AimPoint Group
high-impact marketing

2020 CYBER HYGIENE REPORT
WHAT YOU NEED TO KNOW NOW

Lessons learned from a survey of the state of endpoint patching and hardening

SPONSORED BY AUTOMOX

Contents

Cyber Hygiene in the Real World 3
Summary of Findings 4
The Impact of Endpoint Patching and Hardening on Data Breaches 5
Current Ability to Maintain Cyber Hygiene 6
The Need for Speed: Are Enterprises Patching and Hardening Fast Enough? 8
Factors Preventing Effective Endpoint Patching and Hardening 11
The Current State of Automation 13
A Brief Introduction to Cyber Hygiene Platforms 15

Cyber Hygiene in the Real World

Most IT professionals are aware that endpoint patching and hardening are basic functions that enterprises must master to provide effective cybersecurity. Most are also aware that there is a lot of room for improvement in the way their own organization performs these functions.

But most IT professionals admit that they don't have a good feel for exactly how important endpoint patching and hardening are relative to other security controls, how well most enterprises are handling them now, and what are the most common problems enterprises have in performing them.

This report sheds light on those questions using data from a survey of 560 IT operations and security professionals at enterprises with between 500 and 25,000 employees, across more than 15 industries and at government agencies.

Our goal is to help readers benchmark the performance of their organizations against peers and develop insights into how to make improvements that will pay off.

A LITTLE TERMINOLOGY

The Center for Internet Security (CIS), a non-profit organization devoted to identifying, developing, and promoting best practice solutions for cyber defense, defines cyber hygiene as a set of baseline practices to proactively protect organizations from cyber threats. The CIS provides a list of basic controls for reducing the attack surface of enterprises and protecting information assets. The first six focus on eliminating vulnerabilities on endpoints (mobile devices, laptops, servers, and workstations), especially through automated patching and the detection and remediation of misconfigurations.

The two aspects of cyber hygiene that we focus on here are:

1. **Patch management (informally, "patching")** involves maintaining an inventory of hardware and software assets and ensuring that updates to operating system software and application software are continuously deployed and installed on endpoints.
2. **Endpoint hardening** is concerned with proactive measures that prevent endpoints from being compromised or used in cyberattacks, including closing ports, restricting administrative privileges, eliminating unnecessary and unapproved software, and ensuring that firewalls, antimalware packages and other security tools are correctly configured.

Technically, endpoint hardening includes patch management, but in our survey we defined hardening for the respondents as excluding operating systems and application patching, and asked separate questions about each field. That allowed us to gather data specifically about patch management, while also analyzing issues related to other endpoint hardening practices. The separation of the two fields also reflects the organization of most IT departments, which have dedicated teams for patch management and use different people and resources for other endpoint hardening tasks.

THE ADVANTAGES OF BETTER CYBER HYGIENE

Why should IT professionals care about improving cyber hygiene? Because it can help IT organizations address three major objectives:

Reducing risk—endpoints that are quickly and effectively patched and hardened are much less vulnerable to compromise and much less likely to be involved in data breaches.

Lowering cost—streamlining and automating patching and hardening can dramatically improve the productivity of IT operations and security operations (SecOps) personnel, reduce the number of alerts that teams have to investigate, and free staff to handle other critical operations and security work.

Accelerating business innovation—faster, more reliable processes for patching and hardening, and extending those processes to new technology areas, enable enterprises to quickly and confidently take advantage of innovations in areas like mobile computing and cloud platforms.

BUT...

...while these are all important advantages in theory, in practice:

- Is it really necessary to invest in improving cyber hygiene?
- In what areas are endpoint patching and hardening adequate today?
- In what areas do they need to be improved, and how can they be improved?

Let's look at the data from our survey and see what your peers have to say.

Summary of Findings

- **Missing patches and misconfigurations** are three of the four leading root causes of data breaches. Missing OS patches was cited as the #1 technical attack surface exposure to cause a data breach.

  (See Figure 2 on page 5.) A case can be made that improving cyber hygiene is the most cost-effective way to break the "kill chain" of many advanced attacks.

- **Survey participants are least confident** about maintaining cyber hygiene for systems at remote sites, servers and desktops on cloud platforms, and mobile devices.

  (See Figures 3, 4, and 5 on pages 6, 7, and 8.) This probably reflects the fact many enterprises are using manual methods or patch management and hardening tools designed for corporate data centers and offices which are difficult to use or can't be used at all for remote and cloud environments.

- **Few organizations patch endpoints fast enough** or harden them frequently enough to protect against new threats, especially zero-day attacks.

  (See Figures 5, 6, 7, and 8 on pages 8, 9, and 10.) Less than half can patch affected systems in three days or less (fast enough to defend against most new critical threats). Only about twenty percent can patch in a day or less (fast enough to secure organizations against zero-day attacks). Perhaps most discouraging, almost sixty percent harden desktops, laptops, and servers only monthly or annually, which is an invitation to adversaries.

