinguishes it from low-end and free or low-cost operating-system-based tools such as Microsoft's SCCM. Make sure the tool supports your process and provides the capabilities you need.

For more detail on patch and configuration management, see Implementing and Managing Patch and Configuration Management.

Device Control

End users love the flexibility USB ports provide for "productivity." Unfortunately, that means your employees not only have the ability to share music with buddies, but also the ability to download your entire customer database onto their phones. It all became much easier once the industry standardized on USB a decade ago. The ability to easily share data has facilitated employee collaboration but also greatly increased the risks of data leakage and malware proliferation. Device control technology enables you to enforce policy— both for who can use USB ports and how — and to capture whatever is copied to and from USB devices. As an active control monitoring and control over device usage addresses a major risk.

Device Control Technology Considerations

- **Device support:** Start by confirming the vendor supports the devices you need to protect. That includes operating system support as well as media types (removable storage, CDs & DVDs, tape drives, printers, etc.) on which to enforce policies. Make sure the product supports all the ports on your devices, including USB, FireWire, serial, parallel, and Bluetooth.

- **Policy granularity:** Make sure the product can support different policies for different devices. For example, by enabling you to set a policy that lets an employee download any data to secure, encrypted USB devices but only non-critical data to smartphones. You should be able to set up different policies for different classes of users and groups, as well as by type of data (email vs. spreadsheets vs. databases). You may want to limit the amount of data that can be copied by some users. This list is not exhaustive, so make sure your product supports the policies you need.

- **Encryption support:** If you encrypt data on removable media, make sure your product supports your preferred encryption algorithms and/or hooks into your key management environment. You may also be interested in certifications such as EAL (Common Criteria), FIPS 140-2, etc.

- **Small footprint, secure agent:** To implement device control, you need an agent on each protected device. Besides making sure the agent is not stealing massive amounts of compute power from each device, also ensure some kind of tamper resistance exists to protect agents from being disabled or subverted by an attacker.

- **Integration with endpoint security platforms:** Don't reinvent the wheel, especially for cross-functional capabilities such as discovery, reporting, agentry, and agent deployment/updating/maintenance. Utilize your endpoint security platform to streamline implementation and leverage operationally. Ideally, a common agent should handle anti-malware, patching, configuration management, and device control.

- **Offline support:** Devices are not always connected to the network, so make sure policies are still enforced even when disconnected. Make sure policy violation alerts are forwarded to the main console when devices reconnect, so administrators know of potential issues.

- **Forensics:** In the event of data loss, you will want detailed forensic information enabling a deep investigation of the attack. Thus, logging all user activity is critical. Some offerings copy any files copied to protected device ports to provide a smoking gun in case of data loss.

- **Exception management:** There are times when policy may simply need to be overridden, like when your CEO is trying to get a deal done at the end of the quarter and needs to share an agreement with a customer. Having the ability to allow certain employees to override policies (with proper alerting and audit trails) can prevent tools from causing their own problems *and* keep you employed.

Organizational Buying Considerations

Device hygiene tools are mature, so how should you choose between them? We go into detail on the buying process later in the paper, but your choice depends on who is responsible for keeping up device hygiene. If it's Operations, an operations-oriented platform with broad data center and server management capabilities is probably the way to go. On the other hand, if the endpoint/device team is responsible, a tool or platform optimized for endpoints makes more sense. If auditors are driving the search, focus on assessment for validation and reporting. If different teams handle different functions, an integrated platform may not offer significant leverage. There is no *right* answer to this question, but make sure you consider operational responsibilities as you work through the process.

If different teams handle different functions, an integrated platform may not offer significant leverage. There is no right answer to this question, but make sure you consider operational responsibilities as you work through the process.

Another point to keep in mind is that mature products rarely differ radically from each other. There are always differences in user experience and other marginal features, but primary feature sets converge over time. Our recommendation is to first decide how you want to work, and then find a tool or platform to automate it.

