Interested in learning more
about cyber security training?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Understanding the (True) Cost of Endpoint Management

In this paper, we review the challenges in dealing with complex, ever-changing environments and offer suggestions and recommendations in effective endpoint management. Additionally, we discuss enterprise security as it relates to endpoint management and examine the benefits of integrating endpoint management into your security posture.

Copyright SANS Institute
Author Retains Full Rights

SANS

A SANS Survey

Understanding the (True) Cost of Endpoint Management

Written by **Matt Bromiley**

July 2018

Sponsored by:

IBM

SANS Analyst Program

©2018 SANS™ Institute

Executive Summary

IT endpoint management used to be an easier game: Managers deployed user systems with custom images when employees were hired, and employees returned them on their last day at work. Even during deployment, users had minimal abilities to impact systems and devices that were centrally managed. Servers resided in physical data centers where they could be identified and accessed. Those were the days!

Today, endpoint management is anything but predictable and harmonious. Users can bring their own devices into their enterprises and run their own applications. Organizations outsource operations to browser-based third parties, and users often have full administrative privileges over their systems. Servers have also changed drastically, no longer likely to be physical entities located in a data center to which IT administrators have access.

In this survey, we sought to capture the essence of what it takes to manage modern, multiplatform, complex enterprises. IT and security teams have to enable functionality and implement systems that were once considered futuristic dreams—and to do so across multiple countries simultaneously, among a plethora of ever-changing compliance standards. We also wanted to explore the differences between up-front and hidden costs associated with endpoint management. Lastly, we wanted to understand what security risks enterprises are exposing themselves to today. Endpoint management plays an extremely critical role in efficient operations and enterprise security, and a gap in one could result in an exposed vulnerability.

To find the true cost of endpoint management, we had to ask some tough questions. Specifically, we wanted answers to the following:

- How complex are IT organizations these days, and what does it take to manage and secure endpoints within these environments?
- Are the costs of modern endpoint management face-value, or are there hidden variables that must be considered, giving us the "true" cost of endpoint management? If so, what are these hidden variables and/or considerations?
- Does the lack of efficient endpoint management within an organization create and/or prolong security risks?

Our respondents, who provided insight from a variety of industries, such as finance, government and telecom, shared the following:

- Organizational size is an extremely important variable, with 61% of our respondents having more than 1,000 user endpoints; 5% of that group has more than 100,000 user endpoints. **Larger environments will naturally include larger obstacles.**
- Complexity is significant, with 12% of our respondents having *at least* 11 operating systems within their environment. **Operating system complexity is a huge consideration because enterprises must find compatible management tools.**

For our survey, we define key terms in the following way:

- **Endpoints—**Computing devices, including user systems, servers and other business systems such as point-of-sale (POS) devices
- **Networks—**Groups of endpoints, typically with a common association; networks may be as granular as a department or as high-level as the organization itself
- **Endpoint management—**The operations required to manage the endpoints within an organization, including activities such as system configuration, patching, endpoint inventory and compliance

- Enterprise visibility is lacking, with some respondents indicating they do not have insight into the number of endpoints within their environment. Additionally, we found that 33% of our respondents need at least two days to detect security incidents, and 22% don't know whether their endpoint systems had fallen into a noncompliant state. **Visibility into endpoints and security risks is key to understanding your enterprise's current security posture and ensuring you are remaining compliant.**
- Patching remains a critical concern; 25% of our respondents need *at least one month* to patch servers in their environment. **This is one of the largest security risks for many organizations, and patching speeds need to improve.**

We will cover these findings and more in the sections to come. In this paper, we review the challenges in dealing with complex, ever-changing environments and offer suggestions and recommendations in effective endpoint management. Additionally, we discuss enterprise security as it relates to endpoint management and examine the benefits of integrating endpoint management into your security posture.

Organizational Complexities

When we began our quest of understanding the true cost of endpoint management, we wanted to ensure we understood the complexities that modern organizations face. For example, very few organizations support only one operating system or even one version of an operating system. An enterprise may consider itself a "Windows shop" (meaning it supports only Microsoft Windows), but Windows has multiple versions, each with its own nuances.

Furthermore, in our experience, even enterprises that officially support only one type of operating system usually have to deal with others, given that server functionalities are often achieved by *nix-based operating systems. And executives' preferences for a particular type of operating system or device can be exceptions to the norm, but IT and security are still responsible. We'll cover those responsibilities later in the paper.

Our respondents helped highlight this point, with 48% indicating that they have at least six operating systems in their environment, and 12% reporting they have at least 11. Figure 1 illustrates the varied types of OSes in use.

An additional area of complexity for effective endpoint management is the number of locations (e.g., data centers, offices or stores that have servers, workstations, laptops or point-of-sale machines) and employees the IT team must serve. Additional locations add an obvious increase in system complexity: more systems to manage and thus more opportunities for gaps in coverage. Our survey indicated that

Survey Respondents

Largest Industry Representation

17% finance

16% telecom

12% government

Size of Workforce

18% have more than 10,000 workers

43% have 1,000 workers or fewer

A Worldwide Response

A large majority (**71%**) have operations in the United States

Large percentages of respondents have operations in Europe (**35%**) and Asia (**25%**)

What operating systems do you use in your endpoint ecosystem? *Check all that apply.*

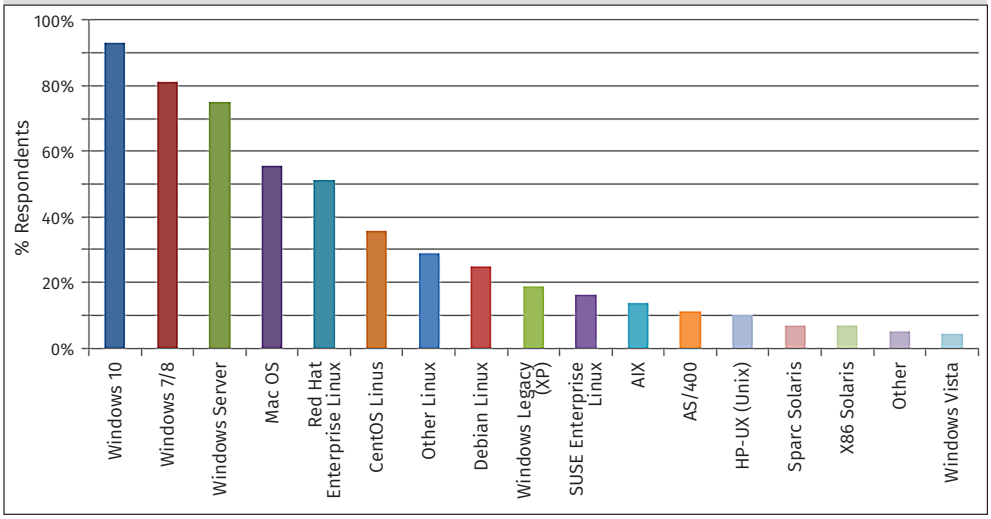

Figure 1. Operating Systems in Use in the Endpoint Ecosystem

24% of our respondents have more than 100 physical locations to protect. As depicted in Figure 2, where we examine the number of employees by physical location, many respondents must manage environments of significant size. We also found, in most of our survey results, that larger enterprises typically present additional complexities, which we will discuss in subsequent sections.