- **Enterprises say they prioritize patching and hardening,** but are inhibited by basic issues such as difficulty patching systems belonging to mobile employees and remote offices, inefficient patch testing, lack of visibility into endpoints, lack of automated patch management, and insufficient staffing in SecOps and IT operations.

  (See Figures 9, 10, and 11 on pages 11 and 12.) Either managers in many enterprises are only paying lip service to prioritizing patching and hardening, or they are not aware of solutions like cyber hygiene platforms that can overcome these inhibitors (discussed in the final section of this report).

- **Organizations that have fully automated endpoint patching and hardening** are outperforming others in the speed and frequency of hardening.

  (See Figures 12 and 13 on pages 13 and 14.) Automation isn't a panacea, but it certainly helps. There is a very strong correlation between automation and the ability to patch endpoints faster and harden them more frequently. Clearly, most enterprises should be automating more of their patching and hardening processes.

The Impact of Endpoint Patching and Hardening on Data Breaches

Is there evidence that endpoint patching and hardening can reduce data breaches?

Yes, definitely! When asked about the root causes of data breaches, respondents cited a missing OS patch as the #1 technical attack surface exposure. And three of the four most common root causes of those breaches can be addressed with better cyber hygiene.

It is no surprise that data breaches are a very serious issue. Among the enterprises in our survey, more than four out of five suffered at least one breach in the past two years. (Figure 1)

FIGURE 1:
Organizations with breaches in the past two years (n=522)

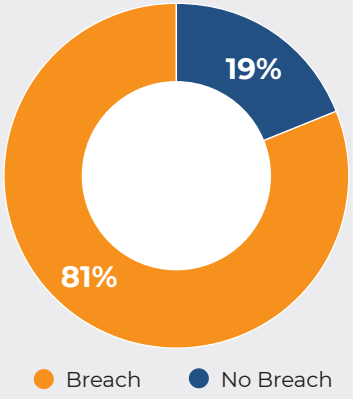
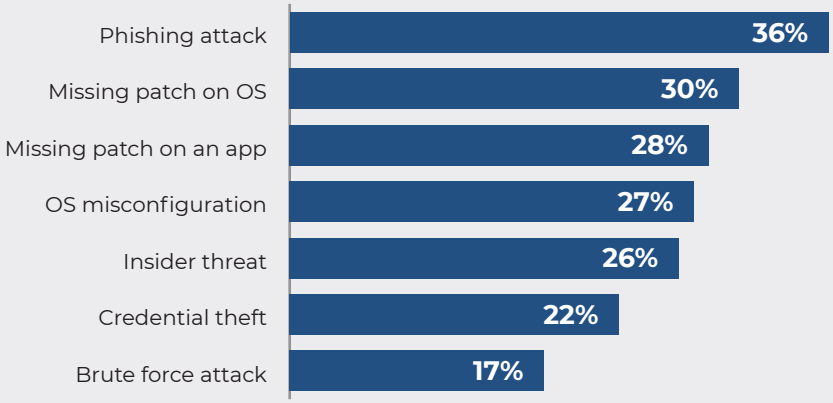


FIGURE 2:
For any breaches your organization experienced in the past two years, select the root causes that were identified (n=482)



But would better cyber hygiene have helped? The data in Figure 2 says yes. When asked about the root causes of data breaches, respondents cited phishing attacks most often, but the next three causes could have been addressed by better patching and hardening. Missing operating systems patches, missing application patches, and operating system misconfigurations were each cited more frequently than such high-profile issues as insider threats, credential theft, and brute force attacks. These results support the idea that faulty patching and hardening are the IT world's most neglected silent killers.

The survey results confirm that most data breaches involve multiple factors (respondents were asked to select "all that apply"). As we know from many studies, advanced attacks often start with a phishing attack or credential theft, then take over an endpoint by taking advantage of a missing patch or a misconfiguration, then use the compromised endpoint to search the network and target systems with confidential data.

Improving endpoint patching and hardening may be the most cost-effective way to break the "kill chain" of most advanced attacks.

An important implication is that you can defeat most advanced attacks by breaking the "kill chain" at any point, and improving cyber hygiene may be the most cost-effective method for doing so, potentially much more cost-effective than trying to vanquish phishing attacks or rogue insiders.

SPONSORED BY AUTOMOX

Current Ability to Maintain Cyber Hygiene

We asked several questions to assess the effectiveness of cyber hygiene practices today.