Managing Mobile Endpoint Security

Endpoint security is evolving pretty quickly, as is apparent from our recent deep dive into Advanced Endpoint and Server Protection. We believe that mobile devices are just additional endpoints that need to be managed like any other device, but the increasing importance and rapidly advancing capabilities of these devices demands special attention.

> Security becomes a consideration only after management issues are under control. Security becomes a consideration only after management issues are under control.

To provide some context, we have said for years that management is the first problem users solve when introducing a new technology. Security becomes a consideration only after management issues are under control. That has certainly been true of mobile devices — as evidenced by the rapid growth, maturity, and consolidation of Mobile Device Management (MDM) technologies. But you cannot really separate management from protection in the mobile endpoint context, as demonstrated by the fact that security features appeared early among MDM offerings.

Mobile devices are inherently safer from malware attacks due to their more modern mobile operating system architectures. Thus hygiene — including patching, configuration, and managing the applications that run on the devices — becomes the key security requirement. Given ongoing investments in traditional endpoint hygiene (as described earlier in the paper), you can gain leverage by integrating mobile devices into the device management stack (where applicable) to enforce consistent policy regardless of device, ownership (for BYOD), or location. This has driven significant consolidation of mobile management companies into broader IT management players.

Defining Endpoints

One of our key points early in this paper is that our definition of 'endpoint' is more inclusive. From a security standpoint, if the device can run applications, access corporate data stores, and store corporate data locally, it is an endpoint and as such needs to be managed and protected. Smartphones and tablets clearly meet these qualifications along with traditional PCs.

From an organizational perspective management of all these devices may not fall within a single operations group. Each company's operational model reflects business realities, particularly at large-scale enterprises with thousands of employees and huge IT shops, which can afford separate teams specialized by device. In many smaller companies (the mid-market), we generally see these operational functions consolidated. But who does the work is less important than what is done to protect mobile endpoints— consistently and efficiently.

Managing Endpoint Device Security

Here is what hygiene means in the mobile endpoint context:

- **Enrollment:** New devices keep showing up, so registering each device and assigning it proper entitlements begins the process of managing it. This is typically handled via a self-service capability allowing users to register their devices and accept the organization's policies (especially for employee-owned devices) without waiting for help desk intervention. Of course, you cannot assume everyone gaining access will register their devices (especially attackers), so you will need some kind of passive discovery capability to identify unmanaged devices when they appear.

- **Asset management:** After enrollment comes the need to understand and track device configuration and security posture, which is really an asset management function. There may be other similar capabilities in use within the organization (such as a CMDB), in which case integration and interoperability with those systems is a requirement.

- **OS configuration:** Configuration of mobile endpoints should be based on policies defined by organizational groups and roles. These policies typically control many aspects of the devices — including password strength requirements, geolocation tracking, activation lock, and device encryption. OS vendors offer robust and mature APIs to provide access to managed the devices, thus most mobile endpoint management platforms will just leverage the APIs. Platform selection largely comes down to a question of leverage — how to best managing and enforce policies with a consistent user experience across all devices.

Platform selection largely comes down to a question of leverage — how to best managing and enforce policies with a consistent user experience across all devices.

- **Patching:** Software updates are critical to device security, so ensuring that mobile endpoints are patched in a timely fashion is another key to mobile endpoint security. For mobile devices, you will need to be sure that you can update device remotely (typically over the air via Wi-Fi or cellular connections) since they are often beyond reach of the corporate.

- **Connectivity:** An organization may want to actively control which networks the devices use, especially because many public Wi-Fi hotspots are simply insecure. So you will need the ability to specify and enforce policies for which networks devices can use, whether connections require a VPN to backhaul traffic through a central gateway, and whether to use a mobile VPN service to minimize the risk of snooping and man-in-the-middle and side-jacking attacks.

- **Identity/group roles and policies:** This involves integrating the mobile endpoint security management policy engine with Active Directory or another authoritative identity store. This leverages existing users and groups — managed elsewhere in the organization — to set MDM policies.