In summary, it is obvious that the days of simplistic system design are long gone. Environments are often quite large, and the numbers of endpoints under management these days can be staggering. Endpoint management requires careful planning and implementation to secure multiple OSes in multiple locations. However, one difficulty that plagued administrators of networks past has been largely overcome with today's networks: bandwidth.

Whereas endpoints in the past were beset by questionable, slow or throttled bandwidth speed, our survey respondents indicated bandwidth has improved significantly. Approximately 63% said at least a majority of their physical locations have high-bandwidth connections. Only 13% indicated that 10% or less were served by high-bandwidth connections. Figure 3 depicts our results for high-speed connectivity, which can be crucial in effective endpoint management.

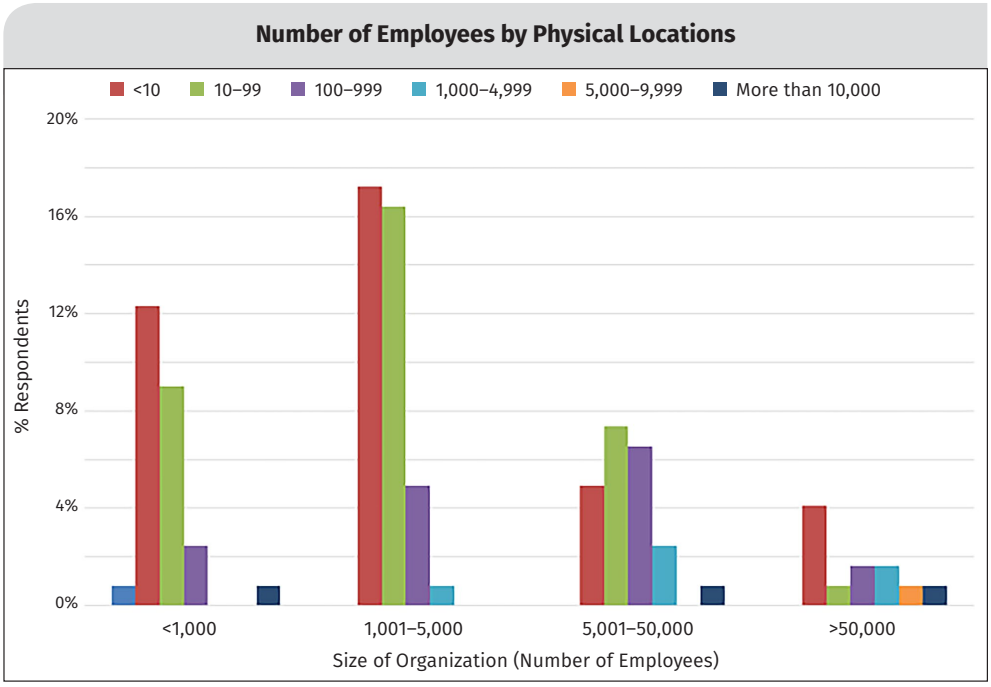

Figure 2. More Locations Often Mean Increased Complexity

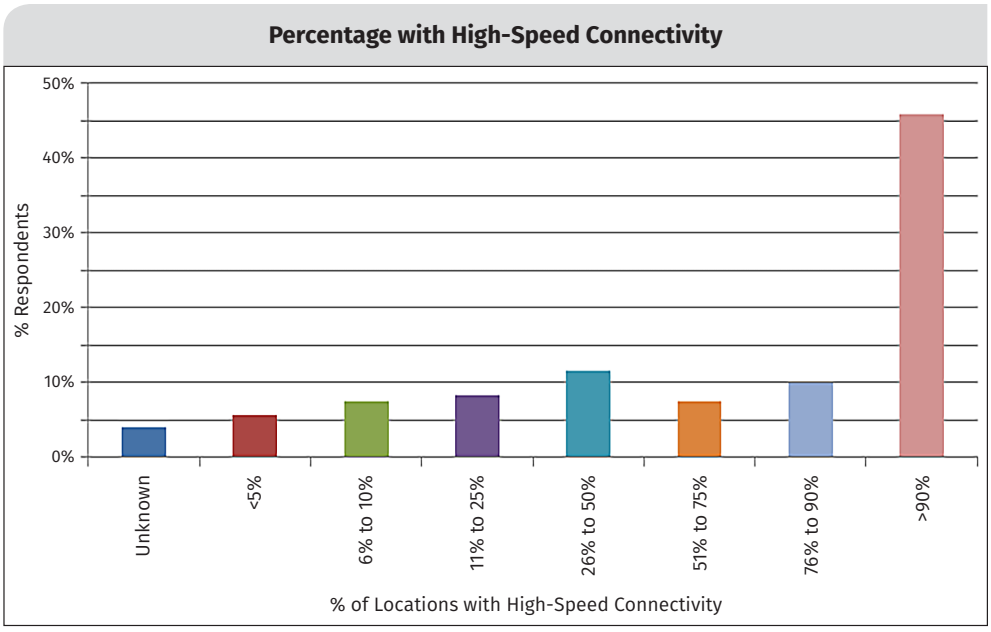

Figure 3. High-Speed Connectivity of Respondents

The Cost of Infrastructure Support

In previous sections, we looked at organization size, number of locations, bandwidth, geographic reach and number of operating systems supported—all of which contribute to complexity of management and impact the true cost of endpoint management. Those attributes, while critical in understanding *why* it takes what it takes to manage endpoints, do not speak to the underlying costs.

In this section, we set out to understand the infrastructure that organizations are currently using for endpoint management. As we examine each high-level topic, we're going to focus on three types of "costs" that we want you, our reader, to consider when assessing your own organization. Those costs are:

- **Money.** Perhaps the simplest form of cost is actual dollars that an organization must spend to achieve a state or level of effectiveness. These include initial costs, implementation costs and maintenance costs.
- **Resources.** While resource costs are ultimately represented in terms of dollars, we instead focus on actual humans that must be in place.
- **Speed.** How quickly organizations can deal with endpoint issues such as patching, responding to alerts and remediating vulnerabilities is the third cost. This cost can be reduced with integration and/or automation of endpoint management tools. While sometimes underestimated, speed can be the most important cost, because it's the one that can also affect your ability to respond to incidents.

Where applicable, throughout this section we identify the various categories of costs associated with each data point our survey uncovered. We encourage you to utilize these subsequent sections as guidance to evaluate your current or future implementations of endpoint management solutions.

When evaluating your current or future endpoint management solutions, be sure to analyze *all* the costs your organization encounters, not just the dollar amount on the invoice. Be aware that there are costs for both initial implementation and ongoing operation.

Managing the Complexity

Previously, we outlined various complexities that organizations face today. One approach that responding organizations use for wide-scale endpoint management is to have a number of servers dedicated solely to endpoint management that are distributed throughout the enterprise. *Note that this does not include endpoint agents or sensors.*

The number of servers used will of course be highly influenced by the size of the enterprise. Still, one result from the survey was very revealing: Approximately 10% of respondents have zero insight into the number of management servers they are using. Such a lack of enterprise visibility is an unfortunate trend we saw throughout our survey analysis. We'll address this throughout various sections, but let's call it out now: Lack of visibility into your environment is a serious concern that should be at the top of the "Fix Now" list. Your organization may find itself noncompliant with respect to the types of data you house or, even worse, breached without knowing it.