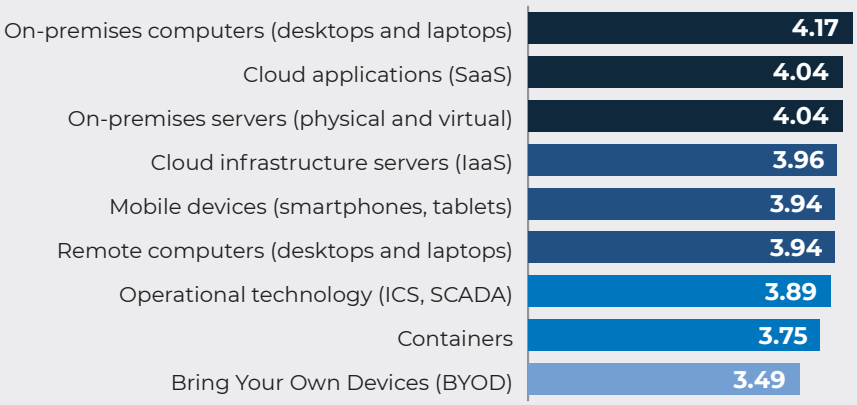
Cyber hygiene is better for some IT components than others

When it comes to cyber hygiene, which IT components are under control and which keep IT teams up at night?

Organizations are most confident about cyber hygiene for on-premises systems and SaaS applications. Remotely located and mobile systems cause the most concern because they are harder to reach and aren't handled well by legacy patch management and hardening tools.

Figure 3 shows how respondents rated their organization's ability to maintain cyber hygiene for a variety of IT components. Cyber hygiene was defined as including both patch management and hardening.

FIGURE 3:
Rate your organization's overall ability to maintain cyber hygiene (best practices like patching and configuring to secure digital assets) for each of the following IT components (Scale of 1 to 5, with 5 being highest, n=560)



Survey participants were more comfortable about being able to maintain cyber hygiene for on-premises computers and servers compared with remote and mobile systems such as servers on infrastructure as a Service (IaaS) cloud platforms, mobile devices (smartphones and tablets), and computers at remote locations. That's not surprising given that (a) it is easier to monitor on-premises systems, and (b) many organizations are using patch management and hardening tools that were designed for on-premises systems and don't provide good coverage of remote computers, mobile devices, and cloud-based systems.

Many organizations are using patch management and hardening tools that were designed for on-premises systems and don't provide good coverage of remote computers, mobile devices, and cloud-based systems.

Respondents did feel comfortable about cyber hygiene for cloud-based software as a service (SaaS) applications, presumably because SaaS service providers take care of patching those applications and their underlying infrastructure.

Respondents were much less confident about operational technologies like industrial control systems (ICS) and supervisory control and data acquisition (SCADA) devices, containers for application workloads, and bring your own device (BYOD) mobile devices. We believe these concerns are based on difficulty reaching these platforms, and again, the fact that many organizations are using legacy patch management and hardening tools that don't address devices outside of the old premises-based model.

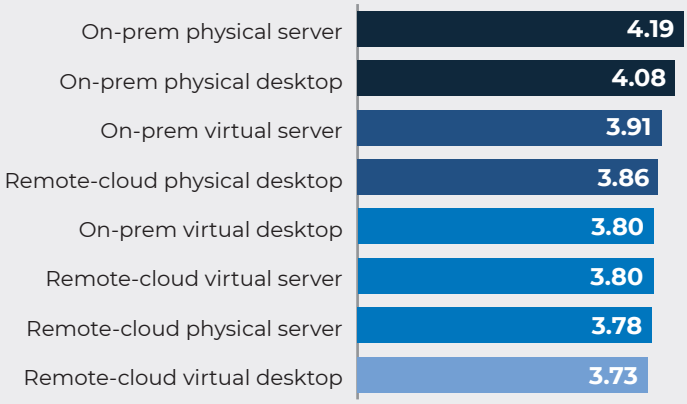
Characteristics of systems most (and least) easily patched

What factors make systems easier (or harder) to patch?

Organizations are most confident about patching on-premises physical servers, and least confident about systems that are in the cloud, and/or desktops, and/or virtual.

Figure 4 shows how respondents rated the adequacy of their organization's ability to patch on-premises and cloud-based desktops and servers in both physical and virtual forms.

FIGURE 4:
Rate the adequacy of your organization's capabilities for patching each of the following systems
(Scale of 1 to 5, with 5 being highest, n=560)



The factors causing confidence or concern are fairly consistent. For the most part:

- On-premises systems are being patched better than their counterparts in the cloud
- Servers are being patched more reliably than desktops
- Physical systems are being patched better than their virtual opposite numbers

Given these three factors, it is not surprising that organizations are least confident about virtual desktops on cloud platforms.

The only exceptions to these rules are physical desktops in the cloud, which evidently are being patched more easily than would be expected, and in the cloud virtual servers are very slightly ahead of physical servers.

These patterns can be explained by the fact that (once again) most existing patch management tools don't work well with cloud-based endpoints, and that virtual systems are very dynamic and therefore harder to monitor and protect than physical ones.

The Need for Speed: Are Enterprises Patching and Hardening Fast Enough?

The effectiveness of cyber hygiene is partly a function of speed.