As you build your mobile endpoint security management strategy keep in mind that different operating systems offer different hooks and management capabilities. Mature PC operating systems offer one level of management maturity; mobile operating systems are maturing rapidly but offer considerably less control — and likely always will One way to address this reality is to reduce protection to the lowest common denominator of your least capable platform. Obviously as security folks, we believe that's a bad option.

Alternatively, you can choose to support only certain functions/capabilities on certain devices. For example, you could implement a policy requiring PCs to access corporate data (and SaaS applications) over the corporate VPN, so that class of devices is easier to compromise and present more risk. But less restrictive policies for mobile devices, factoring in its better inherent protection might be within the risk tolerance of your organization.

This granularity can be established via policies within the endpoint security management platform. Over time MDM platforms will be able to compensate for limitations of underlying operating systems to provide stronger protection.

The improved security architectures of mobile operating systems have required attackers to target applications to access data and compromise devices.

Managing Applications

The improved security architectures of mobile operating systems have required attackers to target applications to access data and compromise devices. In order to protect mobile endpoints, you need to protect applications as well. This requires several capabilities:

- **Authorized applications:** A common concept for application protection is the "corporate app store," which enables organizations to offer a whitelist of authorized applications with centralized purchasing, deployment, and configuration. This entails management of updates (similar to mobile OS patching and configuring, mentioned above) and the removal of apps that violate corporate policies.

- **Application Controls:** Diving deeper into application control, mobile endpoint security requires more granular control over the device's built-in apps, including email and web browsers. Organizations may restrict access to corporate email or web resources to apps that run inside a corporate container. Additionally, if organizations choose to control what employees browse, they can enforce web browsing policies on-device rather than on a corporate web security gateway. You may need to enforce application restrictions on third party apps, so factor in broad application support as well.

- **Privacy/personal data leakage:** One of the hot buttons for mobile endpoints is privacy. Individual privacy may be at odds with what's acceptable for a corporation. For example, many employees allow apps access to their contact lists and text messages without thinking about it. But this presents a clear security issue when business contacts or texts are stored on devices. Organizations can manage potential leakage by controlling what applications have access to what information on the device. Given the wide variance of app capabilities, it is also helpful to be able to access app security/privacy ratings, so you understand which apps might misuse data and violate policies.

This leads to the question of what security means to us in a mobile endpoint context. We increasingly see vendors in this space talk about privacy and security interchangeably. Many apps are deemed insecure because they have access to other resources on the device (as described above). But that is really a privacy issue because data is being shared with the app. We can simplify the discussion down to the root: whether an app is exploiting a vulnerability or other mechanism to provide unauthorized access to the device (a security issue) or legitimately accessing information it shouldn't be able to (a privacy issue). But both increase risk to the organization, and, so that risk needs to be understood and managed.

Managing Data on Mobile Devices

Today's mobile endpoints have as much onboard storage as mainframes of yesteryear, so any employee can hold a significant amount of your organization's intellectual property on his or her smartphone. This makes data protection a critical aspect of mobile endpoint security. We recently produced a much more detailed analysis of protecting data on iOS 7, so we suggest you check that out to go deep on mobile data protection architectures and advanced content management strategies. Here are some high-level considerations for buyers:

- **Remote wipe:** Sometimes the data on a device needs to be removed, like when a lost device needs to be wiped or an employee leaves the organization. Your mobile endpoint security management platform should be able to selectively wipe devices remotely, ensuring that only corporate data is erased while preserving Grandma's pictures.

- **Data protection:** How the data is stored on devices is also pertinent. A number of different architectures exist that encrypt data at rest and as it moves to and from the mobile devices. Operating system vendors tend to handle storage encryption, and you will need to think about how each app handles and protects data in local storage. Again, consult our iOS 7 data protection paper for a more detailed discussion.

