The 2014 Endpoint Security Buyer's Guide

Version 2.5
Released: August 16, 2013

Securosis, L.L.C. 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.

Licensed by 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 Virginia, Texas, Utah, Florida, Ireland, Luxembourg, the United Kingdom, Australia and Singapore. Lumension: IT Secured. Success Optimized.™ More information can be found at lumension.com.

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 8

Endpoint Hygiene: Reducing Attack Surface 12

The Impact of BYOD and Mobility 18

Buying Considerations 22

Summary: 10 Questions 26

About the Analyst 28

About Securosis 29

The Ongoing Challenge of Protecting Endpoints

Last year we offered our thoughts on buying Endpoint Security Management offerings — including patching, configuration, device control, and file integrity monitoring — which are increasingly bundled in suites to simplify management. In this updated and revised 2014 Endpoint Security Buyer's Guide we update our research on the management functions described last year and add coverage of anti-malware, mobility, and BYOD. All very timely and relevant topics. The goal of this guide remains to provide clear buying criteria for those of you looking at these solutions in the near future.

The Ongoing Challenge of Securing Endpoints

We have seen this movie before — in both the online and offline worlds. You have something and someone else wants to steal it. Or maybe your competitors want to beat you in the marketplace using unsavory tactics. Or you have devices that would be useful to a bot network. You are a target, regardless of how large or small your organization is, whether you like it or not. Many companies make the serious mistake of thinking it won't happen to them. With search engines and other automated tools looking for common vulnerabilities *everyone* is a target.

Humans, alas, remain gullible and flawed. Regardless of any training you provide employees, they continue to click stuff, share information, and fall for simple social engineering attacks. So endpoints remain some of the weakest links in your security defenses. Even worse for you, unsophisticated attacks on endpoints remain viable, so adversaries do not need serious security *kung fu* to beat your defenses.

Humans, alas, remain gullible and flawed. Regardless of any training you provide employees continue to click stuff, share information, and fall for simple social engineering attacks. So endpoints remain some of the weakest links in your security defenses.

The industry has responded, but not quickly enough. There is an emerging movement to take endpoints out of play. 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 to address that fact. But technologies remain immature so the problem of securing endpoints isn't going away any time soon.

Emerging Attack Vectors

You cannot pick up a technology trade publication without seeing terms like "Advanced Malware" and "Targeted Attacks." We generally just laugh at all the attacker hyperbole thrown around by the media. You need to know one simple thing: *"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. Attacker capabilities improve much faster than defensive technologies, processes, and personnel.

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's not the only path for attackers. They also target users via sleight-of-hand and social engineering. Employees unknowingly open the doors for attackers — and enable data compromise.

There is no point sugar-coating anything. Attacker capabilities improve much faster than defensive technologies, processes, and personnel. We were recently ruminating in the Securosis chat room that offensive security (attacking things) continues to be far sexier than defense. As long as that's the case defenders will continue to work at a disadvantage.

Device Sprawl

Remember the good old days, when devices consisted of DOS PCs and a few dumb terminals? The attack surface consisted of the floppy drive. Yeah, those days are gone. Now 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, but 'smartphones' are really computers. And don't forget tablet computers — each with as much computing power as a mainframe 20 years ago.

So any set of controls and processes you implement must be consistently enforced across the sprawl of *all* your devices. You need to ensure your malware defenses can support this diversity. Every attack starts with one compromised device. More devices mean more complexity, more attack surface, and a higher likelihood of something going wrong. You need to execute on your endpoint security strategy flawlessly — but you already knew that.

BYOD

As uplifting as dealing with emerging attack vectors and device sprawl is, we are not done complicating things. It is not only endpoints that you need to defend any more. Many organizations support employee-owned devices. Don't forget contractors and other business partners who may have authorized access to your networks and critical data stores, connecting with devices you don't control.

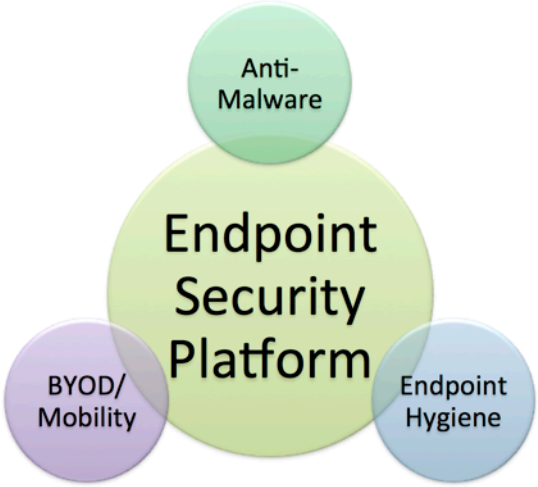
Most folks assume that BYOD (Bring Your Own Device) only applies to those pesky Android phones, iPhones, and iPads. But we know many finance folks are itching to get all those PCs off the corporate books. That means you will eventually need to support any variety of PC or Mac any employee wants to use.