When vendors, security consulting firms, and white hat hackers announce the discovery of critical vulnerabilities, cybercriminals and state actors are usually able to weaponize them within seven days. To ensure protection from the attacks that inevitably follow, security experts recommend that enterprises patch and harden all vulnerable systems within 72 hours.

Zero-day attacks, which emerge with no warning, pose an even greater challenge. Experts suggest that enterprises should aim to patch and harden vulnerable systems within 24 hours of their disclosure.

And it's not only about responding to emergencies. With dental hygiene, it is important to brush and floss teeth frequently to prevent bits of sugar from starting tooth decay. With cyber hygiene, endpoints need to be scanned and assessed on a regular basis, and if problems are found, promptly patched or reconfigured.

So how fast can enterprises respond to threats, and is their current performance good enough?

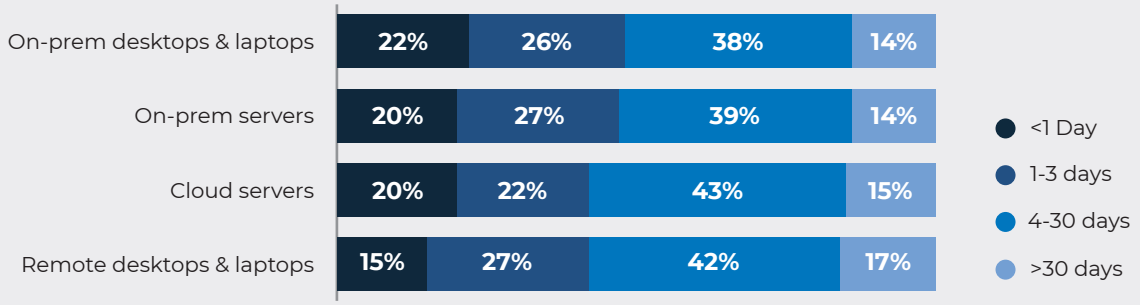
Few organizations patch fast enough

Can organizations patch fast enough to head off new threats before they are weaponized and deployed?

Unfortunately, less than 50 percent of organizations can patch critical vulnerabilities within 72 hours of disclosure, and only about 20 percent can patch within the 24-hour window available to stop zero-day attacks. Also, around 15 percent of systems remained unpatched after 30 days.

The data shown in figure 5 give cause for concern. When survey participants were asked about the time required for their organizations to patch affected systems after the announcement of a new critical or high-severity vulnerability, only about one in five reported that the task could be done in less than a day, and less than half could finish in three days or less.

FIGURE 5:
Upon announcement of a new critical/high-severity vulnerability, how quickly on average, do you patch your affected systems? (n=555)



To put that another way, if best practices are to patch within 72 hours of the disclosure of critical vulnerabilities, and within 24 hours of the appearance of zero-day attacks, less than 50 percent of enterprises can meet the first standard and only about 20 percent can match the second.

Performance is even worse for remote desktops and laptops, with only 42 percent being able to patch within three days and 15 percent within one. This points yet again to the special challenges of patching and hardening remote endpoints.

SPONSORED BY AUTOMOX

Finally, the fact that around 15 percent of systems remain unpatched after 30 days is evidence either that patching workloads are beyond the capacity of current staff and tools, or that patch management processes are broken in a significant number of enterprises.

Note that our survey only asked about patching times for critical and high-severity vulnerabilities. Patching times for medium and low priority vulnerabilities are undoubtedly much longer. Other research indicates that the average time to deploy a patch across all infrastructure is much longer: 102 days.[1] This is a real concern, because some smart adversaries target old CVEs (Common Vulnerabilities and Exposures) and vulnerabilities with medium CVSS (Common Vulnerability Scoring System) ratings, precisely because they know that these are patched more slowly. IT organizations need to track and improve their Mean Time to Patch (MTtP) for medium and low priority vulnerabilities as well as the critical and high priority ones!

If best practices are to patch within 72 hours of the disclosure of critical vulnerabilities, and within 24 hours of the appearance of zero-day attacks, less than 50 percent of enterprises can meet the first standard and only about 20 percent can match the second.

Speed of response

Do survey respondents think their organizations can respond quickly enough to threats?

A full 59 percent agree that their processes and tools do not enable them to respond quickly enough to zero-day threats. Their answers show a general room for improvement in responding to new threats.

As shown in Figure 6, opinions on responding quickly to vulnerabilities are mixed. A solid 39 percent of respondents strongly agree that their organizations can respond fast enough to critical and high severity vulnerabilities to remediate successfully. However, a majority (52 percent) are lukewarm, either agreeing "somewhat" or neither agreeing or disagreeing, and another 8 percent disagree or disagree strongly.