- **Containers:** As described above, some organizations want to restrict access to corporate data within a walled garden on the device, otherwise known as a 'container.' This approach provides convenient access to the corporate app store and approved apps — including secure email and web browsing, along with other apps with access to corporate data. Security and management of the container is critical. Make sure to understand its data protection architecture thoroughly before trusting it with sensitive data.

Management Leverage

We increasingly expect mobile security capabilities to be bundled with broader endpoint security and IT management offerings. We've seen almost every emerging market start as standalone technology that ultimately gets wrapped into a broader offering. Nowhere is this more apparent than with management technologies. We have already seen significant consolidation of MDM players, and these capabilities increasingly become features of major IT/security management offerings. Smartphones and tablets don't need to be managed differently, although that is a choice your organization might make. To be clear, this does not mean all the independent mobile management/security companies will go away, or that there is no room for innovation. But we expect only a few to stay independent over the longer term. This pattern necessarily impacts buying decisions. In early markets independent companies (also known as "best of breed") tend to bring more fully featured offerings to market. If your requirements are less stringent, you might want to look at a bundled offering from the beginning, because many endpoint security and management vendors already provide some mobile security/management capabilities.

To be clear, this does not mean all the independent mobile management/ security companies will go away, or that there is no room for innovation. But we expect only a few to stay independent over the longer term.

Buying dynamics aside, there is leverage to be gained using a bundled suite. The need to patch and enforce configuration policies is universal, regardless of device. If you can do that within a single user experience, bundling is advantageous so long as you don't have to sacrifice policy granularity to operating system differences. The need to protect data spans devices, so common policies can be implemented here as well. Finally, all these endpoint devices are assets, so centralizing asset management and tracking (through mobile geolocation tracking and periodic assessments) is also

useful. This all helps with compliance as well, providing a common reporting infrastructure to substantiate controls for protecting private data on all endpoints.

If you choose to centralize security management of both PCs and smartphone/tablet devices, you will want the ability to define roles within the management environment to support your organizational model. If you have personnel detailed to manage only smartphones, they don't need access to PC management or vice-versa. You will also need to decide the location of your management infrastructure — whether on-premise or in the Cloud. Cloud-based management is becoming pervasive for its ease of deployment and transparent updates. But one size doesn't fit all. You might prefer a local management platform to accommodate specific security or cultural requirements, or want to plug into an existing on-site management console.

Another aspect of selecting a security management platform is integration with other enterprise systems — specifically identity (to define entitlements and access rights) and network security (to restrict certain devices to specific network segments).

Employee-Owned Devices

As mentioned above, we don't see any good reason to limit securing employee-owned devices (BYOD) to smartphones and tablets. Employees may want to run office applications in a virtual window on their new Mac, not their assigned 4-year-old Windows XP laptop, and you should let them. You need to secure devices regardless of operating system or physical device, and whether your organization owns them. This changes how you provision and protect mobile endpoints, particularly in terms of enforcement granularity.

For devices you don't own, you need to selectively enforce policies. It's not practical to dictate what applications employees run on equipment they own. Likewise, you cannot determine which websites they can visit on their own machines on their own time, off the corporate network. You probably shouldn't arbitrarily nuke devices from orbit if you see ambiguous malware indicators. If your policy allows it, you can legally control and wipe the device. But it is probably not worth the headaches and backlash to blow away a device, deleting a bunch of personal pictures and videos, and demonstrating unambiguously to employees that you are watching them with power to delete all their data — even on their own devices.

So the key is granularity. It is reasonable to perform periodic vulnerability scans on each device to ensure it's patched effectively. It is reasonable to require devices to be encrypted so corporate data is protected. It is fair to block access to corporate networks from any device, which isn't configured properly or seems to be compromised.

Let's consider the impact of employee-owned devices on aspects of endpoint security we have discussed already:

- **Anti-malware for BYOD:** If you require anti-malware on corporate-owned computers, you probably want or need to require it on employee-owned machines as well. Anti-malware may be required by compliance mandates for devices which access protected information. The question is whether to require each employee to use the corporate standard anti-malware solution. If so, you would use the existing anti-malware solution's enterprise management console. If not, you need the capability to confirm whether anti-malware protection is running on each device on connection possibly via a technology like network access control (NAC). Additionally, you need to decide whether you will mandate anti-malware protection for mobile devices, given the lack of malware attacks on most mobile platforms.