Of course the security controls you put in place need to be consistent, whether your organization or an employee owns a device. The big 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 if you don't own the device, nuking it can be problematic. What about those pictures of Grandma on an employee's device? What about their personal email and address book? Blow those away and the uproar is likely to be much worse than just idling someone for a few hours while they wait to get their work desktop back.

Secure BYOD requires flawless execution, with an additional layer of granularity you haven't had to worry about before. Good times.

Defining Endpoint Security

Before we jump into the specifics, let's consider what we mean by "endpoint security." This simple picture shows how we conceive endpoint security.



- **Anti-Malware:** The ability to detect today's attacks and malware is a topic folks write books about. We won't go deeply into the topic in this paper because we have already produced Evolving Endpoint Malware Detection and Malware Analysis Quant. Here we merely cover the highlights of how anti-malware is packaged and what to look for, and mention some of the advanced detection techniques emerging to stop the relentless tide of malware attacks.

- **Endpoint Hygiene:** As part of an endpoint security strategy you need to pay close attention to the operational aspects of reducing device attack surface. You do that by ensuring you have sufficient capabilities to manage patches and enforce security configuration policies. You also need to lock down device ports (device control). We covered these in granular detail in last year's Endpoint Security Management Buyer's Guide, as well as Implementing and Managing Patch and Configuration Management.

- **BYOD and Mobility:** Finally you need to think about both employee-owned devices and those that don't fit the definition of a traditional 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 report. 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 legitimately maligned, in light of current success rates of malware attacks. In light of this reality, we need some perspective — not only on where anti-malware has been, but 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's ancient history now, but as we reached tens of thousands of new malware samples per day this model broke. Vendors could neither keep pace with the number of files to analyze, nor update their hundreds of millions of deployed AV agents with gigabytes of signatures every couple minutes. So anti-malware vendors started looking at new technologies to address the limitations of the blacklist, including heuristics to identify attack behavior within endpoints and reputation services to identify malicious IP addresses and malware characteristics.

But the technology is still inherently reactive. Anti-malware vendors cannot protect against any attack until they see and analyze it — either a specific file, or 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 around distributing billions of file hashes to each AV agent. If an agent sees a file it doesn't recognize it asks the cloud 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.

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 anti-malware offerings have increasingly used in recent years. The issue with early heuristics was having enough context to know whether an executable was taking a legitimate action. Malicious actions were defined generically for a 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: a lose/lose scenario.

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

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). These applications have been profiled to identify authorized behavior, and anything unauthorized is blocked. Right, 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, a significant chunk of attack surface can be eliminated. To use a simple example, there really aren't any good reasons for a keylogger to capture keystrokes while filling out a form on a banking website. And it is decidedly fishy to take a screen grab of a form with PII on it. These activities would have been missed previously — both screen grabs and reading keyboard input are legitimate functions in specific scenarios — but context enables us to recognize and stop them.

That doesn't mean attackers won't continue targeting operating system vulnerabilities, applications (including the big 7), or employees with social engineering. But this approach has made a big difference in the efficacy of anti-malware technology.

Better Isolation

The next area of innovation on endpoints is the sandbox. We have talked about sandboxing malware within a Network-based Malware Detection Device, which also enables you to focus on what the file does before it is executed 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 for a limited set of applications (the big 7, for example) to shield the rest of the device from those applications.

Many security-aware individuals have been using virtual machines on our 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 find 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. It is definitely something to keep an eye on.

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.

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 running in an isolated environment. Isolation technology doesn't mean you don't need to manage device hygiene (patching and configuration), so we will discuss the details later in this paper.

Total Lockdown

Finally there is the total lockdown option: defining an authorized set of applications/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 has never became mainstream because it impacts the end-user experience. If an application an employee wants to run isn't authorized, they are out of business — unless either IT manages a very 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. Obviously the grace period opens a hole in the security model, but some organizations are willing to make this compromise in order to protect against unauthorized (and undesired) executables running on the device.