FIGURE 6:
My organization responds fast enough to potential critical/high severity vulnerabilities to achieve impactful results from our remediation efforts (n=560)

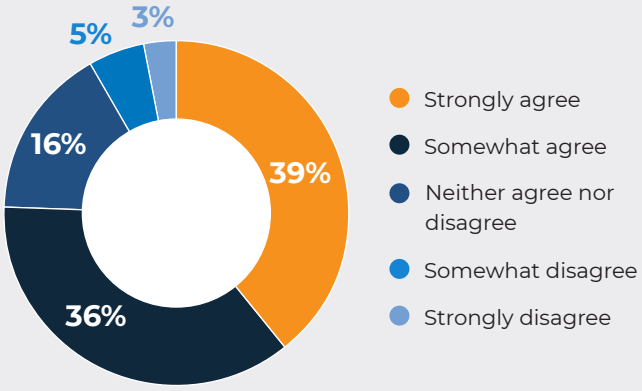
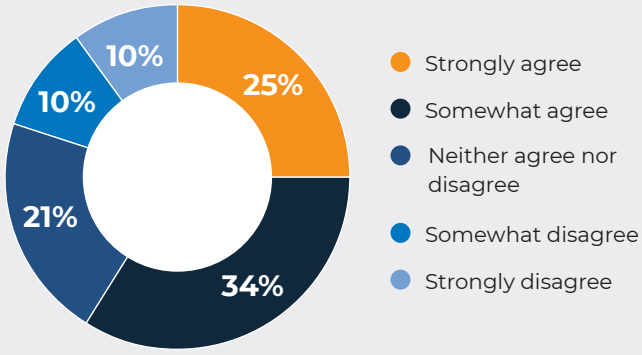


FIGURE 7:
Zero-day threats are a major issue for my organization because our processes and tools do not enable us to respond quickly enough (n=560)



A full 59 percent of respondents agree or strongly agree that zero-day threats are a major issue for their organizations because processes and tools do not enable them to respond quickly enough.

1. Ponemon Institute. *2018 State of Endpoint Security Risk*. October 2018. cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf

SPONSORED BY AUTOMOX

Figure 7 illustrates survey participants have a very high level of concern about zero-day threats. A full 59 percent agree or strongly agree that zero-day threats are a major issue for their organizations because processes and tools do not enable them to respond quickly enough. This is consistent with the data in Figure 5 that shows that only about 20 percent of organizations can patch systems within the 24 hour window before most zero-day attacks start hitting the enterprise.

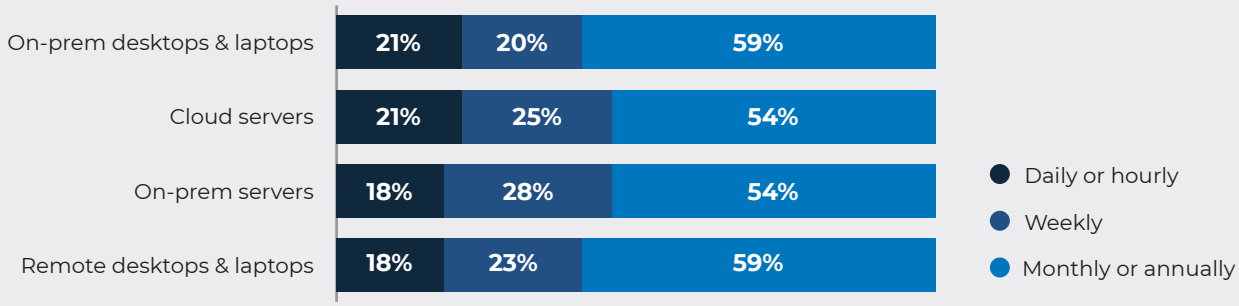
Enterprises are playing with fire on hardening

Do organizations harden systems frequently enough to protect themselves?

About 20 percent are hardening systems daily or hourly, but almost 60 percent perform this task only monthly or annually.

Figure 8 records respondents' reports on how frequently different types of systems are hardened (with hardening defined to exclude patching). The data shows that most enterprises lag badly in this area.

FIGURE 8:
Which choice best describes the frequency for hardening configurations for on-premises and remote or cloud desktops, laptops, and servers? (n=560)



We were very discouraged to see that almost 60 percent reported that hardening is done only monthly or annually—a very serious state of affairs that requires more attention from enterprises.

On one hand, it is encouraging to see that about one in five enterprises are able to harden endpoints daily or hourly.

However, we were very discouraged to see that almost 60 percent reported that hardening is done only monthly or annually. We believe that this is a very serious state of affairs. Leaving servers, desktops, and laptops misconfigured, with extra ports open, and with excess privileges is playing with fire. Clearly this is an area that requires more attention from enterprises.

Factors Preventing Effective Endpoint Patching and Hardening

Recognizing the need for improvement is a first step, but to decide exactly what to improve we need to understand the factors that are preventing endpoint patching and hardening from being carried out effectively today.

Obstacles to patching on-premises and cloud-based systems

What factors inhibit organizations' ability to patch systems on premises and in the cloud?

While patching is not considered a low priority, organizations are struggling with a combination of issues ranging from inability to take systems offline, to difficulties working with systems in remote locations, to inefficiencies in basic patching processes.