Approximately 29% of our respondents indicated needing only one or two servers for endpoint management. At the other end of the scale, 13% of respondents require more than 10 servers, likely indicative of sizable environments, as shown in Figure 4.

We then dug deeper to understand not only how many servers respondents have, but how many tools they use for endpoint administration and/or discovery. See Figure 5.

Approximately 83% of our respondents reported needing between one and nine tools to accomplish this task on user workstations, and 82% claimed the same needs for servers. However, 7% said they are currently using at least 10, and sometimes *more than 20*, tools to manage user workstations, with 8% reporting the same result for servers. That is a significant number of tools for administrators to deal with, and industry experience shows that large tool counts can cause slowdowns within the endpoint management process. As analysts and administrators have to sift through more data and dashboards, the ability to effectively manage endpoints becomes more complex, is subject to inaccuracies, and thus is susceptible to response delays and other inefficiencies. This potentially increases both resource and speed costs.

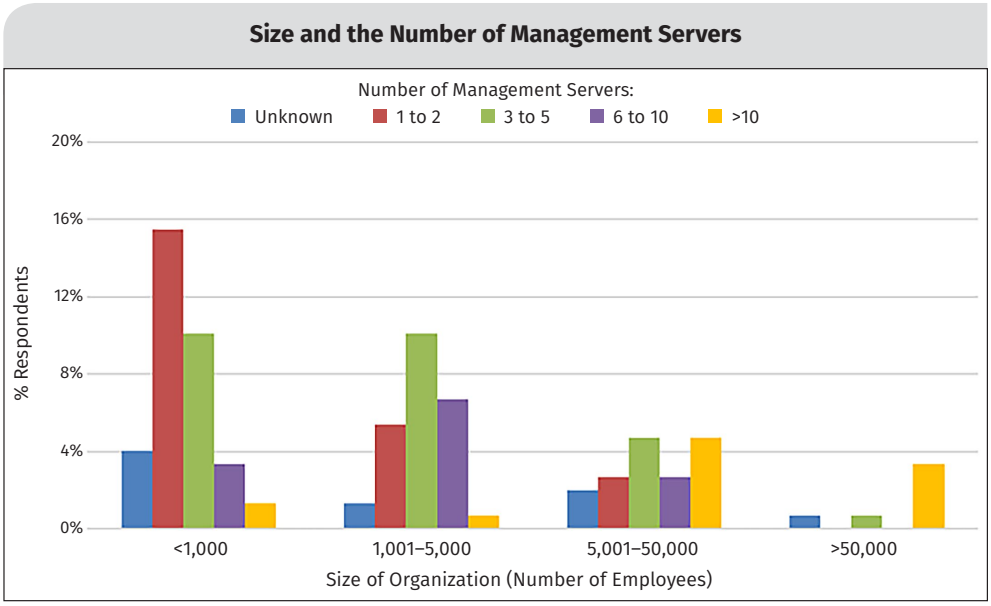

Figure 4. Multiple Servers Used for Endpoint Management, Likely Related to Size

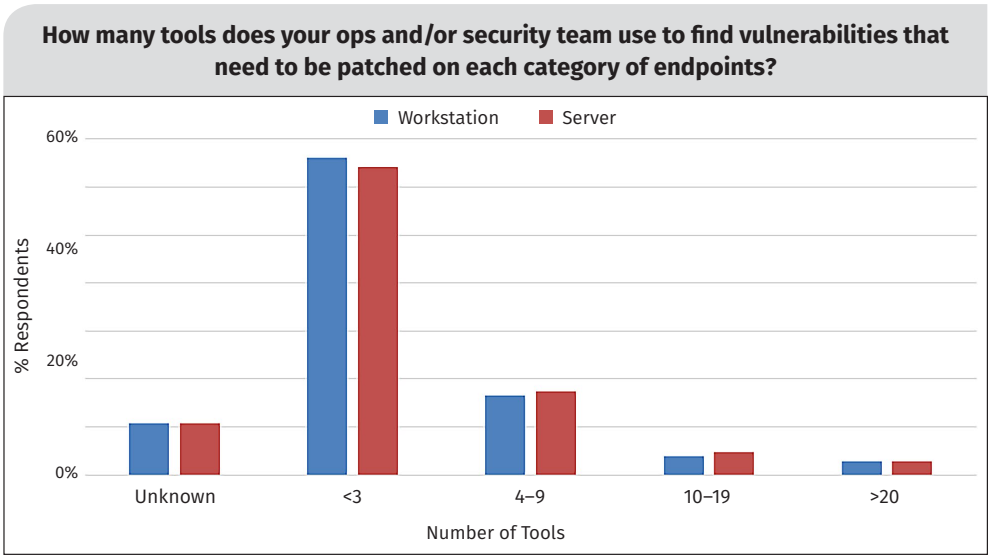

Figure 5. Endpoint Management Tools in Use on Workstations and Servers

Actions for Managing the Complexity

Concerns

- Most respondents' organizations were able to identify how many tools are required to achieve endpoint management. However, approximately 10% do not know how many servers they used, and 11% don't know how many tools were required.
- It is *critical* to have insight into endpoints within your organization. Getting this insight should be a priority, if not the leading priority. After all, you can't protect what you don't know you have.

Costs

- **Money.** Establishing and maintaining multiple servers armed with multiple tools requires significant financial outlay to acquire the necessary hardware and software.
- **Resources.** The more complex the environment, the greater the resource requirements. Servers require administrators. Tools need someone to run them effectively and keep them updated (we'll look at this in the next section).
- **Speed.** With the number of tools we're seeing organizations use, there is potentially a considerable impact on speed to respond to alerts or identify an endpoint if automation and integration (discussed later) are not in use.

Recommendations

- Focus on limiting the number of tools that your teams must use for endpoint management, even if this means upgrading to a more holistic toolset.
- Different operating systems may require different toolsets. Research whether there is an existing toolkit or subsystem that you can use that, with a quick upgrade or enhanced features, may be compatible with multiple platforms.

The Right Team for the Job

Given the varying number of management servers that our organizations are using to manage their enterprises, our next step was to examine the teams behind the magic. Specifically, we sought to identify the division of endpoint management responsibilities between IT and security teams. After all, not all respondents have specific staff assigned to patching and endpoint inventory, configuration, and control. Some teams have to shoulder all these responsibilities.

Based on our results, responsibilities are unevenly divided between IT and security, with IT clearly handling more endpoint management roles. To illustrate just how large that divide is, 96% of respondents said endpoint patching is an IT operations responsibility, whereas 63% indicated that security was involved. When it comes to patching, we think security teams should be more involved, because they have the ability to assess just how critical a patch may be. We'll cover the importance of timely patch management in a later section.

Furthermore, a large majority of responding organizations have teams of just one to five members to monitor endpoint vulnerabilities and prioritize patching across all endpoints (70%) and to manage software deployment and patching across all endpoints and operating systems (78%). Figure 6 provides details on IT operations team size and their various responsibilities.