This user impact has made this technology much more common on servers. Fortunately servers infrequently call the help desk to ask why they cannot install iTunes, so AWL can very effectively protect fixed-function devices (including kiosks) from malware. Users also tend to accept AWL on very high-value endpoints which obviously 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, and might be detected as malicious tomorrow with new information. Given the endless supply of 0-day attacks and the level of variation in attack kits, you need to be prepared for the inevitability that you will miss something. Then you will need to respond as quickly as possible, and it will be helpful to know which devices the bad file was downloaded to, 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, to identify all devices impacted by a specific attack and then remediate in one fell swoop.

So keep track of what's happening on each endpoint 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 all those 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 — all with fine granularity. So 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 infection — regardless of when they were infected.

Success in protecting endpoints still depends more 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, to 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 mentioned earlier, anti-malware tends to be the anchor in endpoint security control suites. Given today's typical attacks that is justified. But too many organizations forget the importance of keeping devices up-to-date and configured securely. Even "advanced attackers" don't like to 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 them to own your devices. The progression in almost every attack — regardless of the attacker's sophistication — is to 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 say 'hygiene', we are referring to three main functions: patch management, configuration management, and device control.

> When we say 'hygiene' we are referring to three main functions: patch management, configuration management, and device control.

Patch Management

Patch managers install fixes from software vendors to address vulnerabilities. The best known patching process is Microsoft's monthly Patch Tuesday, when they issue a variety of software fixes to address defects — 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 'important' issues.

Once a patch is issued your organization needs to assess it, figure out which devices need to be patched, and install it 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 very detailed view of the patching process, so check it out 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. We talk about the big 7 vulnerable applications (browsers, Java, Adobe Reader, Word, Excel, PowerPoint, and Outlook) — ensure those targeted applications are well covered. Keep in mind that the word 'supported' on a vendor's data sheet doesn't mean they support whatever it is *well*. Be sure to test their patch library and the timeliness of their updates. How long do they take to repackage and deploy patches to customers?

- **Discovery:** 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.

- **Reliable deployment of patches:** If patches don't install consistently — including updating, adding, and/or removing software — that means more work for you. This can easily make a tool more trouble than it's worth. Do they get it right the first time?

- **Agent vs. agentless:** Does the patch vendor assess devices with an agent, or do they perform 'agentless' scanning (typically using a non-persistent or 'dissolvable' agent). If so how do they deploy patches? This is almost a religious dispute but fortunately both models 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 includes field employees' laptops as well as devices in remote locations with limited bandwidth. What features are built in to ensure the right patches are deployed regardless of location? Can you be alerted when a device hasn't updated within a configurable window — perhaps because it hasn't connected?

- **Deployment architecture:** Some patches are gigabytes in size, so flexibility in distribution 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 (possibly 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 operating systems. Enough said.

- **Discovery:** 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 better your chance of finding 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 be sure scanning frequency is flexible.

- **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 hasn't updated within a configurable window — perhaps because it hasn't connected?

- **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. This may be managed within the endpoint security platform, but integration 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 just love the flexibility USB ports provide for 'productivity'. You know… the ability to share music with buddies and 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 really has facilitated employee collaboration, but it 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 also to capture what is copied to and from USB devices. As an active control, monitoring and control over device usage addresses a major risk on endpoints.

Device Control Technology Considerations

- **Device support:** The first order of business is to confirm 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 your product can support different policies per device. This enables 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 also 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 isn't exhaustive, but make sure your product supports the policies you need.

- **Encryption algorithm support:** If you will 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 isn't a pig, stealing massive amounts of compute power from each device, also ensure some kind of tamper resistance to protect the agents. It would be bad if an attacker disabled or subverted the agents.

- **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 anti-malware, patching, configuration management, and device control should be handled by a common agent.

- **Offline support:** Devices aren't always connected to the network, so make sure policies are still enforced even when disconnected. Also ensure you can configure policy violation alerts when devices reconnect.

- **Forensics:** In the event of data loss you will want forensics, so logging all user activity can be quite helpful. Some offerings also copy any files copied to protected device ports as 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 below, but your choice depends on which group is responsible for these functions. If it is 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 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 with mature technologies, 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.

The Impact of BYOD and Mobility

When thinking about endpoint security it is important to decide what you consider an endpoint. We define an endpoint as any computing device that can access corporate data. This deliberately broad definition includes not just PCs but also mobile devices: smartphones and tablets. We don't consider that too broad — employees today expect to access the data they need, on the device they are using, wherever they are, at any time. And regardless of the details, the data needs to be protected.

Today's buzzword is Bring Your Own Device (BYOD), which means you need to support employee-owned devices just like you support corporate-owned devices today. These folks go to the local big box retailer and come home with the shiny new iDevice or Android thingy, then show up the next working day expecting their email and access to the systems they need to do their jobs on the shiny new device. For a while you said no because you couldn't enforce policies on those devices, nor could you assure the employee's children or friends wouldn't get into email and check out the draft quarterly financials.

> Fortunately you probably have many of these policies in place already, so it is time to go back and revisit them to ensure they reflect both the differences in supporting mobile devices, and the fact that you may not own the devices.

Then you were summoned to the CIO's office and told about the new BYOD policy put in place by the CFO to move some of those expensive devices off the corporate balance sheet. At that point 'no' was no longer an option, so welcome to the club of everyone who has to support BYOD — *without* putting corporate data at risk. The first step is to define the rules of engagement — which means *policies*.

Fortunately you probably have many of these policies in place already, so it is time to go back and revisit them to ensure they reflect both the differences in supporting mobile devices, and the fact that you may not own the devices. This is a Buyer's Guide rather than a policy guide, so we won't focus on specific policies, but we need to point out that without an updated set of policies to determine what employees can and cannot do — covering both mobile devices and BYOD — you have no shot at controlling *anything*.

BYOD

First let's blow up the misconception that BYOD simply means mobile devices. Restricting BYOD to a mobile context is overly limiting. Employees may decide they want to run their office applications in a virtual window on their new Mac, not the 4-year-old Windows XP laptop they were assigned. Which means you need to support them even though you don't own the devices. This changes how you provision and protect devices, particularly in terms of enforcement granularity.

> Actually, if your policy says so, you probably can legally control and wipe the device. But it would make you very unpopular if you blew away a device, deleting a bunch of personal pictures and videos in the process.

For devices you don't own, you need the ability to selectively enforce policies. You cannot dictate what applications employees run on their own machines. You cannot whitelist all the websites they visit. You cannot arbitrarily nuke a device from orbit if it shows indicators of possible malware. Actually, if your policy says so, you probably *can* legally control and wipe the device. But it would make you very unpopular if you blew away a device, deleting a bunch of personal pictures and videos in the process.

The key is granularity. It is reasonable to perform periodic vulnerability scans on each device to ensure it's patched effectively. It is also reasonable to require devices to be encrypted so the corporate data on them 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 BYOD in terms of aspects we have discussed already:

- **Anti-malware:** If you require anti-malware on corporate-owned computers, you probably want to require it on employee-owned machines as well. Anti-malware may also 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 your 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. You also need to decide whether you will mandate anti-malware protection for mobile devices, given the lack of malware attacks on most mobile platforms.

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

Dealing with BYOD comes down to adding another dimension to policy enforcement. You need to review each policy to figure out whether it needs an update for employee-owned devices. It is also a good idea to make sure you can both visualize and report on employee-owned devices, because there will be sensitivity around ensuring they comply with BYOD policies.

Mobility

We just explained why mobile devices are endpoints which need attention like PCs, so we need to provide guidance on protecting them. As with most newish technology, management presents a bigger initial problem than security. The good news is that mobile devices are inherently better protected from attack, due to modern operating system architectures. That makes hygiene — including patching, configuration, and determining which applications can and should run on the devices — the key security requirement for mobility.

Of course that doesn't mean there is no mobile malware threat. Rooting devices, having employees jailbreak their devices, dealing with new technologies which extend the attack surface such as NFC (Near Field Communications), and attackers exploiting advanced device capabilities are all real issues. But none of these are currently the most pressing issue. That can and probably will change, as attackers get better and management issues are addressed. But for now we will focus on management.

The technologies that enable us to manage mobile devices fall into a handful of categories. Of course there is overlap, and all these capabilities are increasingly bundled into packages, but let's start with the categories.

- **MDM (Mobile Device Management):** This is very popular technology now, providing a mechanism for defining policies for different categories of users and enforcing device configurations. You also can ensure timely mobile operating system updates and remotely wipe lost devices. There are hundreds of separate features in a typical MDM product, but for endpoint security you should focus on defining profiles and determining what employees can do with devices.

- **MAM (Mobile Application Management):** Should a user be able to use the Salesforce.com app on their mobile device to get your data? That is a microcosm of the issue MAM addresses for organizations. There are tons of corporate 'apps' which employees should be using, and MAM provides a corporate app store to authorize which apps they can use. You can also use this capability to stop employees from accessing unauthorized apps and manage or protect specific applications — including mobile browsers and email clients.