Figure 9 shows the factors inhibiting the ability of organizations to path on-premises systems against new critical and high severity vulnerabilities. Figure 10 shows obstacles for successfully patching remote and cloud systems.

FIGURE 9:
Upon announcement of a new critical/high severity vulnerability, rate how the following inhibit your ability to patch affected on-premises systems? (Scale of 1 to 5, with 5 being highest, n=560)

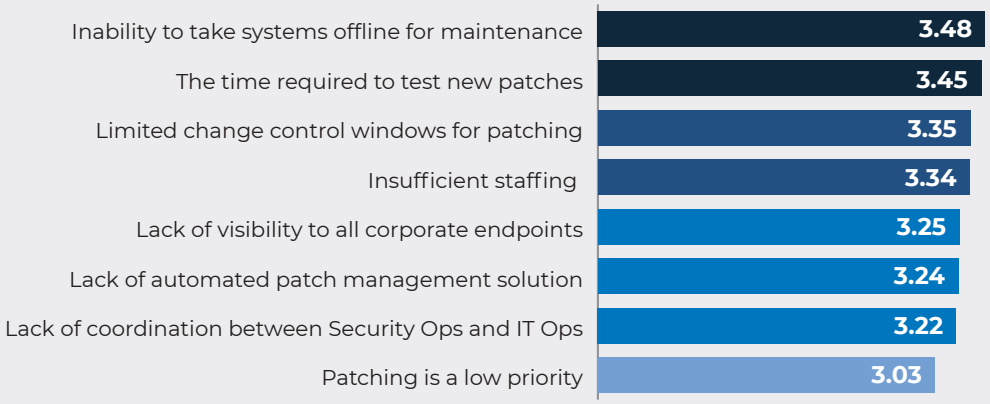
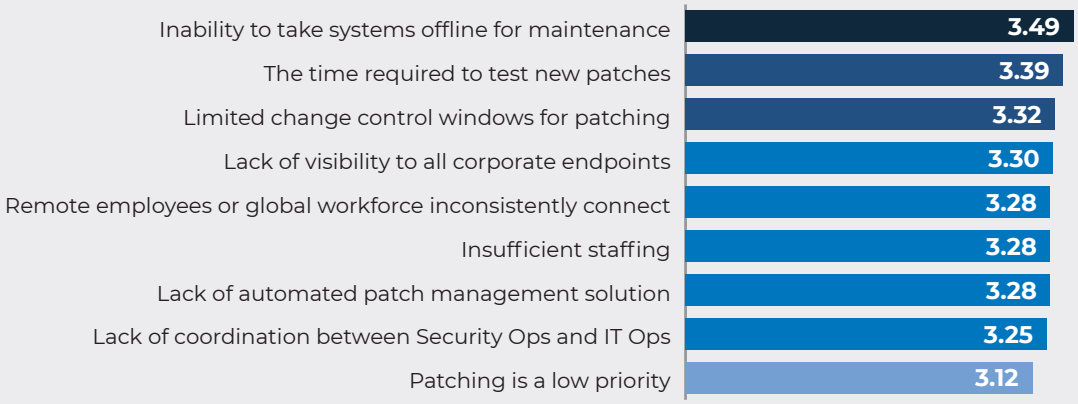


FIGURE 10:
Upon announcement of a new critical/high severity vulnerability, rate how the following inhibit your ability to patch affected remote or cloud systems (Scale of 1 to 5, with 5 being highest, n=560)



It is encouraging that "patching is a low priority" is the least commonly cited negative factor. This finding implies that management is aware of the importance of efficient patching, so IT operations and SecOps staff don't have to fight battles for recognition of the importance of their tasks in this area.

The most commonly cited factor is the inability to take systems offline for maintenance. This reflects the fact that systems running mission-critical applications can only be brought down very briefly for maintenance. It may also be a symptom of patching tools that require too long to update and configure software, creating a high cost in terms of application downtime.

Another major issue is difficulty patching systems belonging to mobile employees and remote offices which don't connect consistently to the corporate network.

Other inhibitors relate to inefficiencies in the day-to-day "blocking and tackling" activities related to patch management, such as testing new patches, lack of visibility into endpoints, and lack of an automated patch management solution. Many of these could be addressed by better patch management tools and processes.

Finally, insufficient staffing is an important issue. That's not surprising given the worldwide shortage of IT talent in general, and SecOps personnel in particular.

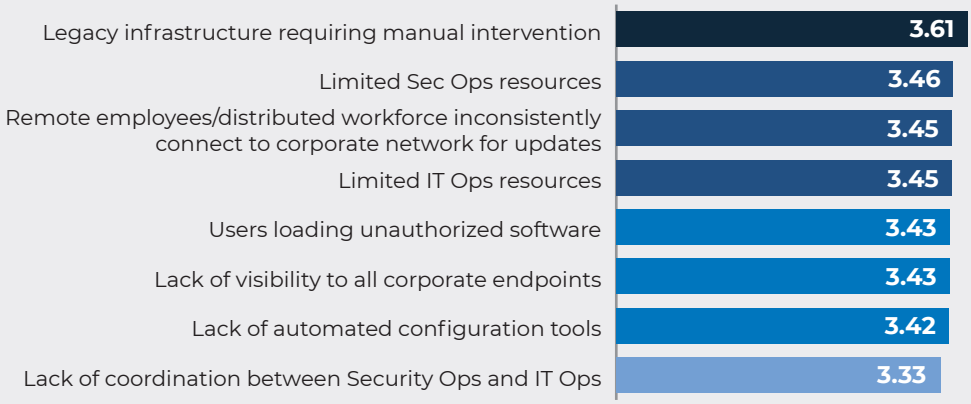
Obstacles to more frequent hardening of endpoints

What factors negatively affect organizations' ability to harden systems?

Legacy infrastructure, limited SecOps and IT Ops resources, and difficulties working with systems in remote locations are common obstacles that negatively affect the ability of organizations to harden their systems.

Figure 11 shows participants' assessment of factors that have a negative effect on how often endpoints are hardened. We know from the data in Figure 8 that more than half of the enterprises harden endpoints only monthly or annually, leaving them unnecessarily exposed to attacks, so these inhibitors clearly have a negative impact on overall IT security.

FIGURE 11:
Rate how the following negatively affect the frequency of hardening your systems
(Scale of 1 to 5, with 5 being highest, n=560)



The most common problem is legacy infrastructure that requires manual effort for assessment and remediation. Limited staffing in both SecOps and IT operations are also near the top, as are challenges managing endpoints of remote employees who don't often connect to the corporate network and are therefore outside the view of the IT organization for long periods.

The Current State of Automation

Where do organizations stand today in their use of automation for cyber hygiene, and does this automation really help?

A full 96 percent of organizations have some automation for endpoint patching and hardening, but only 23 percent are fully automated. While automation is no panacea, higher levels of automation are associated with better cyber hygiene.

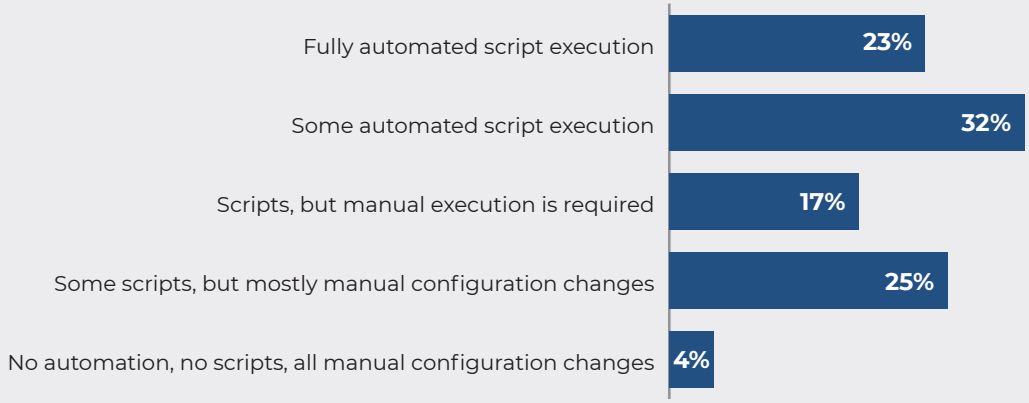
Automation of endpoint patching and hardening processes is potentially an antidote for nearly all of the challenges described above. Automation can dramatically speed up cyber hygiene processes, thereby:

- Enabling existing IT operations and SecOps staffs to patch and harden more systems with less effort
- Reducing the amount of system and application downtime needed for patching and hardening

Part of automation in this context means scheduling and automatically managing activities like scanning systems for software and vulnerabilities, collecting data, analyzing what needs to be done, and reporting on successful and unsuccessful tasks. But the other critical, and in practice more challenging, aspect of automation for patching and hardening involves managing scripts for installing and configuring software updates on endpoints and for performing tasks like fixing misconfigurations and closing ports.

Our survey asked participants to describe their organization's level of automation for hardening processes, and the results are shown in Figure 12.

FIGURE 12:
Which option best describes your organization's level of automation for hardening practices, such as following the Center for Internet Security CIS Controls™ (e.g., port lockdown, setting least privilege, setting administrator privileges)? (n=532)



The good news is that a mere 4 percent of enterprises have no automation and handle all tasks manually. The not-so-good news is that only 23 percent are fully automated. Roughly three out of four fall in the middle, with some scripts and automation, but also tasks being performed manually. Those include 25 percent that are still making manual configuration changes and 17 percent that still execute some scripts manually.

But does automation really produce significant benefits? To find out, we cross-tabulated the data from Figure 8 and Figure 12 to produce Figure 13.