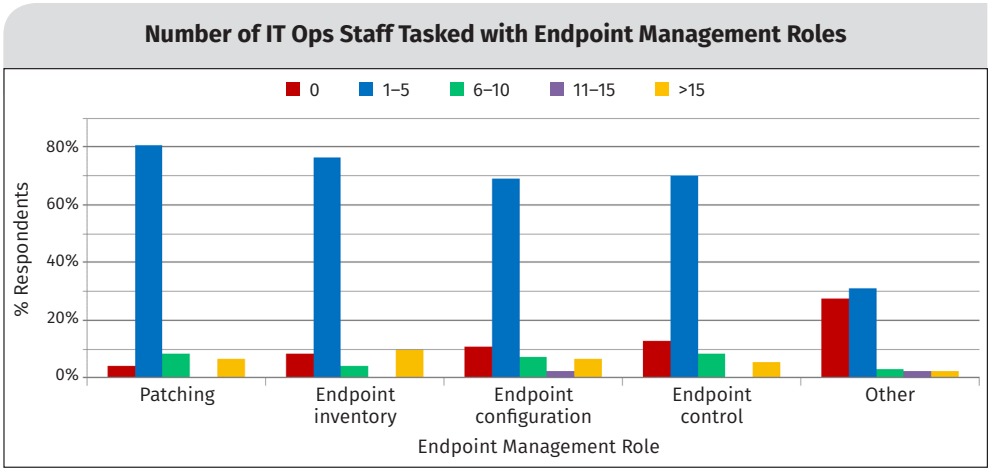

Figure 6. Number of IT Ops Staff Tasked with Endpoint Management Roles[1]

While IT operations certainly had the most endpoint management roles, we did have some organizations indicate that their security teams also shared some of the responsibilities. As expected, the numbers are lower, with the most common team size, at an average of 41%, being between one and five people. While the results were not dismal, we'd like to see security play a larger role in all endpoint management activities.

Figure 7 provides insight into the size of security operations teams and their various responsibilities.

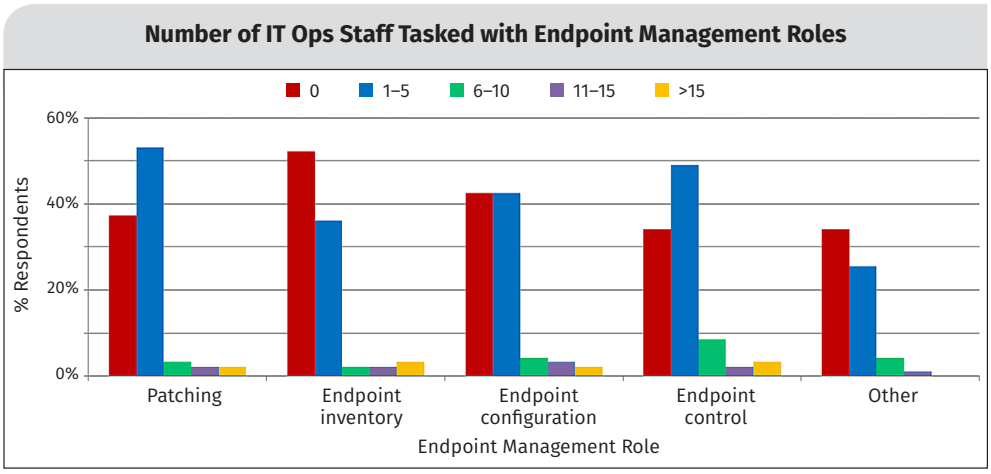

Figure 7. Number of Security Ops Staff Tasked with Endpoint Management Roles[2]

[1] We've summed up the various endpoint roles. Actual jobs are likely much more granular.

[2] We've summed up the various endpoint roles. Actual jobs are likely much more granular.

Actions for Assessing the Right Team for the Job

Concerns

- Security teams do not play as large a role as we'd like to see in patching and endpoint control. It's not that IT operations is doing a bad job, but security can bring critical insight to endpoint management.
- From both IT and security perspectives, the most common team size charged with endpoint management is between one and five people. With the right tools, this team size may be adequate, but it seems likely that some teams are overloaded.

Costs

- **Money and resources.** Building IT and security operations teams clearly involves money; more experienced and/or larger teams mean more outlay in compensation. However, correct resource allocation, tooling (more on this later) and diversity can keep costs within budget and still provide value to the organization.
- **Resources.** Hiring analysts of varying levels of experience can help build a diversified, functional team. Our experience is that having too many senior staffers or having too few experienced leaders can result in inefficient operations. We recommend a blend of both experienced and inexperienced, allowing the team to grow organically and train within.
- **Speed.** Having the right number of people and associated skillsets means your IT and security operations teams can work together and quickly respond to incidents. However, too few or too many analysts can result in response delays. Patching, for example, should typically be deployed as rapidly as possible to defend against attacker weaponization.

Recommendations

- If your environment is experiencing multiple security incidents, determine how much support security is providing to endpoint management, specifically patching and control.
- Clearly define the expectations of the IT and security operations teams with regard to endpoint management and ensure that they are in communication. Establish lines of communication if they are not already in place, and look for ways to integrate tools and processes.

Does the Tool Make the Difference?

One particular area of concern when it comes to endpoint management is the use of free and open source versus commercial software. To be clear: We are not advocating one over the other. Each type of software has its pros and cons. Open source tools, for example, may have fewer startup costs but may end up requiring significant resources in the long run. Commercial tools will cost more initially but traditionally come with support teams to assist in implementation and troubleshooting.

SANS' experience suggests that some organizations implement open source and/or commercial software simply to say that *something* is there, without ever assessing whether the *right* something is there. For example, an organization might decide it needs to purchase a tool for compliance reasons, even though it doesn't know what the device is or why it needs it. And organizations often look at the initial price tag of a tool and assume that represents the eventual complete cost. But costs can grow quickly, given that ongoing maintenance and upgrades are likely to be needed.

Although 11% of respondents were unable to provide the number of tools their organization uses to find vulnerabilities on workstations, 66% reported using three or fewer tools, with 17% said they use between four and nine tools. The numbers are similar with respect to servers.

Our survey results on open source management tools were very interesting with regard to the number of tools and vendors being utilized. Lack of visibility is demonstrated again in that 43% of respondents don't know how many open source tools they are using.

Approximately 57% of respondents said that they use one or more open source or freeware tools within their environment for endpoint management, with just 11% indicating that they don't use open source or freeware tools. Nearly half (46%) of

those using such tools noted they were provided by one to five vendors. The number of tools utilized by our respondents varied, with 14% of respondents saying they use at least four tools, as illustrated in Figure 8.

When compared to the previous statistic of endpoint management tools in use, this gives us some indication that most organizations (57%) are utilizing some sort of open source or freeware within their endpoint management arsenal.