- **Hygiene for BYOD:** Under our definition (patch management, configuration management, and device control), the key change is reassessment of the security posture of employee-owned devices on each connection to the network. Then it comes down to a policy decision: whether you allow insecurely configured or unpatched devices on your network or patch and update devices as necessary using enterprise management tools, which may incur a software licensing cost.

Dealing with employee-owned devices requires you to review each security policy to determine whether it needs an update for BYOD. It is a good idea to make sure you can both visualize and report on employee-owned devices because ensuring they comply with mobile endpoint security policies can be a sensitive subject. In terms of enforcement, you should be able to selectively enforce applicable policies, reducing organizational risk while maintaining employee freedom. That's a tough standard to meet, but it's critical to employees and management.

Buying Considerations

We will conclude with buying considerations, which will help you decide between one solution or another. We also offer you a procurement process to select the technology.

Platform Features

As in most technology categories (at least in security), the management console (or "platform") connects the sensors, agents, appliances, and any other security controls. You need several platform capabilities for endpoint security:

- **Dashboard:** You should have user-selectable elements and defaults for technical and non-technical users. You should be able to show only appropriate elements, policies, and alerts to different users or groups, typically with entitlements stored in the enterprise directory. Nowadays, given the state of widget-based interface design, you can expect a highly customizable environment, letting each user configure what they need and how they prefer to see it.

- **Discovery:** You cannot protect an endpoint (or any other device) if you don't know it exists. So the next key platform feature is discovery. Surprise is the enemy of the security professional, so make sure you know about new devices (including mobile devices) as quickly as possible.

- **Asset repository integration:** Closely related to discovery is the ability to integrate with an enterprise asset management system or CMDB for a heads-up whenever a new device is provisioned. This is essential for monitoring and enforcing policies. You can learn about new devices proactively via integration or reactively via discovery. But either way, you need to know in a timely fashion what's out there.

- **Policy creation and management:** Alerts are driven by the policies you implement, so policy creation and management are essential.

- **Agent management:** Anti-malware defense requires a presence on the endpoint device. You need to distribute, update, and manage agents in a scalable and effective fashion. You need alerts when a device hasn't updated for a certain period of time, along with the ability to report on the security posture of endpoints.

- **Alert management:** A security team is only as good as its last incident response making alert management is critical aspect of mobile endpoint security. Alerts enable administrators to monitor potential malware attacks and policy violations that might represent attacks. Time is of the essence during any response, so you need further detail via drill-down and to send relevant information into a root cause analysis/incident response process. The interface should be concise, responsive, customizable, and easy to read at a glance. When an administrator drills down into an alert, the display should clearly and concisely summarize the reason for the alert, the policy violated, the user(s) involved, and any other information helpful for assessing criticality and severity.

- **System administration:** Pay attention to the experience and capabilities for user and group administration, since that's a huge issue when managing multiple devices for all of the employees in an organization. For more widely distributed environments you will want some kind of role-based access control (RBAC) and hierarchical management to manage access and entitlements for a variety of administrators with varied responsibilities to reflect your organizational operational model.

- **Reporting:** Compliance tends to fund and drive investments in endpoint security technologies, so substantiating and documenting efficacy is a requirement. Look for a mixture of included customizable reports and tools to facilitate ad hoc reporting both at the specific control level and across the entire platform.

Cloud vs. Non-cloud

Cloud-based offerings for endpoint security have forced many organizations to evaluate the value of running a management server on-premise. The Cloud fashionistas focus on the benefit of not having to provision and manage a server or set of servers to support the endpoint security offering, which is especially painful in multi-site environments. They talk about continuous and transparent updates to the interface and feature set of the platform without disruptive software upgrades. They may even mention the ability to have the environment monitored 24/7, with contractually specified uptime. And they are right about all these advantages.