FIGURE 13:
Relationship between automation and the frequency of server hardening (n=560)

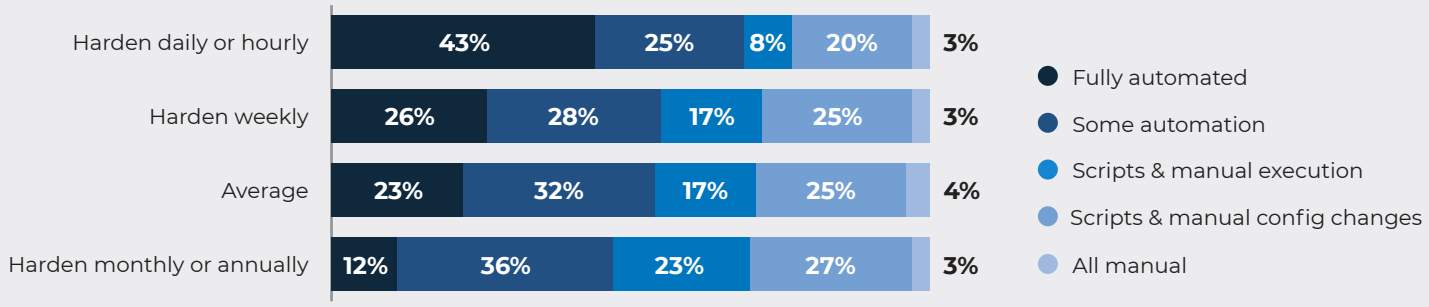


Figure 13 shows how much the enterprises that reported each range of hardening are automated. It demonstrates that more automation usually leads to the ability to harden servers significantly more frequently.

The correlation is very clear: on average, more automation is associated with faster, more frequent hardening.

Forty three percent of organizations who are able to harden daily or hourly are fully automated, while only 26 percent of those who harden weekly and 12 percent of those that harden monthly or annually make the same claim. This doesn't mean that every organization that had daily or hourly hardening are automated. A few say they have very little or no automation. This may be because they have very large, skillful staffs, or more likely, that they have relatively simple environments where frequent hardening faces fewer obstacles. But the correlation is very clear: on average, more automation is associated with faster, more frequent hardening.

SPONSORED BY AUTOMOX

A Brief Introduction to Cyber Hygiene Platforms

Good business people never raise issues without recommending a solution, or at least suggesting how to find a solution, so that's what we'll do here.

Cyber hygiene platforms can address many of the problems raised by the participants in this survey. They are designed to systematize and automate many of the tasks that go into patching and hardening endpoints. That includes automating and managing processes that:

- Provide visibility into all the endpoints in the enterprise and maintaining a complete inventory of the software on them
- Identify missing patches for operating systems and both approved and unapproved application software
- Identify misconfigurations and compliance issues
- Deploy and install software on endpoints
- Run scripts to fix configuration issues
- Ensure reliable patching and hardening of systems used by remote users and global workforces
- Provide reporting and documentation showing that patching and hardening activities are being carried out in compliance with regulations and corporate policies

The best cyber hygiene platforms extend these processes not only across data centers and corporate offices, but also to remote locations and cloud platforms. They handle applications deployed in containers and virtual environments across multiple operating systems.

You can probably imagine how these capabilities can minimize or eliminate many of the issues and inhibitors raised in our survey. For example, a cyber hygiene platform can help an organization:

- Better manage patching and hardening of systems in remote locations and on cloud platforms and applications in containerized and virtual environments
- Protect mobile devices and workers, even when they infrequently connect to the corporate network
- Speed up patching enough to protect against even zero-day attacks
- Harden systems on a continuous basis to dramatically reduce the window in which adversaries can exploit misconfigurations
- Improve staff productivity so existing SecOps and IT operations teams can manage patching and hardening for more systems, across more environments, with less effort

Ultimately, these capabilities can enable IT organizations to succeed in the three areas we mentioned at the beginning of this survey: reducing risk, lowering cost, and accelerating business innovation.

Learn how you can reduce your risk with simple, fast, and cloud-native endpoint hardening from the Automox cyber hygiene platform at:
www.automox.com/features

A Word from the Sponsor

Facing growing threats and a rapidly expanding attack surface, understaffed and alert-fatigued organizations need more efficient ways to eliminate their exposure to vulnerabilities. Automox is a modern cyber hygiene platform that closes aperture of attack by more than 80% with just half the effort of traditional solutions.

Cloud-native and globally available, Automox enforces OS and third-party patch management, security configurations, and custom scripting across Windows, macOS, and Linux from a single intuitive console. IT and SecOps can quickly gain control and share visibility of on-prem, remote, and virtual endpoints without the need to deploy costly infrastructure.

Automox dramatically reduces corporate risk while raising operational efficiency to deliver best-in-class security outcomes, faster and with fewer resources.