- **Containers:** Another key aspect of security for mobile devices is data protection. Containers keep corporate data within a "walled garden" on mobile devices. This provides better granularity and selective wipe capability for only corporate data, which is particularly helpful in BYOD environments.

Regardless of which capabilities you need, there are a couple key buying criteria for mobile security offerings. The first is platform support. Obviously you need to protect the devices your employees use. All of them, even those old BlackBerries. Another key consideration is enterprise integration — whether you can leverage your existing identify stores, security operations center (SIEM), and reporting infrastructure. Depending on the organizational boundaries of whichever team is responsible for managing mobile devices, integration with existing endpoint security offerings may also be important.

Do BYOD and Mobile Stand Alone?

We increasingly expect mobile security capabilities to be bundled with broader endpoint security and management offerings. That isn't brain surgery — simply a realization that every emerging market starts as standalone technology, which ultimately gets wrapped into broader management offerings. We have already seen tremendous consolidation of MDM players, and we expect more. Given the critical management needs, we expect these capabilities to be built into and managed from endpoint management platforms. That doesn't mean all the independent mobile management/security companies will go away, but we expect a handful to stay independent while the rest are integrated into offerings from larger IT management vendors. We have all seen this movie before.

> We increasingly expect mobile security capabilities to be bundled with broader endpoint security and management offerings.

This 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 may want to look at a bundled offering from the beginning because many endpoint security and management vendors already provide some mobile security/management capabilities. If you need more advanced capabilities be sure to look for the key integration points you need for mobile security functions to work with your other enterprise systems — specifically identity (to define entitlements and access rights) and network security (to restrict certain devices to specific network segments). Then revisit the bundling question as the technology matures.

Buying Considerations

We will wrap up this paper with a discussion of the buying considerations. These buying considerations drive you toward one solution or another, and develop a procurement process that can work for your organization.

Platform Features

As in most technology categories (at least in security), the management console (or 'platform', as we like to call it) 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 only show certain elements, policies, and alerts to different authorized users or groups, with entitlements typically 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 as quickly as possible — including mobile devices.

- **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 what's out there in a timely fashion.

- **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, so alert management is key. It enables administrators to monitor potential malware attacks and policy violations, which might represent attacks. Time is of the essence during any response. Thus it is critical to provide deeper detail via drill-down and 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:** You can expect the standard system status and administration capabilities within the platform, including user and group administration. For larger 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.

- **Reporting:** As we mentioned under specific controls, compliance tends to fund and drive these investments, so substantiating 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

The advent of cloud-based offerings for endpoint security has 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 their 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.

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

You also want a feel for service levels, downtime, and support for the cloud offering. It's great to not have another server on your premise, but if the service goes down and your endpoints are either bricked or unprotected, that on-premise server will look pretty good.

Buying Considerations

After doing your research to figure out which platforms can meet your requirements, you need to define a short list and 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.

Working with a larger vendor is all about leverage. One type is pricing leverage, achieved 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. Another type is platform leverage from using multiple products managed via a single console. The larger endpoint security vendors offer comprehensive product lines with a bunch of products you might need, and an integrated console can make life easier.

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 a serious analysis capability to figure out what needs to be done. You will probably hear a lot about big data, the buzzword *du jour*. More relevant is the vendor's level of investment in keeping their platform current.

You will want to ensure the vendor has the ability to support your environment, wherever it is geographically. Local support is best for dealing with endpoints, because you may not have capable staff on-site to troubleshoot issues. 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

There is no need to reinvent the wheel. Some organizations are formal and issue RFI/RFP (Requests For Information and 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 minimize 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. For example 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 you will know what you need an endpoint security platform to do.

2. **Establish 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 testbed 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 will 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. Both during 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 their 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: 10 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 the 10 key questions we would ask 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?
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 by your 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 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)?
8. Where does your management console run? Do we need a dedicated appliance? What kind of hierarchical management do you environment support? How customizable is the management interface?
9. What kind of reports are available out of the box? What is involved in 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?

Of course we could write another 10 questions. But these hit the highlights of dealing with today's malware attacks, device & application coverage, research & intelligence, mobility & BYOD, 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 5 (agents) and question 10 – the security of the management capability 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 obviate 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.

So your buying approach needs to balance innovation against maturity. Given this backdrop and the criticality of blocking malware, ensure that you are comfortable with your endpoint security vendor's ability to block attacks, and that their management capabilities will reduce you 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 elQnetworks 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/>.