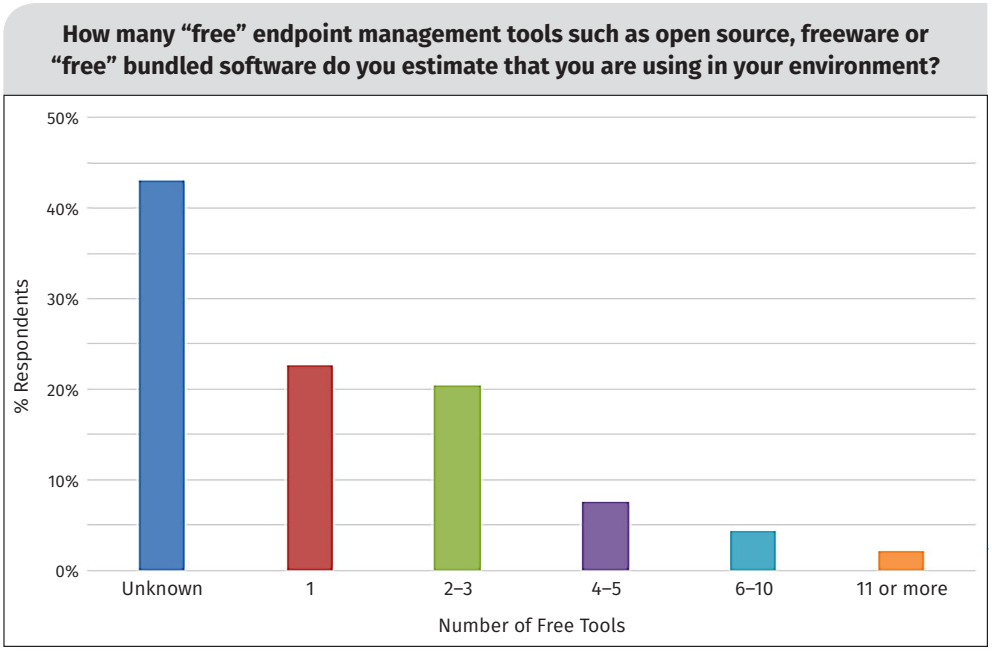

Figure 8. Number of Open Source or Freeware Tools Used for Endpoint Management

Actions for Assessing Endpoint Management Tools

Concerns

- A large portion of our survey respondents had no insight into the number of open source/freeware tools (43%) within their environment or the number of vendors that supply them with such tools (45%). This highlights a common recurring theme in our survey results that we will continue to state: Enterprises *must* work toward *endpoint visibility*—knowing what and when endpoints are on your network, and what those endpoints are running.
- Tools of all kinds make it really easy to "check a box." Open source and freeware tools can be downloaded and somewhat implemented so that an organization can feel as if it has accomplished something. But the true costs of those tools may end up being higher than the costs of commercial tools because organizations need to prop up and maintain the infrastructure necessary to run such open source/freeware tools.
- All tools have price tags; commercial tools provide baseline pricing up front; open source tools require you to discover the costs for yourself as your organization, use of the tool and the tool's requirements grow.

Costs

- **Money.** Commercial tools will have invoice and implementation costs. Open source tools can likely be acquired for free—but they will have implementation costs associated with them.
- **Resources.** Both types of tools will require resources for implementation and ongoing management and support. Note that open source tools may or may not provide adequate support and documentation, potentially requiring significant IT investment.
- **Speed.** Depending on the tool and level of implementation, both open source and commercial tools can lead to speed decreases and inefficiencies. Look ahead to the next section, "Making the Job Faster," for suggestions on combating speed issues.

Recommendations

- Focus on whether endpoint management in your organization is *truly effective* with the tools you have in place. If you are dedicating a significant amount of your budget to a tool that doesn't work, make a change.
- Ask key questions up front. How many endpoints can a single server manage? How many endpoints can a single administrator manage and secure effectively? What are your first-time patching success rates? How long does it take to patch all your systems? How many operating systems (and versions) does your solution support? How many software solutions will it patch? How much patch content does the vendor provide, or do your admins have to create this? How long will this take? How long does it take to query all your endpoints? How accurate is this data? Is it available from a single dashboard? How well does the tool scale?
- Evaluate, evaluate, evaluate! Utilize proof-of-concept periods to allow your IT team to test products in development environments. Don't commit to any tool until you know it's the right one for your organization.

Making the Job Faster

One way to aid in management of large-scale organizations, or even assist smaller organizations with multiple platforms, is to use integrated, automated tools. In the context of endpoint management, "integrated" and "automated" typically refer to systems that are part of a larger IT infrastructure. For example, endpoint telemetry is being collected and analyzed automatically by existing tools, which are alerting to anomalies and areas of concern. In these situations, administrators only have to deal with anomalies, not manually collect data.

Integration and automation don't just make endpoint updates easier; they should also be thought of as a way to help mitigate incoming endpoint threats. More on security later.

We do not believe that environments can ever become 100% automated and integrated. Human beings will always be necessary, because machines sometimes do not understand the nuances of the enterprise. However, automation and integration can be excellent in helping free up analysts and managers to solve the tough problems—letting the machines handle the simple ones. With that in mind, we were pleasantly surprised to see that 48% of respondents to the survey have achieved greater than 50% automation across their endpoint management tools, and 43% have achieved greater than 50% integration of those same tools. See Figure 9.

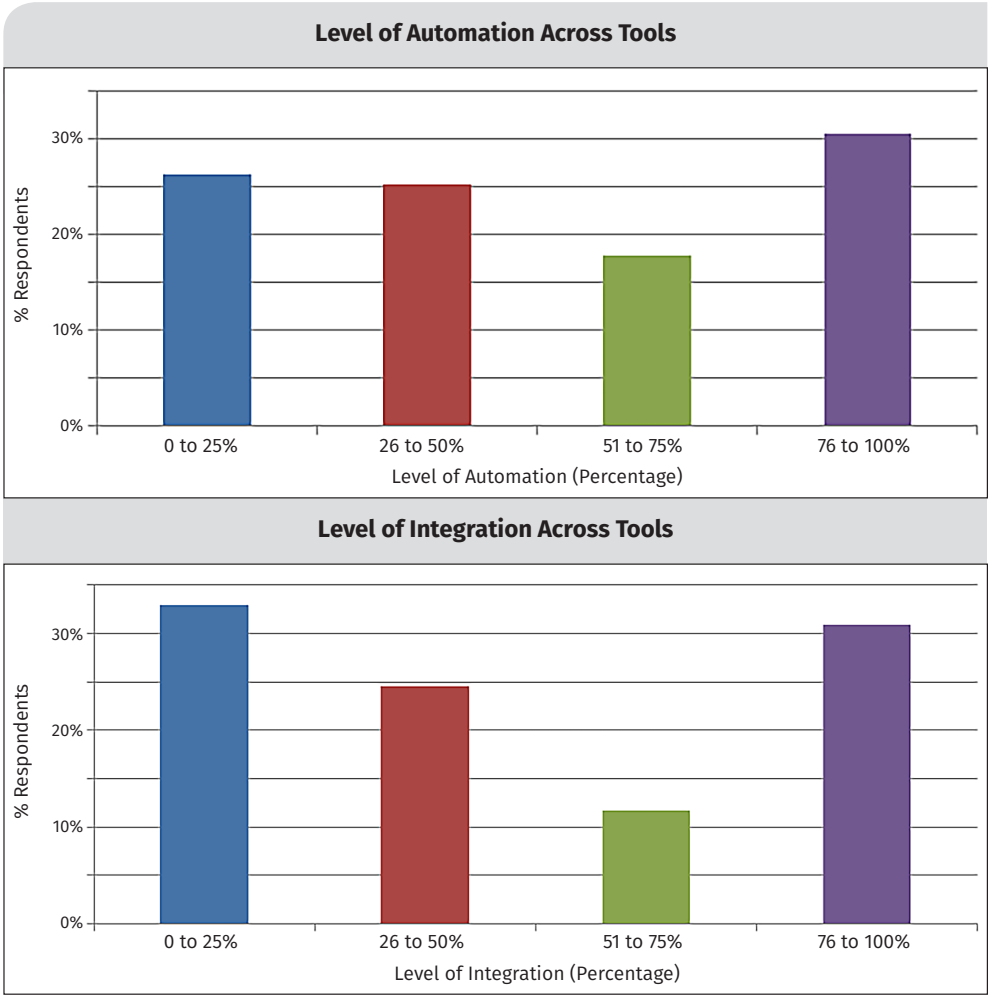

Figure 9. Levels of Automation and Integration of Endpoint Management Tools

Actions for Making the Job Faster

Concerns

- A large number of respondents reported that their organizations' levels of automation/integration are at 50% or greater. While this number may never reach 100%, we'd like to see it climb higher than 50% for all enterprises.