But for an endpoint security vendor to manage their offering from the Cloud, they need to do more than just load the existing software onto a bunch of AWS instances.

But for an endpoint security vendor to manage their offering from the Cloud, they need to do more than just load the existing software onto a bunch of AWS instances. The Cloud infrastructure needs to provide data segregation and protection for multi-tenancy. And the user experience needs to be rebuilt for remote management, because there are no longer "local" endpoints on the same network as the management console. Make sure you understand the vendor's technology architecture and how they protect your data in their Cloud, not just in transit.

Get a feel for service levels, downtime, and support for the cloud offering. It is great to have one less server on your premises, but if the service goes down and your endpoints are either bricked or unprotected that on-premise server will look pretty good.

Understanding Intangibles

After doing your research to determine which platforms can meet your requirements, you need to define a short list and then choose something. One decision point involves large vs. small vendors. Given the pace of mergers and acquisitions in the security space, even small vendors may not remain small and independent forever. As a rule, every small vendor is working constantly to get big — either by selling more stuff or finding a larger partner.

Given the pace of mergers and acquisitions in the security space, even small vendors may not remain small and independent forever. As a rule, every small vendor is working constantly to get big — either by selling more stuff or finding a larger partner.

Working with a larger vendor is all about leverage. Organizations can achieve pricing leverage by buying multiple products and services from the vendor and negotiating a nice discount on all their products. But smaller vendors can get aggressive on pricing as well, and sometimes have even more flexibility to discount. Platform leverage stems, from using multiple products managed via a single console. The larger endpoint security vendors offer comprehensive product lines of products you might need, and an integrated console can make operations easier. In a nutshell, pay attention to the total cost of managing the environment — not just on the initial purchase price.

Given the importance of intelligence for tracking malware and keeping current on patches and configurations, it is important to consider the size and breadth of the vendor's research team and customer base. Keeping policies current and issuing effective updates requires a huge dataset and serious analysis capability; more is required to figure out what needs to be done. You will probably hear a lot about big data, the buzzword *du jour*. More important is the vendor's investment in keeping its platform current.

Ensure your vendor has the ability to support your environment, wherever it is. Local support is best for dealing with endpoints because you may not have capable staff on-site to troubleshoot. But as time goes on we will see improved collaboration with better remote management and troubleshooting tools making centralized support increasingly viable for a global customer base with a cloud-based deployment.

Purchasing Cycle

Some organizations are formal and issue RFI/RFP (Requests For Information/Proposals). Others work with resellers or rely on personal contacts to learn about alternatives and negotiate deals. However you buy products and services, you are likely to go through the same basic process:

1. **Define requirements:** Don't dismiss the need for internal fact-finding and requirement gathering before engaging with vendors. Know what you're buying and why. Understand what works in your environment and what doesn't. Get a feel for the importance of each function. Is anti-malware your most important requirement, or are you more concerned with managing the patch cycle across a highly distributed user community? Once you answer those questions and questions like them, you will know what you need an endpoint security platform to do.

2. **Establish a short list:** This may be a formal or informal process. You need a handful of vendors who can meet your requirements. Talk to them and dig deeper into their products and services to figure out which vendors can really solve your problems.

3. **Test products:** Set up a test bed and let the tools do their thing. Depending on which controls you are looking to implement, you can run all sorts of tests during proof of concept. Figuring out the device overhead of agents is key, as is the user experience of setting policies, managing alerts, and remediating issues. Keep in mind that you won't really be able to compare effectiveness of anti-malware protection without a library of 0-day attacks, so you may need to rely on third-party tests and reviews.

4. **Talk to your buddies:** Given the challenges of comparative anti-malware testing, you should probably reach out to security peers in other organization to hear which endpoint security offerings they use, as well as what works and doesn't.