Costs

- **Money.** Automated and integrated systems often require investment to integrate within the environment. Additionally, these tools may require capital outlay.
- **Resources.** Intelligent, automated systems may require specialized training and/or engineers on hand.

Recommendations

- Organizations of all sizes need automation and integration. There is simply too much data to process and too many variables to leave up to manual decision making. Don't shy away from automating part of your environment.
- Focus on the pain points for your administrators. Ask them, "What tasks take the longest?" Then determine how many of those steps can be automated.

Endpoint Management + Security = Enterprise Harmony

Thus far, we've examined the complexities that go into managing a modern, multiplatform enterprise. It has come as no surprise that a larger workforce, more endpoints and/or multiple operating systems can make asset management more difficult. However, up until this point, we've also viewed endpoint management as an extension of IT that is often used as a statistics collector, answering questions such as "How many of *{thing}* do we have in our environment?" If that is as far as we take our tools, then we are doing our enterprise a disservice.

The true value of endpoint management can be assessed when we think of it as a tool for enterprise information security: It's a natural fit. Each area of complexity we've examined up until this point—operating systems, geographic locations, servers and workstations, etc.—presents new attack vectors and/or areas of concern for the security team. When coupled with a manageable number of tools and automated/integrated solutions, well-implemented endpoint management can give your security team the knock-out punch it needs to defend the environment.

Endpoint management should be integrated with information security teams and tools to provide real-time insight into the state of the enterprise. This visibility must include insight into all endpoints that are online and offline.

Preventing Disruption to Normal Business Operations

Unfortunately, there are too many examples of security breaches occurring due to mismanaged endpoints, whether servers, workstations or POS systems. This is not always the fault of a single department. Organic and non-organic growth can increase the size of an enterprise faster than the team(s) can keep up. As networks are joined through mergers and acquisitions and employees are brought on en masse, the endpoint management team can very quickly find itself with tools designed to manage a small enterprise trying to keep up with a large one. This may lead to lack of visibility. Typically, limited visibility translates into a larger attack surface, which can be detrimental to any organization.

We saw evidence of this in that 42% of survey respondents have suffered some sort of exploit that led to data exposure, exfiltration and/or business disruption. Even worse, 15% *do not know* whether their organization had been exploited. This statistic is perhaps the most shocking and speaks volumes to why endpoint management is critical to effective security. See Figure 10.

We also considered compliance as an area where lack of endpoint management could disrupt normal business operations. If an organization processes, handles or stores regulated data types (think PCI), those systems (and potentially the organization's entire network) are subject to certain compliance requirements. In the same thread of detecting endpoint exploits, we asked our respondents about incidents of endpoint noncompliance.

Have any of your endpoint systems been exploited (malicious activities that resulted in data exposure, exfiltration or business disruption) in the past 12 months?

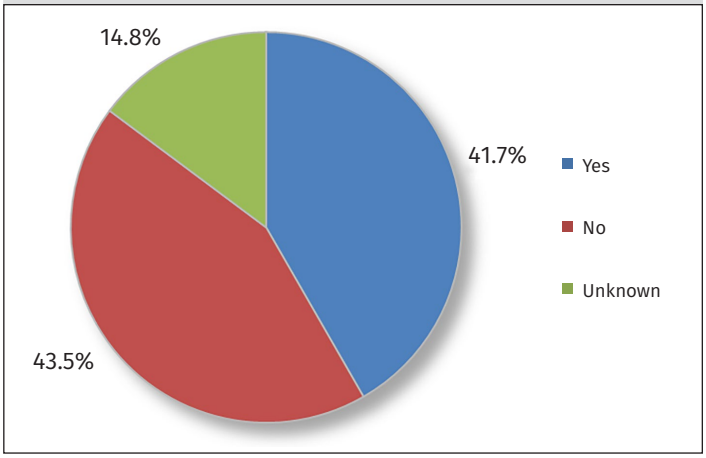

Figure 10. Respondents' Exploit History

The results were somewhat similar to endpoint exploitation, with 41% reporting at least one endpoint compliance issue within the past 12 months. Again, we see a severe gap of visibility, with 22% unable to determine whether an endpoint had fallen within noncompliance status (see Figure 11).

The most troubling statistics lie in the fact that organizations are continuing to operate *blindly*, without knowledge of exploitation or noncompliance. Unfortunately, these gaps often leave room for attackers to infiltrate and pilfer an environment.

To combat how long attackers are surviving within an organization, we sought to understand how long it takes organizations to detect, respond to and remediate security incidents. It's great news (see the annual SANS Incident Response survey for more insight): Approximately 55% of organizations are able to detect within 24 hours, and 59% can respond within the same amount of time. Where the time frame extends is in remediation: Only 33% of organizations can remediate threats within a day. These results are similar to our findings in patching, where organizational complexities are potentially causing longer time frames on endpoint management activities. We'll cover patching in a moment.

See Figure 12 for a breakdown of organizational detection, response and remediation times.

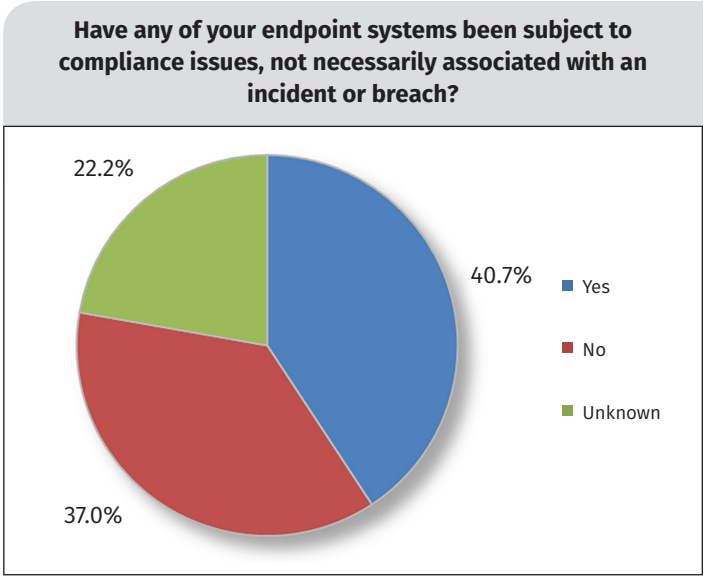

Figure 11. Respondents' Endpoint Noncompliance Status

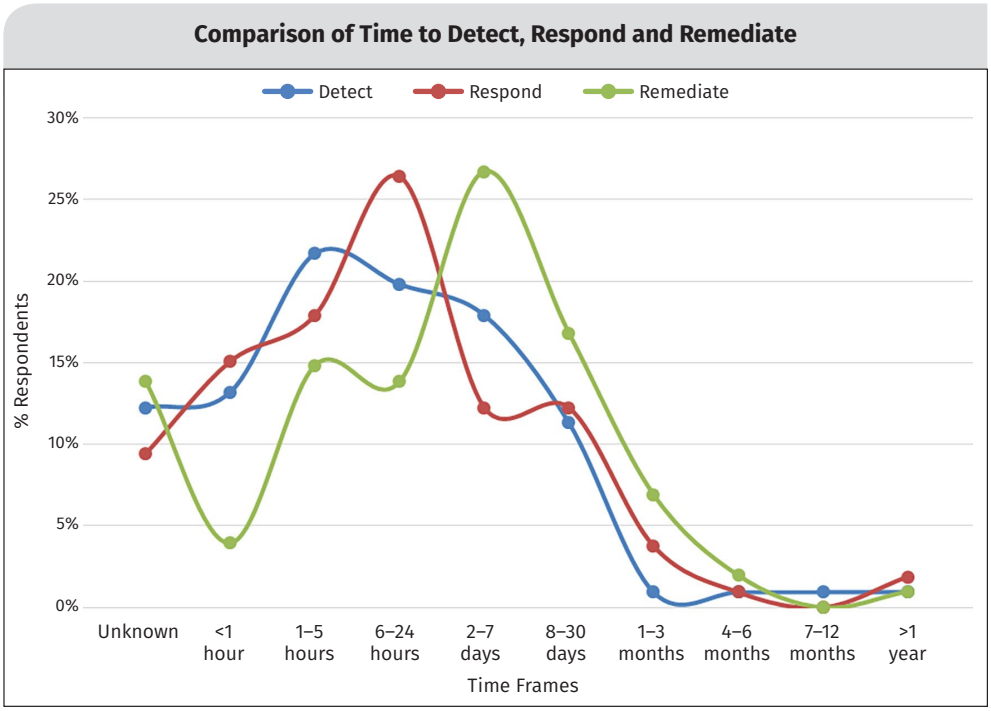

Figure 12. Detection, Response and Remediation Times

Closing the Gaps with Patch Management

While examining endpoint exploits and/or lack of compliance, we also focused on our respondents' abilities to effectively address unpatched systems within their environments. As mentioned multiple times, unpatched systems can lead to exploits that allow attackers to gain unauthorized access to an environment. If there was ever an argument to tie endpoint management and information security together, it's patch management.

However, patch management is often easier said than done. The complexities we examined in the previous section speak directly to the challenges an organization may face when trying to successfully apply patches in its environment.

Every additional application and operating system within an enterprise only makes patching more cumbersome. Focus on unified platforms covering a minimal number of products with a minimal number of dashboards that provide a holistic approach to patch management.

Patches typically fall into two categories: routine and critical/emergency. Let's examine both.

Routine

Routine patches, such as those released on Microsoft's Patch Tuesday, fall on well-known schedules and fix noncritical application and operating system issues. There may be situations where a critical patch is issued during a routine release; however, in such instances, the significance of the patching cycle is amplified by Microsoft. Regardless, for the purposes of this survey, we will consider routine patching as something organizations can plan and prepare for.

Our survey found that a small percentage of our respondents patch within a commendable 48 hours across both workstations (13%) and servers (12%). But several organizations clump at the other end of the spectrum: 11% of respondents reported that workstation patches may take at least one month, and a whopping 25% reported that server patching may take at least *one month, frequently longer*. This is very concerning because SANS' experience has shown that server-side vulnerabilities are often exploited for initial attacker foothold, providing a platform from which to pivot into other areas of the organization.

Patching windows should be considerate of user acceptance testing and business continuity, but not be so long as to provide attackers with the opportunity to take advantage of exploits. Patch as soon as your business can accommodate the inconvenience to avoid leaving yourself unnecessarily exposed.

Critical/Emergency

Critical/emergency patches should, within all enterprises, have an extraordinarily high priority. These types of patches are often released out of band with routine patching and may indicate either a significant operating system or application vulnerability and/or a vulnerability that is currently being exploited in the wild. Neither situation is one an organization wants to experience. Luckily, our survey respondents held this same belief.

The majority (84%) of our respondents indicated that critical patches are applied within two weeks to both user workstations and servers. There is certainly an argument for two weeks being too long, but user acceptance testing and business continuity must also be considered. That being said, an average of well over half of respondents said that critical patches are applied to both user workstations (58%) and servers (56%) within four days, which is certainly an acceptable time frame. See Figure 13.

Finally, patching is more than just pushing an update and calling it a day. We also asked our survey participants just how successful their patching mechanisms were. Particularly, we wanted to find out how many organizations are finding success on the first push. Achieving success

On average, how long does it take your organization to patch impacted endpoints in your enterprise after an emergency or high-priority patch or hotfix that would affect security becomes available?

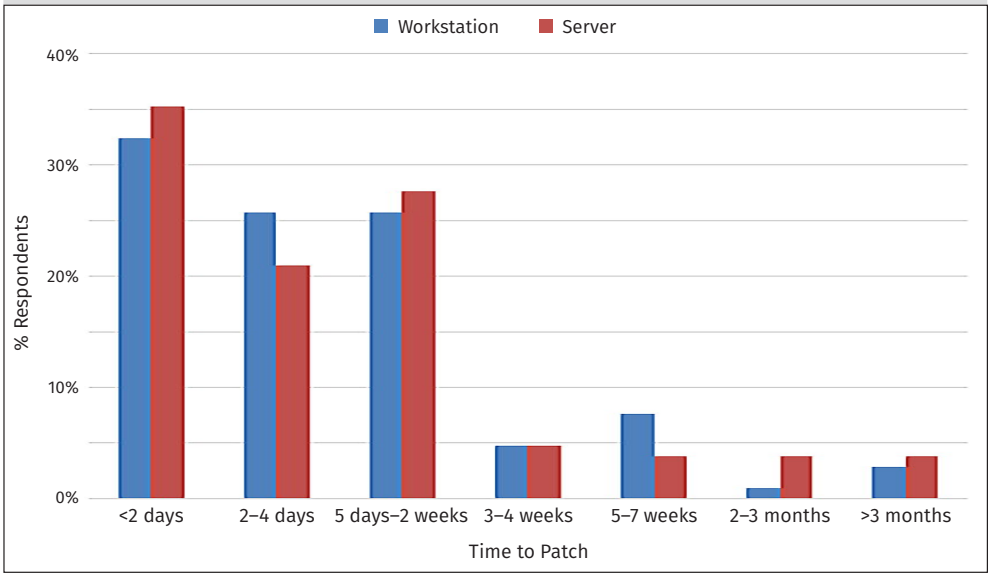

Figure 13. Time to Apply Critical Patches

on the first patch—or being able to determine whether you can—speaks directly to an organization's ability to defend itself. Once a vulnerability has been announced, it's a ticking clock before attackers have weaponized and utilized the exploit. We always want our patch windows to be short and the first patch to be successful so the attackers don't have a chance to take advantage of our systems.