5. **Try support:** Make sure you put a number of calls into the vendor's support team. Call during both typical business hours and off-hours to understand how they'll support you when it counts.

6. **Negotiate:** We could write a book about vendor negotiation, but for now suffice it to say that leverage is good. Try to negotiate with at least two vendors to get them competing for your business. And don't believe them when they say end of quarter discounts don't happen. Unless the sales rep is way ahead of quota, they deal at the end of the quarter.

We could go much deeper into purchasing. It's a discipline like any other aspect of a security professional's job. But this high-level process should serve you well as you procure an endpoint security offering.

Summary: Key Questions

Normally we wrap up each paper with a nice summary that goes through the high points of our research and summarizes what you need to know. But this is a Buyer's Guide, so we figured you would get more value out of a list of questions to ask endpoint security vendors. With apologies to Alex Trebek, here are 10 key areas we would delve into with vendors if we were buying this technology today.

1. What specific controls do you offer for endpoint management? Can the policies for all controls be managed via your console? How do policies differ based on device type (PC, Mac, iOS, Android, etc.)

2. Does your organization have an in-house research team? How does their work make your endpoint security product better?

3. How do you handle 0-day malware? What about dormant malware that doesn't execute immediately?

4. What products, devices, and applications can be patched with the offering? How quickly after the vendor issues a patch can we install it in our environment?

5. What standards and/or benchmarks are offered out of the box with your configuration management offering?

6. What kind of agentry is required for your products? Is the agent persistent or dissolvable? How are updates distributed to managed devices? How do you ensure agents are not tampered with? How do you handle mobile, remote, and disconnected devices?

7. How do you support mobile devices and/or virtual desktops (VDI)? Do you offer any capabilities specifically to handle employee-owned devices (BYOD)? Do you do anything to manage applications on endpoint devices?

8. Where does your management console run? Do we need a dedicated appliance? What kind of hierarchical management do you support? How customizable is the management interface?

9. What kinds of reports are available out of the box? What is involved customizing specific reports?

10. What have you done to ensure the security of your endpoint security management platform? Is strong authentication supported? Have you performed a penetration test on your console? Does your engineering team use any kind of secure software development process?

We could write another 100 questions, but these hit the highlights of dealing with today's malware attacks, device/application patching and configuration, research/intelligence, securing mobile endpoints, platform consistency/integration, and management console capabilities. Our list cannot replace a more comprehensive RFI/RFP, but it can provide a quick idea of whether a vendor's product family can meet your requirements.

The one aspect of buying endpoint security that we haven't really discussed appears in question 6 (agents) and question 10 — the security of the management toolset itself. Attacking the management plane is like attacking a bank rather than individual account holders. If the attacker can gain control of the endpoint security system, they can change policies and circumvent your controls. But that is just the beginning of the risks of a management environment compromise.

Attacking the management plane is like attacking a bank rather than individual account holders.

As we described, endpoint security has two major components: anti-malware and hygiene. Hygiene is relatively mature technology, so look less at specific feature/capability differentiation and more at policy integration, console leverage, and user experience. Anti-malware technology, on the other hand, is evolving rapidly through significant innovation.

Your procurement process needs to balance innovation against maturity. Given this backdrop and the criticality of blocking malware, ensure that you are confident that your endpoint security vendor is able to block attacks and that their management capabilities will reduce your attack surface. That approach should yield the most effective solution for your environment.

If you have any questions on this topic or want to discuss your situation specifically, feel free to send us a note at info@securosis.com or ask via the Securosis Nexus <https://nexus.securosis.com/>.

About the Analyst

Mike Rothman, Analyst/President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **The Securosis Nexus**: The Securosis Nexus is an online environment to help you get your job done better and faster. It provides pragmatic research on security topics that tells you exactly what you need to know, backed with industry-leading expert advice to answer your questions. The Nexus was designed to be fast and easy to use, and to get you the information you need as quickly as possible. Access it at <https://nexus.securosis.com/>.

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and/or speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <https://securosis.com/>.