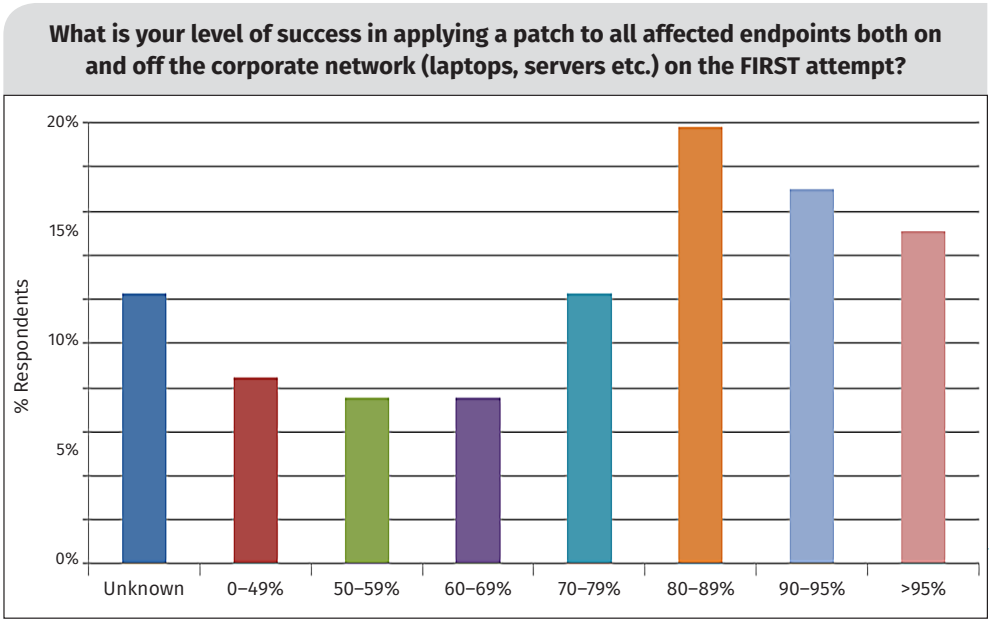

Figure 14. Patching Success of the First Attempt

Luckily, these numbers gave us hope on the state of patching. Approximately 64% of survey respondents indicated that at least 70% of their environment is receiving patches on the first push; a staggering 32% had success rates within the 90th percentile! Only 16% of respondents are seeing less than 60% first-pass patching success rates, which gives them room to improve. As shown in Figure 14, approximately 12% of respondents did not know how successful they were on the first push—again, speaking to the need for visibility among endpoints.

Conclusion

Modern endpoint management is no easy task. As we've seen with this year's survey results, our organizations are dealing with enterprises of vastly different sizes across significantly different geographies. Workforces are becoming increasingly mobile, and users are demanding more and more from their systems, all while IT administrators are trying to keep up. If that weren't enough, we are seeing significant global cyber attacks (think WannaCry or Petya/NotPetya) take advantage of unmanaged and/or unpatched endpoints. **Yes, the need for effective endpoint management is apparent.**

Despite the growing need for endpoint management systems, we encourage stakeholders and IT leaders to be vigilant in choosing tools that complement their organizations. Too often we see organizations simply buying tools to achieve a compliance check box without consideration of the nonmonetary value the organization receives from the tools. Potentially worse, some organizations are asking such questions without any knowledge of the systems in place. **Avoid tool overload. Make sure you're giving your teams the right tools, training and support they need to effectively manage and secure your environment.**

When you decide upon a tool and begin implementation within your environment, the testing has just begun. Ensure that your team is stress-testing your tools and reporting back whether the department is receiving actionable data. **If your team is not seeing improvements in data reported or faster response times to endpoint issues, get a tool that works for you.**

Lastly, we encourage organizations to focus on studying the true cost of whatever tools they decide to implement. Every tool has a cost—whether it's in the form of money, resources or speed. Your organization is going to have to pay at some point. But if you are looking for justification, remember the security risks of inefficient endpoint management. **Can your organization afford to leave multiple operating systems on multiple servers or user workstations open for exploitation? Can you afford the cost of a breach?**

Endpoint management is key to protecting your endpoints. But it comes with a cost, and those costs are not always apparent. Costs may be hidden or take years to surface depending on tool type and implementation coverage. Is the true cost of endpoint management something you are ready to pay? Or would you prefer to pay for the damage done when your ineffective management program enables a successful breach?

About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor, teaching Advanced Digital Forensics, Incident Response, and Threat Hunting (FOR508) and Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (FOR572), and a GIAC Advisory Board member. He is also a principal incident response consultant at a major incident response and forensic analysis company, combining experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, memory and network forensics, as well as network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

IBM Security

Last Updated: October 15th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Houston 2018	Houston, TXUS	Oct 29, 2018 - Nov 03, 2018	Live Event
SANS Gulf Region 2018	Dubai, AE	Nov 03, 2018 - Nov 15, 2018	Live Event
SANS Sydney 2018	Sydney, AU	Nov 05, 2018 - Nov 17, 2018	Live Event
SANS DFIRCON Miami 2018	Miami, FLUS	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS London November 2018	London, GB	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS Dallas Fall 2018	Dallas, TXUS	Nov 05, 2018 - Nov 10, 2018	Live Event
Pen Test HackFest Summit & Training 2018	Bethesda, MDUS	Nov 12, 2018 - Nov 19, 2018	Live Event
SANS Mumbai 2018	Mumbai, IN	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Rome 2018	Rome, IT	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Osaka 2018	Osaka, JP	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS San Diego Fall 2018	San Diego, CAUS	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS November Singapore 2018	Singapore, SG	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS ICS410 Perth 2018	Perth, AU	Nov 19, 2018 - Nov 23, 2018	Live Event
SANS Paris November 2018	Paris, FR	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS Stockholm 2018	Stockholm, SE	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Austin 2018	Austin, TXUS	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS San Francisco Fall 2018	San Francisco, CAUS	Nov 26, 2018 - Dec 01, 2018	Live Event
European Security Awareness Summit 2018	London, GB	Nov 26, 2018 - Nov 29, 2018	Live Event
SANS Khobar 2018	Khobar, SA	Dec 01, 2018 - Dec 06, 2018	Live Event
SANS Dublin 2018	Dublin, IE	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Santa Monica 2018	Santa Monica, CAUS	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Nashville 2018	Nashville, TNUS	Dec 03, 2018 - Dec 08, 2018	Live Event
Tactical Detection & Data Analytics Summit & Training 2018	Scottsdale, AZUS	Dec 04, 2018 - Dec 11, 2018	Live Event
SANS Frankfurt 2018	Frankfurt, DE	Dec 10, 2018 - Dec 15, 2018	Live Event
SANS Cyber Defense Initiative 2018	Washington, DCUS	Dec 11, 2018 - Dec 18, 2018	Live Event
SANS Bangalore January 2019	Bangalore, IN	Jan 07, 2019 - Jan 19, 2019	Live Event
SANS Sonoma 2019	Santa Rosa, CAUS	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Amsterdam January 2019	Amsterdam, NL	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Threat Hunting London 2019	London, GB	Jan 14, 2019 - Jan 19, 2019	Live Event
Secure DevOps Summit & Training 2018	OnlineCOUS	Oct 22, 2018 - Oct 29, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced