WHITE PAPER

Combating Patch Fatigue

Are we overwhelming IT to the detriment of enterprise security?

AUTHORS:

Lane Thames, Security Researcher, Tripwire

Tyler Reguly, Manager, Security Research, Tripwire

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

A vulnerability is a bug or flaw in software or hardware that can be exploited for malicious gains. In order to avoid miscommunication and facilitate coordinated discussion, MITRE maintains the CVE (Common Vulnerabilities and Exposures) database, which establishes a naming standard for all vulnerabilities. In 2015, over 6,000 new CVEs were assigned. If only one-tenth of those vulnerabilities affected devices in your area of responsibility, you would have been responsible for resolving 630 vulnerabilities annually or 2.5 vulnerabilities each business day.

The logical response is that a single patch generally resolves multiple vulnerabilities. Take, for example, MS15-112, the November security bulletin for Internet Explorer, which resolved 26 vulnerabilities. It's all too common to hear the statement, "just apply the MS15-112 patch." This statement leads to the assumption that a single patch resolves multiple vulnerabilities. While it's true that the application of a single patch will resolve multiple vulnerabilities, within MS15-112 there are 32 patches available for download and four more that are referenced. If we assume that this is normal, we can then conclude that there are more patches issued annually than there are vulnerabilities.

These numbers bring us to the concept of Patch Fatigue, which can be summed up in a single question: Are we overburdened with patches?

Based on a recent survey we conducted of 483 IT professionals who are involved in the patch management process across organizations of all sizes, the answer is a resounding "yes." Here are some of the data points that led us to this conclusion:

- Almost 20 percent of organizations manage their patching process without patch management software
- Nearly half of all individuals surveyed admit that at times they struggle to keep up—or find themselves completely overwhelmed with the volume of patches released
- More than two-thirds of organizations surveyed have fewer than five people actively involved in their patch management process

On top of the negative impacts to employees, overburdened IT and security teams lead to poor security hygiene within the enterprise. If teams cannot install security patches as quickly as they are released then vulnerabilities will linger, providing additional attack vectors for malicious actors to use during a data breach. This can result is substantial losses, as a report1 by IBM indicates that the average cost of a data breach is $3.8 million.

Employees that find themselves overburdened by their workload tend to be stressed and anxious according to a report published by Workforce2. This stress decreases employee productivity and leads to a loss of talented, skilled employees. According to WebMD3, stress can lead to heart disease, asthma, obesity, diabetes, headaches, depression, and a number of other health-related issues. In a follow-up report4 published by Workforce, they showed that employees that are stressed and feeling pressured are generally unhappy and end up looking at other employment opportunities where their happiness will increase.

With the impact of Patch Fatigue clearly defined and rather self evident, we will take a look at the reasons for and causes of Patch Fatigue in the remainder of this white paper. More specifically, we will investigate the historical trends in patch management and the current shifting trends across vendors. We also highlight a number of factors contributing to patch fatigue on both the vendor and enterprise sides of the equation. Finally, we offer a number of solutions that both vendors and enterprises can employ to lessen the pain of Patch Fatigue.

Setting the Stage

Patch management is the process of acquiring, testing and installing software patches for information technology assets. Patch management plays a critical role in maintaining the overall security posture for enterprise information technology systems. Unfortunately, it seems like every day we hear about a new data breach, many of which occur or escalate due to improper patch management. Moreover, the footprint of assets that IT departments have to manage is exploding due to business needs revolving around new technology trends such as mobile computing and the Internet of Things. Given the constant flux of new security events happening across the globe along with rapidly changing environments of modern day IT systems, we should evaluate the current state of affairs with respect to patch management.

To begin this study, we considered the amount of workload required to maintain patches for a "gold" desktop image representing a typical enterprise workstation. The gold image contained a collection of baseline software common to many enterprise organizations. Next, we calculated the number of security

Software Component	Security Patches in 2015
Windows 7	120
Internet Explorer	13
Chrome	16
Microsoft Office 2013 Professional	13
Oracle Java	4
Adobe Flash	13
Adobe Shockwave	3
Microsoft Silverlight	3
Adobe Reader	3

Table 1. Security patch statistics for the gold image

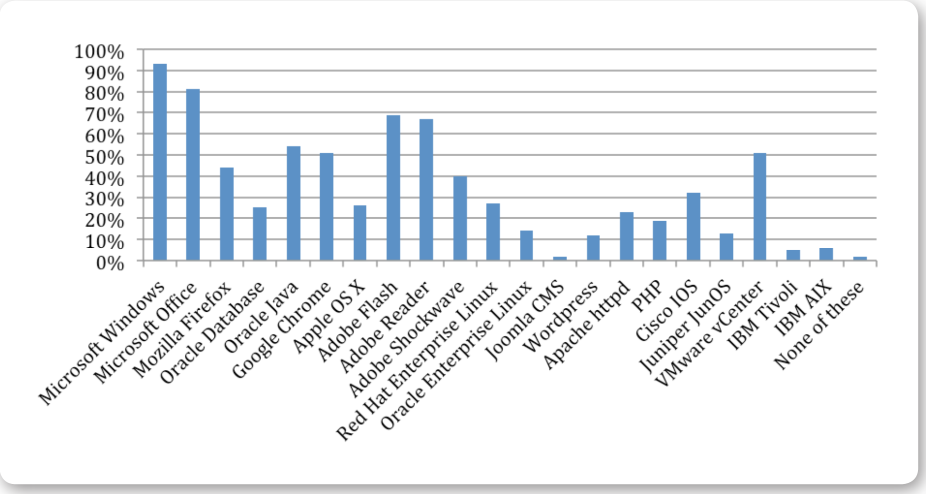

Fig. 1 Tripwire Log Center screenshot showing the creation of a correlation rule that correlates five failed logins to a successful login and to modified user privileges.

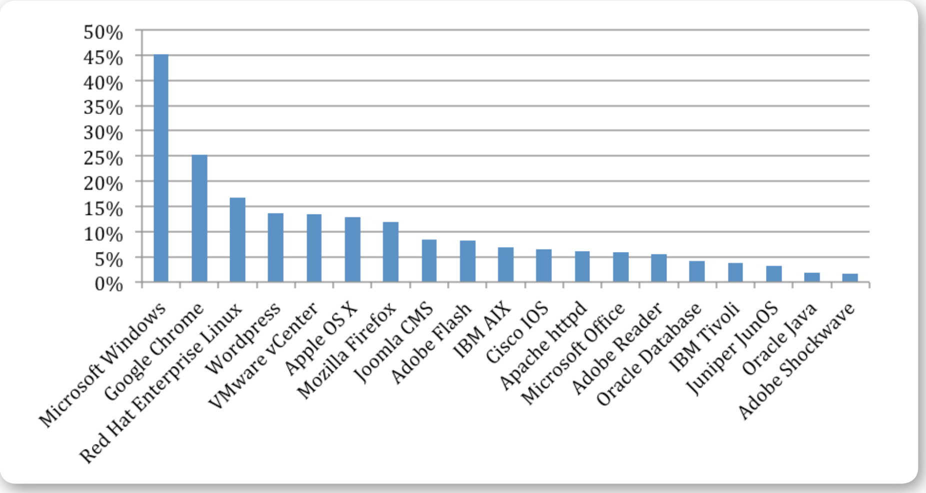

Fig. 2 Rank of platforms by patching ease

patches released for each software element in 2015. In this white paper, we are concerned mostly with security-based patches. We defined a security patch as a patch that addresses at least one known vulnerability. The results are shown in Table 1.

This very basic enterprise desktop configuration required a total of 188 security patches during 2015, or approximately 15 security patches per month. Fifteen security patches per asset per month can accumulate rapidly for organizations with a large number of assets. For example, 46 percent of our survey respondents were responsible for a number of IT endpoints ranging from 500 to 5000.

Organizations have software footprints based on business needs. Respondents were asked about their involvement with security patching for various types of software used within their organization, and these results are shown in Figure 1.

Microsoft Windows, Microsoft Office, Adobe Flash Player, Adobe Reader, Oracle Java, VMware vCenter and Google Chrome ranked the highest in terms of our respondents' patch management responsibilities. As a result, we will dig deeper into these various products throughout the remainder of this white paper in order to better understand Patch Fatigue.

Given the wide array of products that make up the modern IT ecosystem, we asked respondents about their comfort levels in terms of patch management. Particularly, we asked respondents to rank various products in terms of those that are easiest to patch and those that are hardest to patch. Figure 2 shows how respondents rank the easiest to patch platforms, and Figure 3 reveals how respondents rank the hardest. According to the results, the top five easiest platforms to patch are Microsoft Windows, Google Chrome, Red Hat Enterprise Linux, WordPress and VMware vCenter. The top five hardest platforms to patch are Oracle Database, Oracle Java, Cisco IOS, VMware vCenter and Microsoft Windows. It is interesting to see the overlap for Microsoft Windows and VMware vCenter, which made it into both top five lists. When comparing the results, we see that overall Microsoft Windows is viewed as the easiest platform to patch. Conversely, Oracle database "won" for the most difficult platform to patch.

Now that we have an understanding of how difficult various platforms are to patch, let us consider the relationship between difficulty and patch quantity. For this, we evaluated the top five platforms and calculated the total number of patches delivered for them in 2015. The results are provided in Table 2.

When coupling the data from Table 2 with the difficulty levels associated with each platform, as described by the rankings from Figures 2 and 3, one observation is immediately obvious: Patch difficulty is not a result of the number of patches per year. For example, Oracle Database had substantially fewer patches than Microsoft Windows in 2015, yet it ranked as the most difficult platform to patch, while Microsoft Windows ranked as the easiest.

Structured Patch Release Cycles

One of the more interesting patch management changes over the past decade has been the introduction of the structured patch release cycle. Microsoft introduced the world to the concept of structured patch release cycles in

October 2003 when they launched Patch Tuesday. This regular cadence allowed enterprises to plan and schedule their updates. Some companies even introduced the concept of "Patch Saturday," a day IT teams set aside two weeks after patches are released to regularly install needed updates.

A couple of years after Microsoft started with a structured cycle, Oracle joined the game, announcing in 2005 quarterly updates. In 2008, Cisco joined in by initiating biannual updates for IOS. Adobe, who has become closely entwined with Microsoft, started following Microsoft's Patch Tuesday schedule in late 2012. While Adobe doesn't strictly abide by this schedule and unscheduled updates still drop, they've done a good job of being in line with Microsoft's patch release schedule.

With structured updates comes structured information. All of the vendors listed above started preannouncing their security updates to inform customers of what was coming so that they could properly prepare for the patch before it dropped. This put enterprises IT and security teams in a much better position, as they were able to ensure they had adequate resources available to deal with the patches when they were released. While many vendors continue this cycle, Microsoft decided to discontinue the advanced notification, now delivering an unknown number of updates affecting various platforms.

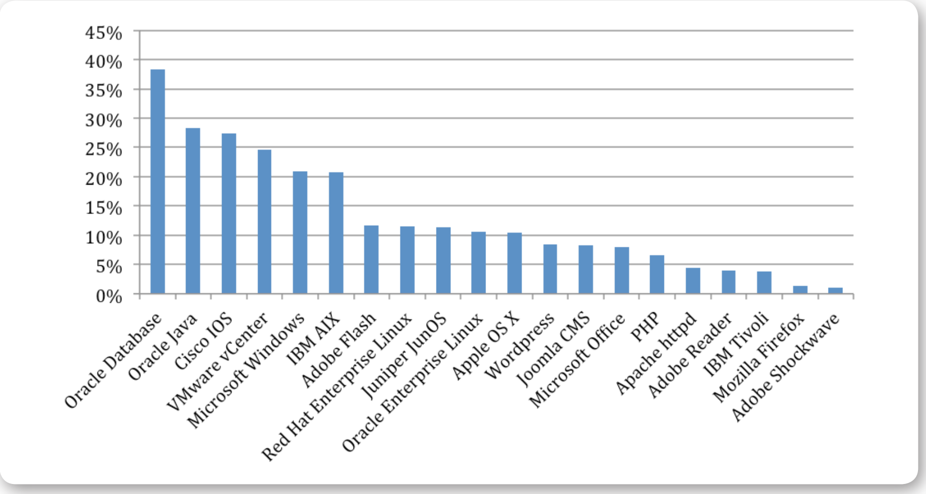

Fig. 3 Rank of platforms by patching difficulty

Software Component	Security Patches in 2015
RHEL	120
Windows	13
Oracle Database	16
Oracle Java	13
IBM AIX	4
Cisco IOS	13
Google Chrome	3
VMware vCenter	3
WordPress	3

Table 2. Security patches delivered in 2015 for the top five easiest and hardest platforms to patch

Our enterprise patch management survey looked to garner feedback from respondents on structured patch cycles and found that nearly two-thirds of organizations prefer Microsoft's monthly patch cycle over longer intervals. One of the more interesting discoveries was that one-third of organizations would prefer individual patches be released as they are available, similar to the cycle that Red Hat uses for its RHEL patches.

It should come as no surprise to readers that less than two percent of those surveyed preferred the Cisco (quarterly) and Apple (unscheduled bundle) approaches to patch releases. This should be an eye opener for vendors like Apple that don't adhere to a schedule. Cisco's extended cycle can greatly increase risk by increasing the window where a vulnerability can be exploited, increasing the attack surface. On the other hand, Apple's cycle allows for no preparation or preplanning, causing IT organizations to rush to apply unannounced updates. Both of these methods should be recognized as contributing factors to the increasing Patch Fatigue that we're seeing across enterprises.

When our survey looked at actively exploited vulnerabilities, the focus shifted. Eighty percent of those surveyed would like to see vendors test patches and then release them immediately. Unsurprisingly, fewer than one in 10 respondents advocated for vendors to maintain their regular schedule when critical fixes are needed to mitigate active attacks.

One thing is clear: Structure is greatly preferred in the enterprise world. Many vendors have strived to provide this, and it's critical that it be maintained going forward in order to ensure we limit the effects of Patch Fatigue on employees working in IT.

Shifting Trends with Microsoft

When you start to investigate Patch Fatigue, it's impossible to discuss the concept without considering some of the shifting trends affecting both vendors and enterprises. As we discussed above, numerous vendors have introduced scheduled patch drops into their process, making it easier for enterprises to plan for and manage new updates. However, it is clear that these processes are living, breathing entities that change over time. The shift to scheduled patch drops is evidence of how the process changes. By scheduling their releases, vendors allowed enterprise IT and security teams to plan accordingly. This ensured that major projects were not impacted, available resources were properly scheduled, and that potential downtime was announced. When considering these benefits, it's very easy to see how a shift in the trend can positively or negatively impact Patch Fatigue within an organization.

One of the more interesting shifting trends has been Microsoft's stance on enterprise security and the release of patches. One such example is the inclusion of Adobe Flash bundled with Internet Explorer and Edge. Flash in Windows XP proved to be a challenge, as we'll see in section Adobe Flash Player: The Battle of the Bundle, so many were surprised to see it return. Initially, the inclusion of Flash packaged with Windows lead to a single security advisory that persisted over three years. Microsoft's shift away from issuing security bulletins and instead continuously updating the same security advisory made things more challenging for Windows administrators. However, Microsoft resolved this issue as it relates to Flash in the February 2016 Patch Tuesday drop when they released a security bulletin that replaced the security advisory. Normally, you don't have this type of replacement, indicating that Microsoft realized they could improve the process and sought to resolve this pain point.

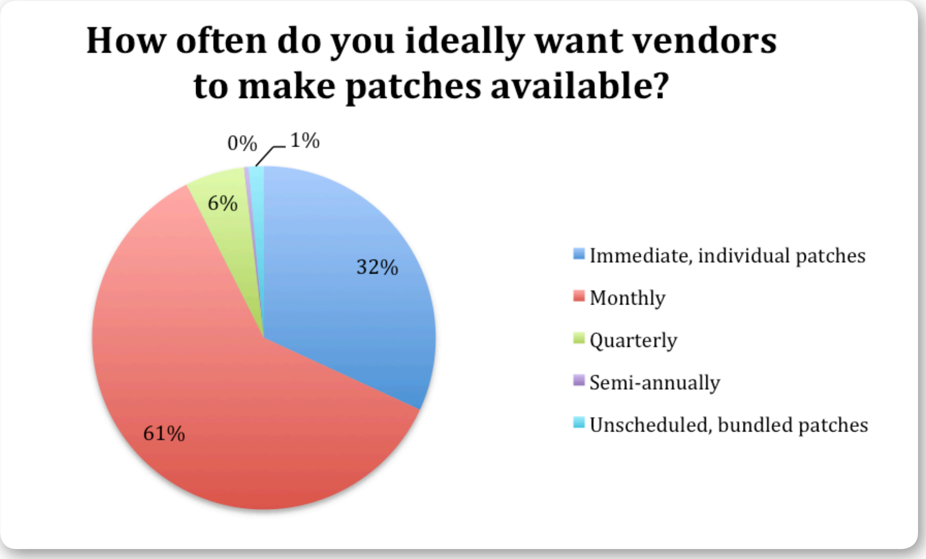

Fig. 4

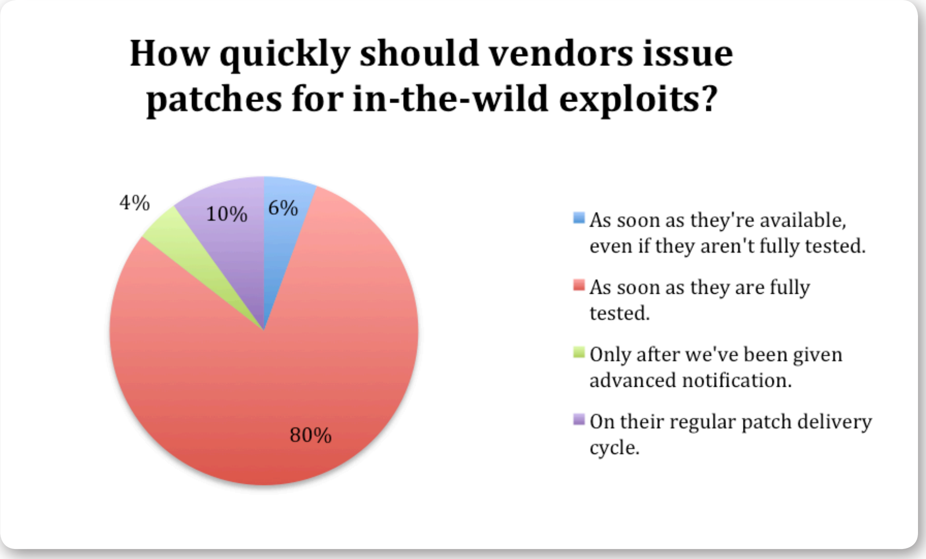

Fig. 5

Windows 10 patch releases have demonstrated a shift away from straightforward Windows patch management. Gone is a single line of security patches as used by previous versions of Windows; instead we see a shift toward multiple release branches, all with different rules for patching. The three branches include Current Branch (CB), Current Business Branch (CBB), and the Long-Term Servicing Branch (LTSB) and each requires a commitment to a different release cycle that is unlike anything Microsoft has offered before. The process is complex enough that Microsoft has published a multi-page document5 to help explain the process.

The new line of servicing options is confusing and reminiscent of Cisco's versioning. As we're discussing Patch Fatigue, it's probably worth noting that only one-third of Cisco IOS administrators are able to decipher which updates to install without contacting Cisco's technical support team. Windows 10 appears to be heading down a similar path, with only one-third of those surveyed feeling that Windows 10 has improved patch management. This number is surprisingly similar to the number of individuals who can decipher Cisco IOS updates. These results are even more telling when you consider that 41 percent of those surveyed felt that Windows 10 was making enterprise patch management more difficult. Microsoft's decision to combine servicing options with a single cumulative update that Microsoft releases for Windows 10, which allows for no control over the individual updates installed may explain why this number is so high.

What to do About Java

Java was introduced to the world in 1995. At that time, the Internet, along with the World Wide Web, was booming, and the Web was largely built with static HTML pages. Java introduced the ability to add dynamics to the Web via its graphical capabilities with applets. This single capability drove very wide adoption of the Java language, and played a huge role in its success. In a world hungry to build distributed networked applications using the Web, Java quickly dominated the scene. However, there was one other feature that also played a big role: security. Upon its debut, Java was advertised as a highly secure language. Security was especially important when building applications for the Web, but we know that there is no such thing as absolute security and, over time, the number of insecurities and weaknesses discovered in Java began to increase.

Java originally debuted as a secure platform because of several features. One was that the language was built with mechanisms capable of enforcing runtime constraints such as preventing buffer overflows. Java checks the bounds of buffers and will prevent access to any memory beyond those bounds. Java also contains a security management mechanism that uses a sandbox to isolate untrusted code from the overall system. However, all of these systems are built with software, and all software contains flaws that can lead to security vulnerabilities. Figure 6 shows the approximate count of core Java vulnerabilities that have been discovered since 2000.

Between 2000 and 2005, Java experienced linear growth in the number of vulnerabilities being discovered. From 2005 until 2008, that growth followed an exponential trend, and since 2008 the trend has been stochastic. We can see a peak in 2013, which represents 193 distinct vulnerabilities. The continual discovery of new Java vulnerabilities means that outdated versions of Java cannot be considered secure. The need to constantly manage these installations appeared to be a pain point among survey respondents.

It turns out that Java patches introduce Patch Fatigue-inducing challenges for IT and patch management teams. The decoupled aspect of managing applications written with Java separately from the Java platform (e.g. Java Runtime Environment (JRE)) is one of these challenges. In particular, IT departments and patch management teams often need to wait for developers to update their Java applications before they are able to apply security patches for the Java platform. This is a common problem connected with legacy applications, and this timing delay places organizations that depend on Java-based applications at risk. This scenario is of great concern for organizations—86 percent of respondents stated that they are concerned about the security of Java-based applications. When asked for more details about their concerns, the sheer number of reported Java vulnerabilities ranked as the highest concern, followed by the fact that the Oracle Java updater does not remove older, more vulnerable versions6. When asked to provide specific concerns related to Java, respondents clearly signaled that issues with application compatibility and the need to run older versions of Java for legacy applications were particularly troubling. As a result, 27 percent of respondents say they are to be phasing out Java-based applications within their IT environments.

Adobe Flash Player: The Battle of the Bundle

Adobe Flash Player is another product that is often on the minds of IT departments and patch management teams. The continuous discovery of new Adobe Flash vulnerabilities is definitely a key issue. Figure 7 shows the number of known vulnerabilities that have been discovered in Adobe Flash since 2000.

Another key issue is the consistent appearance of exploits for Adobe Flash vulnerabilities within exploit kits. There was a time when Java was a consistent exploit kit target but Adobe Flash appears to be the favorite today. We analyzed the vulnerabilities included in the Angler exploit kit dating back to 2013 and found that 76 percent of the exploits targeted Adobe Flash. The remaining 24 percent targeted predominantly Java, alongside Internet Explorer and Microsoft Silverlight.

The above data clearly indicates why administrators are worried about new vulnerabilities in Adobe Flash. Unfortunately, managing Adobe Flash security patches is not easy because this software is now bundled with other products. Bundled software can raise the level of difficulty for administrators who need to understand which parts of the application need to be updated and which vendor is responsible for the updates. Adobe Flash has seen its share of patch difficulty over the years due to this bundling scenario.

One particular issue that highlights the difficulty caused by bundled software becomes evident when determining the ownership of security updates. A great example of this problem occurred between Microsoft and Adobe back in 2010 when KB9792677 was released. Microsoft had bundled Adobe Flash

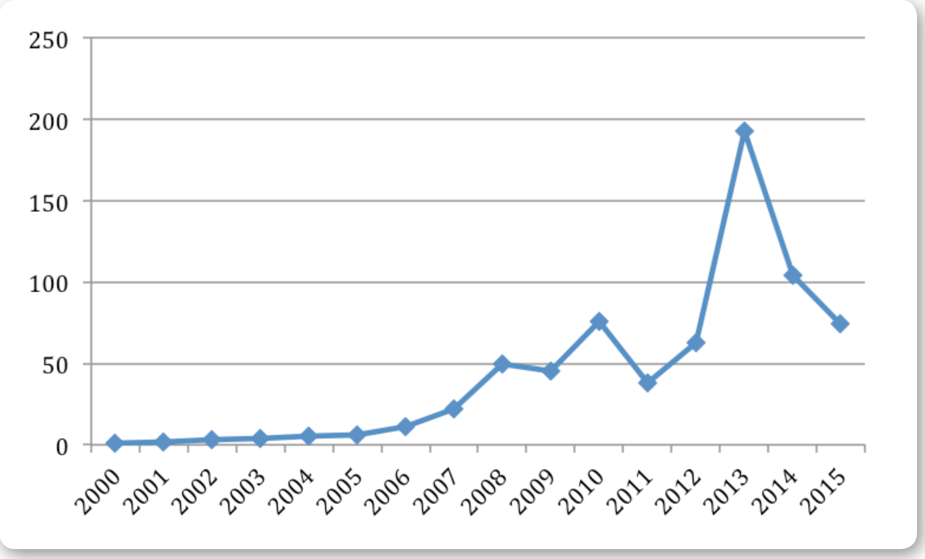

Fig. 6 Java vulnerabilities over time

Player 6 with Windows XP, but did not ship security updates as Adobe issued patches. After multiple vulnerabilities surfaced in this version of Flash, Microsoft released the security advisory warning users to uninstall Adobe Flash 6 and upgrade to a newer version. Once Microsoft stopped bundling Flash, the boundaries became clear: users were responsible for the installation of Flash along with its patch management via one single source, Adobe. Unfortunately, it didn't take long for the Flash bundling situation to occur again with multiple vendors. Google began bundling Adobe Flash Player within the Chrome browser, and then Microsoft began bundling it with Internet Explorer. Administrators were placed in a difficult situation where attributing Adobe Flash vulnerabilities became problematic. They were back into a patch management scenario where Flash vulnerabilities might need to be patched by either the browser's vendor or Adobe, or in some cases, both. Microsoft has recently made an effort to ease this patch management pain. Until February 2016, Microsoft maintained a single security advisory that detailed Adobe Flash vulnerabilities related to bundled installations for Microsoft products. However, MS16-022 marked the first security bulletin to directly address bundled versions of Adobe Flash Player in Microsoft products.

Obviously, software vendors feel that bundling software has its benefits. However, what do IT professionals think of this patch management paradigm? Eighty-six percent of our survey respondents stated that products with multiple distribution methods (standalone and bundled in other products) such as Adobe Flash create challenges in understanding the impact of security patches.

CONTRIBUTING FACTORS: PATCH PRIORITIZATION AND TIMING

Patch management plays a critical role in strengthening the security posture of most organizations. Fifty-nine percent of our respondents claimed that security-related patches take priority over non-security related patches, but this is not the only set of priorities. Figure 8 shows how organizations prioritize patches based on various categories. The data shows that issues such as known attacks, public exploit availability and reboot requirements play significant roles when prioritizing security patches.

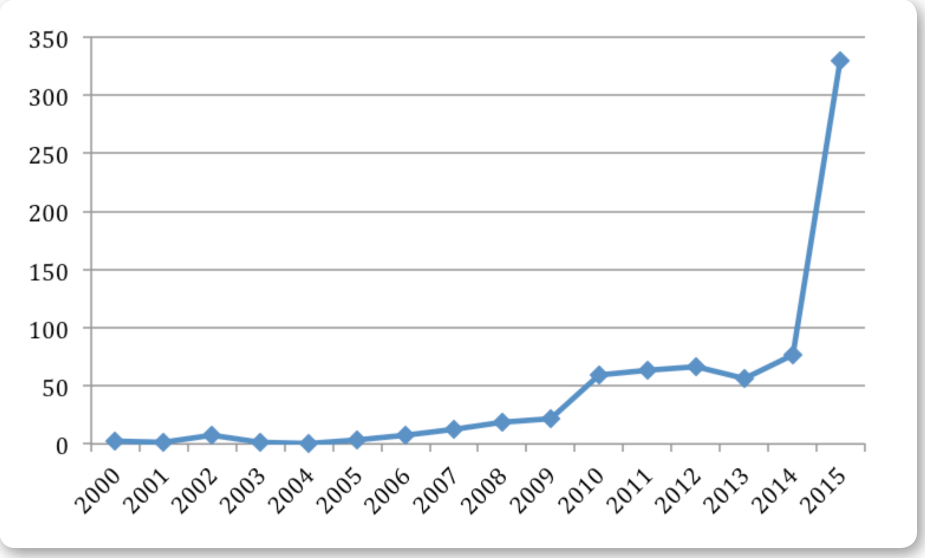

Fig. 7 Adobe Flash vulnerabilities over time

It is interesting that the "Reboot Required" category ranked third in importance when prioritizing patches. However, it makes sense when you consider that server footprints are very large in modern IT infrastructures. From our survey, we found that 90 percent of respondents had responsibility for patching server endpoints. Another noteworthy point is related to CVSS scoring. CVSS is an open standard used for assessing the severity of known vulnerabilities, and many security vendors and various industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS), use it. PCI, which requires that all vulnerabilities with a CVSS score of 4.0 or higher be patched, is a retail industry standard that's applicable to all companies processing credit card transactions. Respondents were asked about their organizations' adherence to industry standards. Figure 9 shows these results.

Even though 39 percent of respondents must adhere to PCI DSS standards, CVSS ranks next to last in terms of how administrators prioritize patches.

Timing and prioritization are important aspects of patch management. Figure 8 shows that security patches related to vulnerabilities with known attacks or with publicly available exploits are most important to those involved with patch management. When exploits surface, vendors should respond accordingly by providing patches for the associated vulnerabilities. However, our survey indicated that when it comes to patches released for vulnerabilities with in-the-wild exploits, IT teams consider prudence to be more important than urgency. Survey respondents strongly preferred thoroughly tested patches, and we found that 80 percent of the respondents wanted to receive security patches for in-the-wild exploits as soon as the patch was developed but only after it was fully tested. Comparatively, only six percent of those surveyed wanted the patch as soon as it was available regardless of testing, and 10 percent were simply satisfied with delivery during the vendor's normal patch delivery cycle.

The survey clearly indicated that thorough testing of security patches was desirable, yet we observed a small discrepancy between the viewpoints of executives and individual contributors. While executives tend to be more concerned with risks associated with unpatched vulnerabilities that have known exploits, individual contributors tend to be more concerned with risks associated with the deployment of untested security patches. When asked if a security patch for an in-the-wild exploit should be delivered as soon as it is available even without being fully tested, 11 percent of executives agreed to that approach versus four percent of individual contributors. This may be due to a difference in responsibilities. While executives are responsible for higher-level concerns (such as the cost of a data breach), individual contributors are concerned about day-to-day operations and better recognize the risks associated with deploying untested patches on critical infrastructure.

The constant influx of patches across the many different types of IT assets means that time becomes a critical factor. Respondents were asked about the amount of time considered acceptable between the release of a security patch and its installation in their environments. They were also asked how long it takes to deploy security patches in their environments. The results are shown in Figure 10.

As the data suggests, organizations are currently on track with the amount of time deemed acceptable and the actual amount of time needed to deploy security patches. The majority of respondents feel that security patches should be tested and deployed within seven days of release. Together, 93 percent of respondents take no longer than one month to deploy security patches. This participant perception doesn't seem to mesh with the reports published by other vendors and researchers. A report8 published by NopSec indicates that the financial and education sectors take an average of 176 days to remediate a vulnerability.

One key component affecting the amount of time needed to deploy patches is testing. Respondents were asked if they tested patches before deployment, and 47 percent said they did for desktops and 55 percent for servers. Figure 11 shows the amount of time taken by our respondents to test patches.

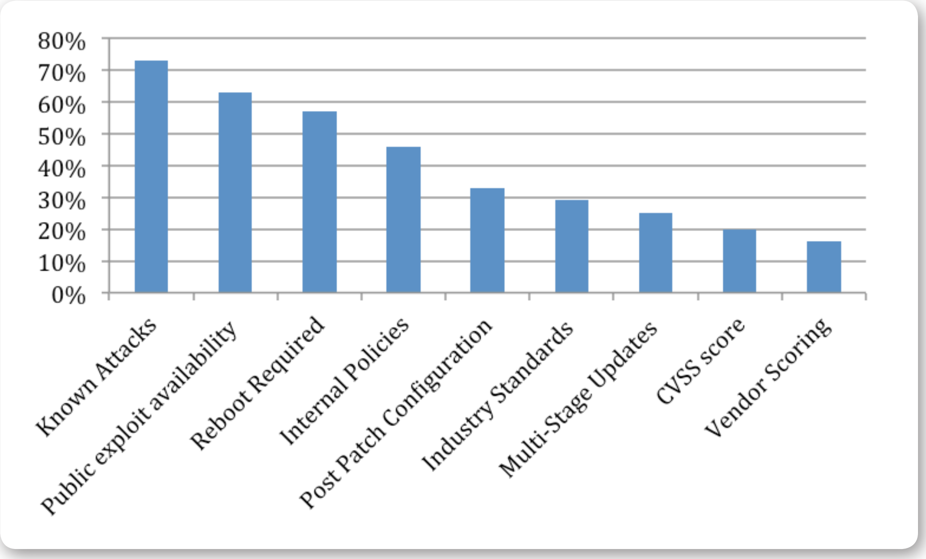

Fig. 8 Patch prioritization categories

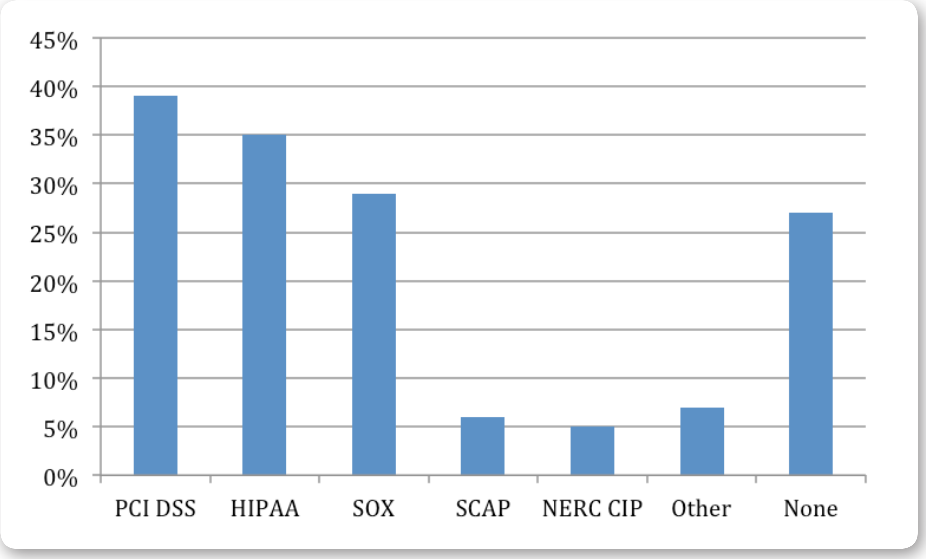

Fig. 9 Participant involvement with industry standards

As Figure 11 reveals, respondents tend to spend less time testing patches for desktops and slightly more time testing patches for servers. When considering the impact that a faulty patch can have on IT environments, it is obvious that administrators want more time to test server patches. Although the vast majority of respondents are comfortable with deploying patches within seven days, we observed a small discrepancy between executives and individual contributors in terms of immediate patch deployment requirements. Of those respondents who feel that security patches should be deployed immediately, 12 percent were executives, and only five percent were individual contributors. This shows a clear distinction between motivations of executives versus administrators—executives are more concerned about the potential impact of a security event, and administrators are more concerned with the potential impact of deploying a faulty patch since this can impact availability and reliability of critical business systems.

Contributing Factors: Recognizing Vulnerabilities

When discussing security-related updates, it's important to remember the goal of patches: remediating a vulnerability rather than fixing a functional bug or adding new features. For those on the security side, that may seem like a straightforward concept, but there's often a disconnect between security and operations teams on exactly what needs to be done. This disconnect is one of the major contributing factors of Patch Fatigue.

Figure 12a shows the responses to the survey question, "Does your IT staff have difficulties understanding the difference between applying a patch and resolving a vulnerability?" If the answer is yes, then you can represent the data as illustrated in Figure 12b.

A great example in the difficulty presented when attempting to understand the difference between applying a patch and resolving a vulnerability is MS15-1249, the December 2015 Internet Explorer cumulative update that resolved 30 CVEs. In most cases, Windows admins expect to install the update and be done, but one CVE in this bulletin contained a special note.

The bulletin laid out details on how to take the additional steps required to truly mitigate the vulnerability. In many cases, this additional step was not taken, leaving systems in a vulnerable state. This meant that companies that verify with Vulnerability Management products rather than Patch Management products left their internal teams with the additional overhead of verifying if systems were truly vulnerable. This may or may not lead to external requests to vendors, consultants, or others.

In order to better recognize individual vulnerabilities, administrators should completely review vendor security bulletins. There are varying degrees of useful information in the bulletins provided by the vendors, which we'll investigate in an upcoming section. However, understanding bulletins is important to properly resolve vulnerabilities via patch application.

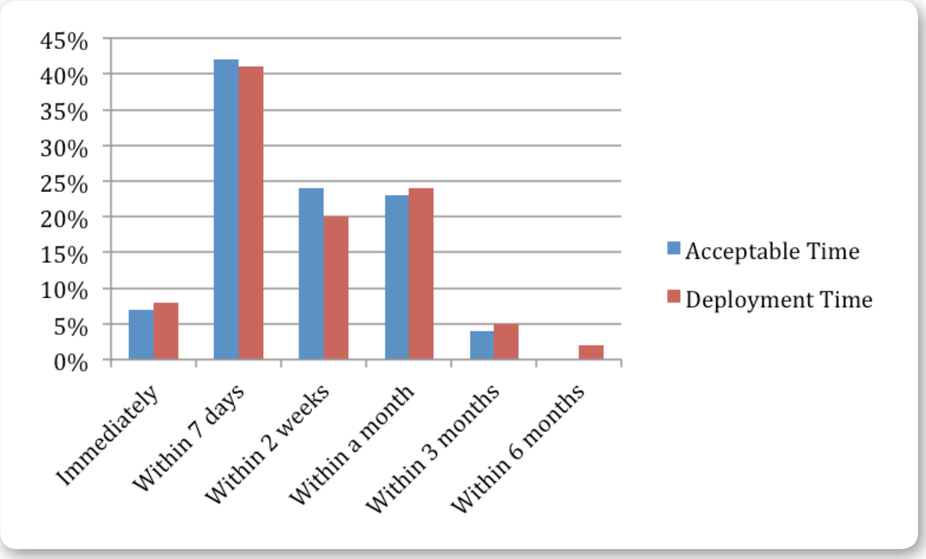

Fig. 10 Timing aspects of security patches

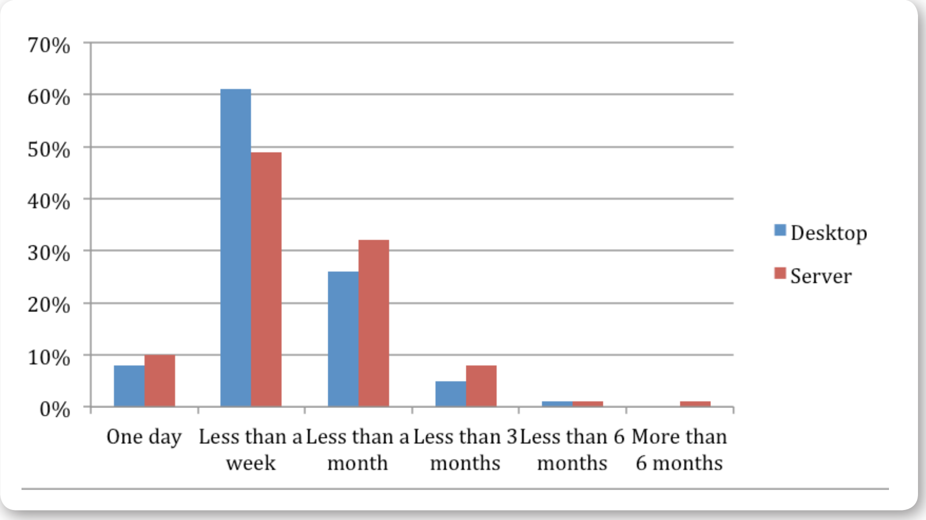

Fig. 11 Patch test times

Take a look at the team around you. According to the survey results, half of your team do not understand if a vulnerability is resolved after applying a patch. Think about the extra cycles caused by that lack of understanding, the additional work done by individuals within your team, and by the vendors that support you. This is clearly a widespread issue within the industry, and it's easier to understand how this contributes to the overburdening of teams responsible for enterprise patch management.

In the security world we often talk about end-user education as the key to good security hygiene, but it may be that within patch management, education is a missing piece. Many post-secondary institutions talk about cryptography whenever the word security is mentioned, while others are starting to bring in courses focused on exploit development. These lessons don't seem to cross paths with operations-related teachings.

Security conferences and local meetups present the perfect place to provide this type of education. Unfortunately, many of the events are focused on introducing cutting-edge or "cool" concepts rather than solidifying core knowledge.

It's the responsibility of the community to create a solid forum for sharing this knowledge and educating others.

Internally, companies should look to create and promote knowledge sharing. If half of your team understands what is going on, they should be spreading that knowledge to the other half. Brown bag lunches are a great way to start a program like this, and those can be further improved if the company pays for lunch. This expense is a relatively small investment to help reduce the Patch Fatigue that the knowledge gap contributes to. Trainers can be brought in to provide additional knowledge transfer, as well as a recognized expert to answer questions. There are plenty of training organizations available, and many vendors are able to provide indirect guidance on this subject during product training.

Contributing Factors: Security Bulletins

It's practically impossible to talk about security patching and Patch Fatigue without considering the role that vendor bulletins play. When you're patching a system, bulletins tell you what to patch, how to patch it, and which vulnerabilities are resolved. These should be a critical source of information for all administrators, but many find them to be more of a hindrance than help.

We looked at major vendors and asked survey respondents to classify their top vendors for both best and worst security bulletins. Microsoft provides the best content (see Figure 13), but it simultaneously ranks near the top of the list for worst information providers. Microsoft likely appears as the best information provider because it is among a short list of vendors that clearly call out post-configuration steps, provide details on the nature of the vulnerability resolved, and provide work-arounds (when available) to those that can't be patched immediately.

When looking at the worst information providers, some respondents providedadditional commentary. While only one individual expressed dissatisfaction with Microsoft bulletin quality, several respondents wanted to call out Oracle. This is unsurprising since an Oracle bulletin can contain several hundred links to patches—a number that appears to be unrivalled by any other vendor. This method of dumping updates without adequate information clearly doesn't sit well with survey respondents. A proper security bulletin would remove this concern, which is potentially harming Oracle's reputation and unnecessarily increasing the workload of their customers.

The sheer quantity of security patches consumes an enormous amount of an enterprise's resources in part because IT teams are often unsure of when to apply specific patches. Figure 14 shows that only 34 percent of enterprise patch management teams are "always confident" that they understand which patches apply to which systems. This number is disturbingly low, and is also a clear indicator that the remaining 66 percent end up doing additional work.

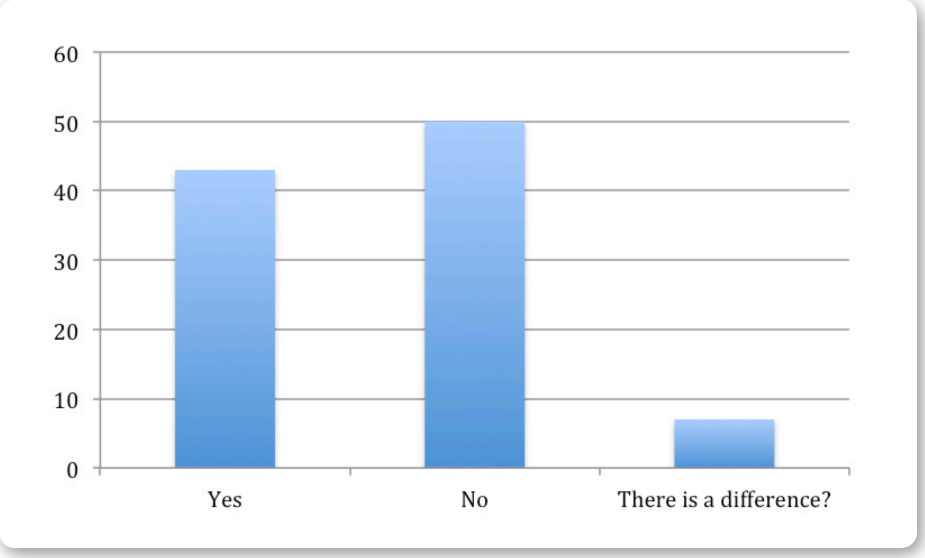

Fig. 12a Does your IT staff have difficulty understanding the difference between applying a patch and resolving a vulnerability?

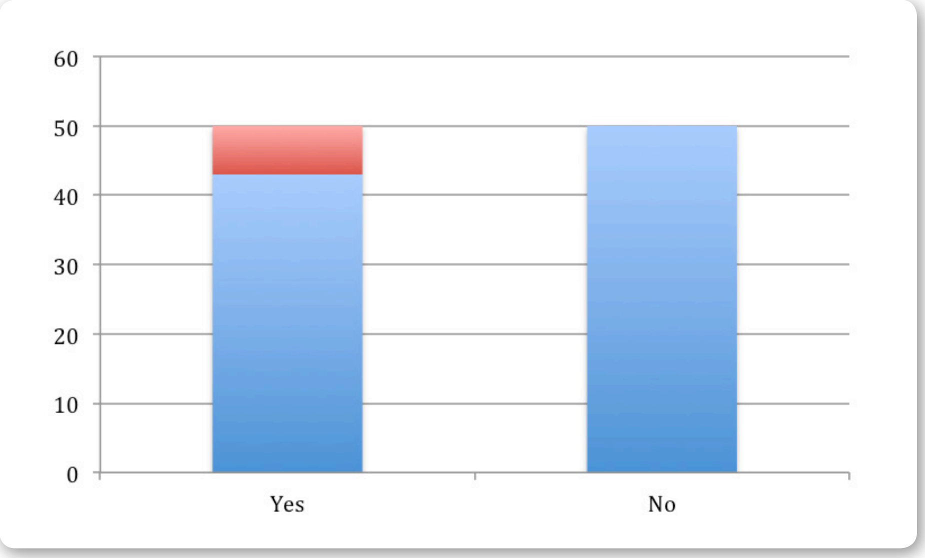

Fig. 12b Does your IT staff have difficulty understanding the difference between applying a patch and resolving a vulnerability?

> Important: Your system is not protected from this ASLR Bypass unless you install the applicable updates and then enable the User32 Exception Handler Hardening Feature
>
> — *CVE-2015-6161*

This additional work could include trial and error patch installations, phone calls and tickets to vendors, and internal meetings to discuss patch deployment. All of these additional tasks add to patch deployment times and increase the teams collective Patch Fatigue.

To further investigate this issue, we looked deeper into Cisco patches. Conference presentations and entire books have been published on the complexity of the Cisco release model. Their bulletins with lists of affected software were so complex that the lists were removed and a tool was written that now allows you to enter your software version to determine if you are affected.

When you break it down, nearly two-thirds of administrators require outside assistance to update their Cisco IOS devices, which slows down the patch cycle and increases the burden on others.

The data makes it clear that one vendor stands out with more than four positive responses for every negative: VMware stands above every other vendor in the eyes of those surveyed. A quick look at a VMware Security Advisory (VMSA) reveals why. They are clearly organized without information overload, and communicate sufficient detail quite well. Within a few minutes of reviewing these bulletins, we were able to understand what was fixed, identify the products that we were running, and found the fixes that should be applied. This is a major improvement over the bulletins of the other vendors we reviewed.

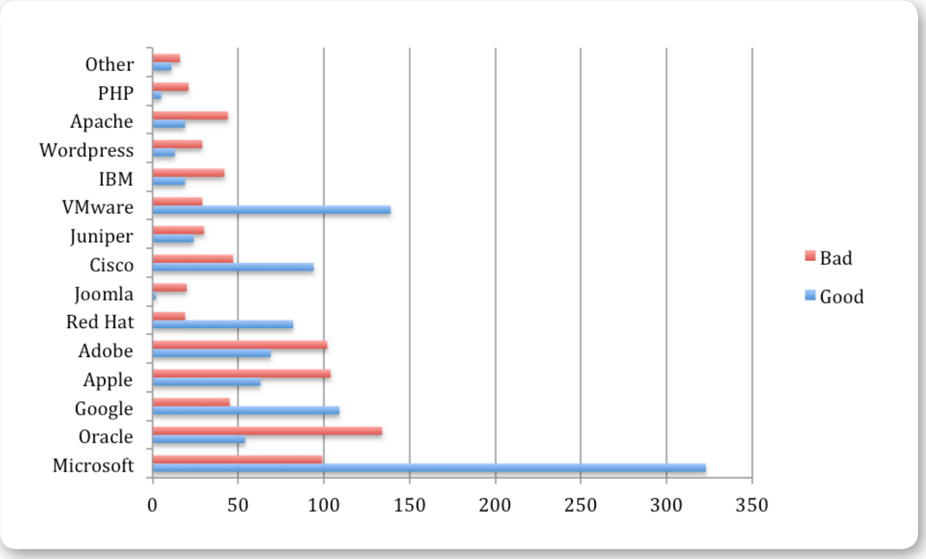

Fig. 13

While many vendors have started to move to CVRF and OVAL for machine-readable bulletin content, very few have standardized the human-readable web interfaces. In fact, even though patch volumes and complexity have increased, over the years many vendors have decreased the information they make available to their users. This makes it harder for administrators and security teams to tell what an update is doing, if it is resolving specific issues that concern you, and makes it difficult to identify which updates you need to apply. These communication failures are all major contributors to the build-up of Patch Fatigue within an organization.

In this case, the majority of the onus is on the vendors. Every vendor needs to commit to making their security bulletins and all patch documentation easier to read and understand. Standardizing human-readable content is clearly an important step in improving our patching ecosystem—and thereby reducing enterprise Patch Fatigue.

That doesn't mean that administrators and operations teams are off the hook. Investments in training and education can go a long way in improving the ability of your team to understand security bulletins. If your organization is lucky enough to have an employee in the two percent of Cisco administrators who fully understands bulletins, have them cross-train the rest of the team. If not, find someone and bring them in-house to perform training. While it would be nice to wait for vendors to delivery better documentation, there are definitely steps that can be taken within the enterprise to alleviate Patch Fatigue and decrease the overall burden on security and operations teams.

Patch Management vs. Vulnerability Management

When evaluating enterprise patch management programs the prevalence of patch management versus vulnerability management technologies is an interesting factor. The two terms are often used interchangeably and many would be hard-pressed to explain the difference. Before we investigate the applicability of both systems to the enterprise patch management program, let's discuss the unique aspects of these tools.

Patch management usually acts on one of two levels, depending on the functionality of the product involved. At the highest level, it looks at vendor bulletins, but these products tend to be the least accurate offering as vendors seldom release bulletins with a 1:1 mapping to patches. Higher-end patch management software looks at the individual patches, often rolling them up to the bulletin level. This approach more accurately tracks the deployment of patches across the enterprise.

On the other hand, vulnerability management breaks patches and bulletins down to the individual vulnerabilities, often using CVE as the standard identifier. One common misconception is that vulnerability management requires the exploitation of vulnerabilities. In reality, the concepts applied within vulnerability management are similar—if not identical—to patch management. This includes checking for indicators that a specific patch has been applied. Where vulnerability management differs from patch management is in checking for post-patch application steps that may be required.

A proper enterprise patch management program should utilize both vulnerability and patch management tools to ensure a holistic solution. Using only one of the tools can often leave you without enough information to ascertain your true security posture, and while 87 percent of organizations surveyed use patch management software, only 43 percent understand the difference between applying a patch and resolving a vulnerability. These numbers indicate that a mature vulnerability management program could help reduce Patch Fatigue.

One of the better examples of the limitations of patch management tools with minimal functionality is Microsoft Baseline Security Analyzer (MBSA). This tool has the potential to lead IT organizations astray by indicating that systems were fully patched. MBSA fails to report issues in software that is no longer supported (such as older versions of the .NET Framework and the antiquated Microsoft Java). This causes confusion among organizations with mature vulnerability management programs because they are led to believe there are issues with their vulnerability management products, but in reality the issue is caused by discrepancies in the way unsupported software products are reported.

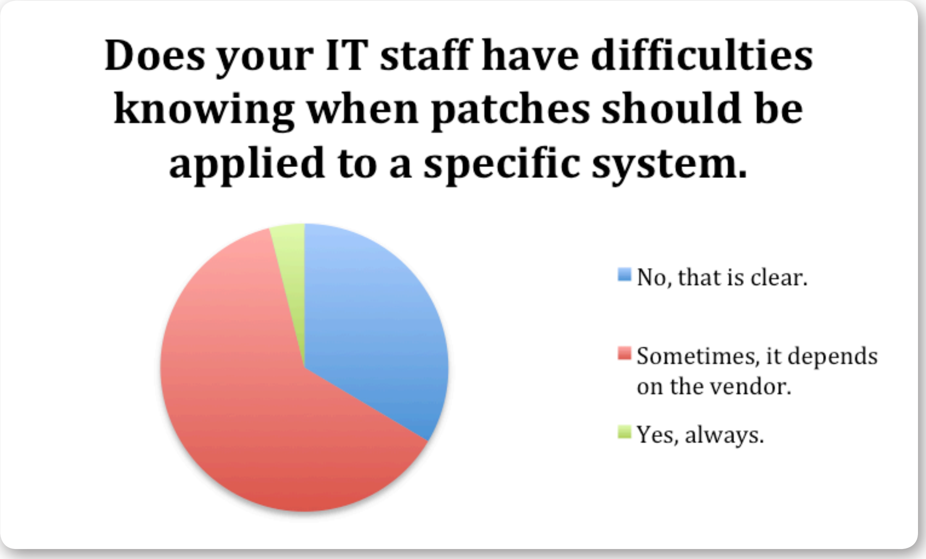

Fig. 14

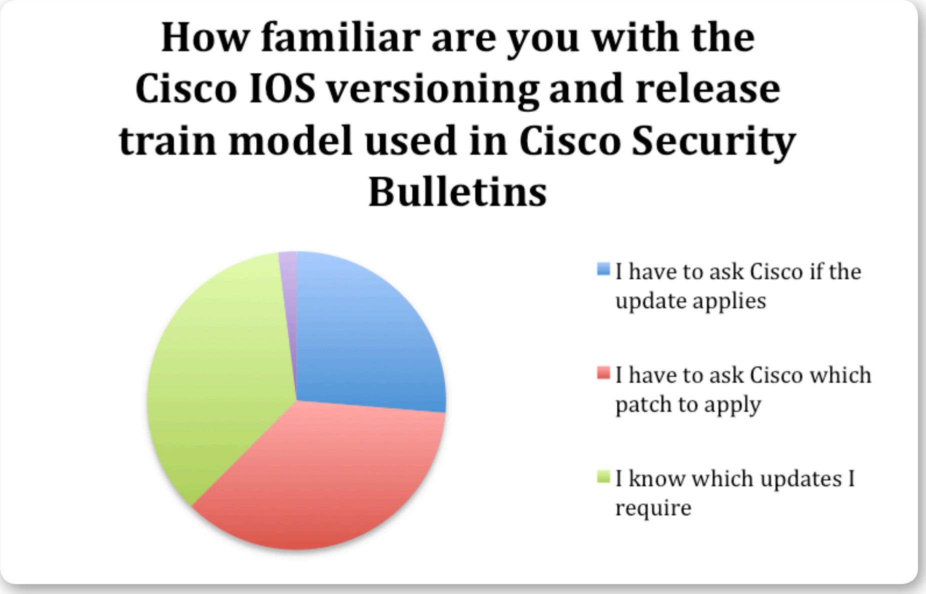

Fig. 15

A more recent example of why organizations need both patch and vulnerability management software is MS15-124, the December 2015 Internet Explorer security bulletin that we discussed earlier. While patch management software may indicate whether or not the patches associated with MS15-124 are installed, the reporting generally stops there; the reports don't indicate if the additional step required to resolve one of the vulnerabilities contained within the bulletin has been taken. This is where the difference between vulnerability management and patch management is further highlighted. As noted in the section Contributing Factors: Recognizing Vulnerabilities, one of the vulnerabilities, CVE-2015-6161, requires users enable a registry setting in order to enable the mitigation installed by the patch. Without this change, the system remains vulnerable.

The flip side of this conversation is that while vulnerability management is great at finding the one-off conditions that patch management misses, it doesn't necessarily show the easiest path to resolution. It's much easier to have one line item that says, "Install patch x from

MS15-124," than to have 30 line items for each CVE identified within MS15-124. This is why patch management should be used hand-in-hand with vulnerability management to ensure adequate security and reduce Patch Fatigue.

Combating Patch Fatigue with a Mature Patch Management Program

One of the more surprising statistics from this survey was that nearly one-fifth of those surveyed don't use patch management software (Figure 16). An important part of combating Patch Fatigue is a mature patch management program. While other contributing factors to Patch Fatigue require vendor changes or extensive training, this specific contributing factor can be resolved with changes to your internal patch management process.

The first step in this process is the proper use of software, which is something we've already discussed. Vulnerability and patch management solutions should be used together to get a picture of the enterprise security posture, including both current patch levels and known risks. When either of these tools is missing, additional responsibility is placed on individuals instead of technology. Without these tools, individuals must be aware of every asset and every application installed on every asset. As mentioned in the section Setting the Stage, a typical enterprise workstation could require nearly 200 patches annually. Expecting any employee to manually track and manage this is simply unfeasible, and would add additional stress that those working in security and operations don't need.

Moreover, as we discussed above, scheduling and testing are important factors for many enterprises in the deployment of patches. While many enterprises have clear policies around this, which is a sure sign of a mature patch management program, some don't. Setting up schedules, assigning responsibilities and defining roles are easy steps to take in combating Patch Fatigue. It's much easier for an administrator to plan for server downtime and patch installation if they know that patches are installed on the third Saturday of every month, as opposed to unscheduled events.

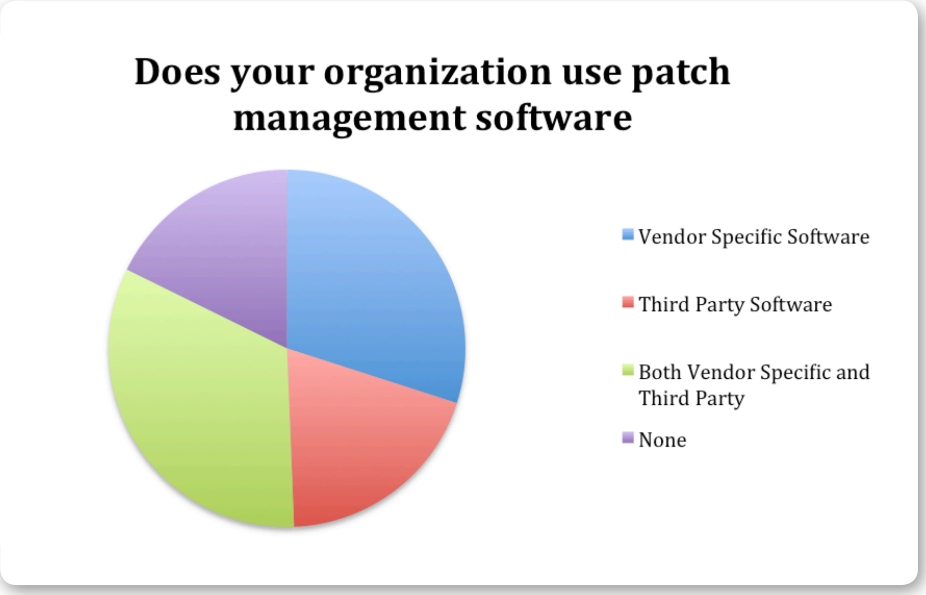

Fig. 16

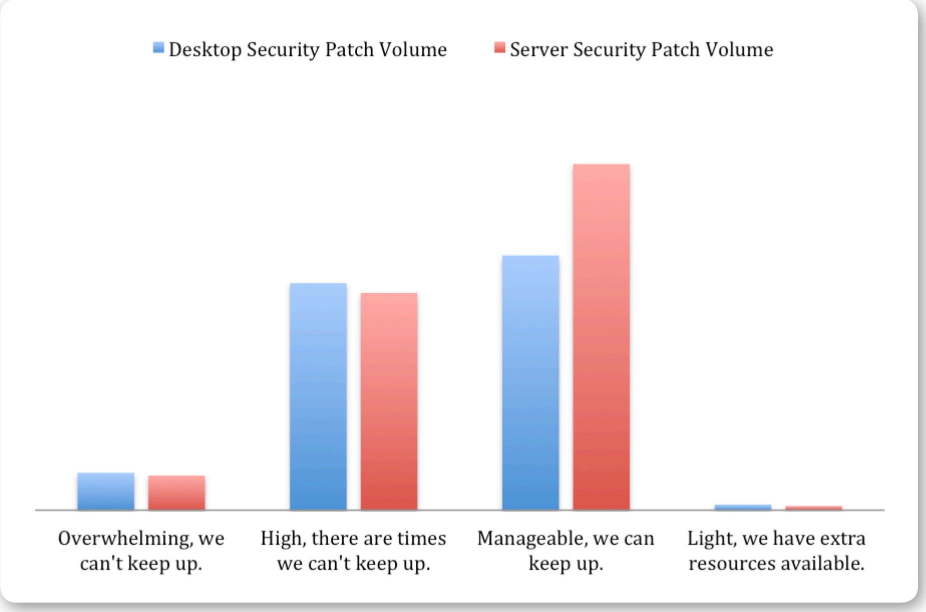

Fig. 17

Consider your plan for unexpected issues. If a patch installation fails or takes a system offline, what is your recovery plan? It's not uncommon for vendors to release bad patches that produce completely unexpected results. A recent Windows 10 update broke Citrix functionality, which was a potential nightmare for enterprises unaware of this negative interaction. This is why testing is so important and why back-up systems for mission-critical roles are a great way to reduce the stress an organization feels when deploying an update.

One of the major contributing factors to Patch Fatigue is the lack of adequate headcount. Staffing to appropriate levels is important. Do employees have time to review bulletins? Are they rushed when they deploy patches? Do they have time to understand and apply post-installation steps or to make sure they understand changes before deploying an update? These are important questions for management to ask. If your employees suffer from Patch Fatigue, employee morale will drop, your enterprise security posture will be negatively impacted, and the potential for downtime will increase.

If you feel that your enterprise is "doing fine," consider Figure 17, which demonstrates that while more than half of enterprises are managing the volume of patches, a substantial number are not.

Ultimately, the first step in resolving Patch Fatigue is identifying it, so sitting down with your team and identifying potential points of failure and stress is beneficial to any discussion. Once you start to resolve the points identified above, you're on your way to a more mature enterprise patch management program, which will subsequently improve your security posture.

In conclusion, while we've thrown a lot of numbers and statistics at you with this paper, it's important to remember the end goal. Patch Fatigue is very real for many organizations, and resolving it will lead to happier, more productive employees and, ultimately, more secure environments. Security should be at the top of every company's priorities given today's threat landscape and all improvements, especially low-hanging fruit like this, should be seen as positive gains. So plan that first meeting and figure out if Patch Fatigue is affecting your team today.

[1] http://www-03.ibm.com/security/data-breach/

[2] http://www.workforce.com/articles/today-s-workforce-pressed-and-stressed

[3] http://www.webmd.com/balance/stress-management/features/10-fixable-stress-related-health-problems

[4] http://www.workforce.com/articles/20310-two-years-later-still-stressed-and-pressed

[5] https://technet.microsoft.com/en-us/library/mt598226(v=vs.85).aspx

[6] https://www.ftc.gov/news-events/press-releases/2015/12/oracle-agrees-settle-ftc-charges-it-deceived-consumers-about-java

[7] https://technet.microsoft.com/en-us/library/security/979267.aspx

[8] http://info.nopsec.com/2015StateofVulnerabilityRiskManagement_ThinkLikeaHacker.html

[9] https://technet.microsoft.com/en-us/library/security/ms15-124.aspx

Study Demographics

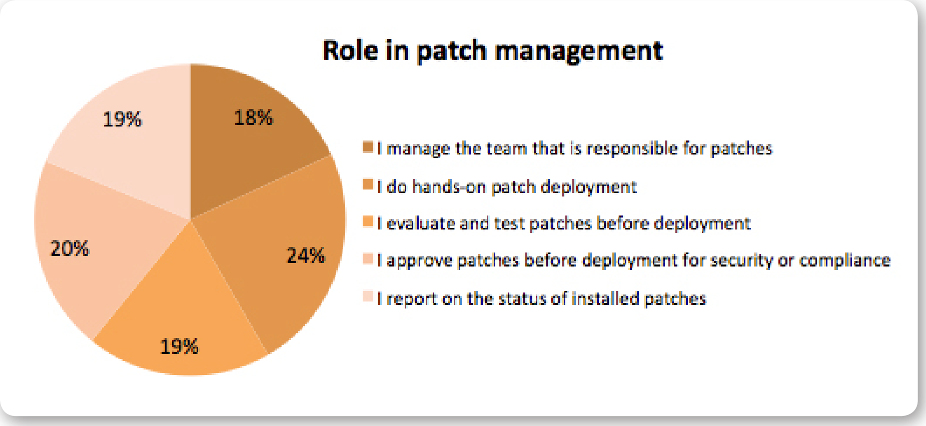

Fig. 18

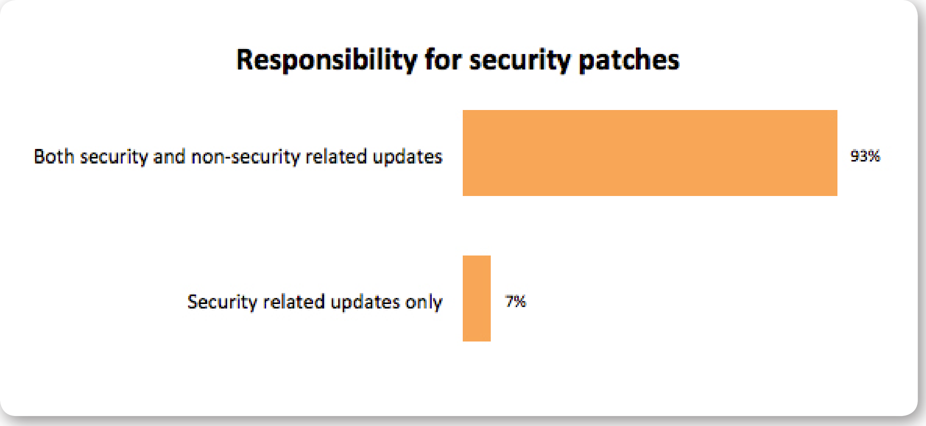

Fig. 19

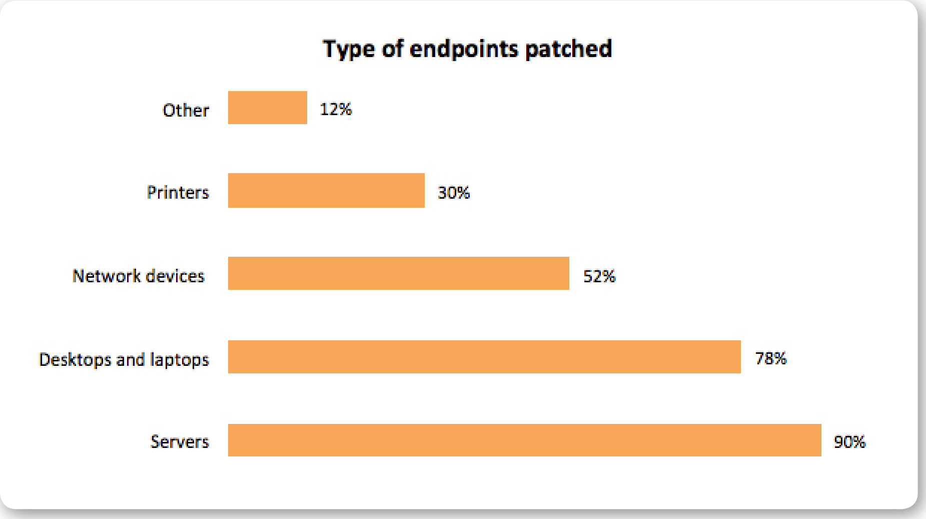

Fig. 20

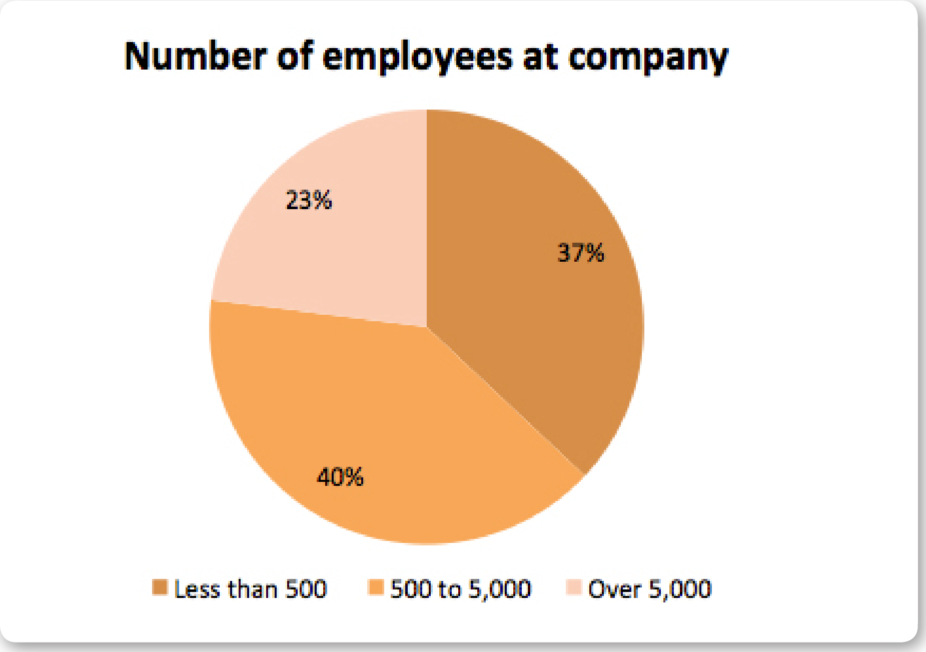
Number of employees at company
23%
37%
40%
Less than 500
500 to 5,000
Over 5,000

Fig. 21

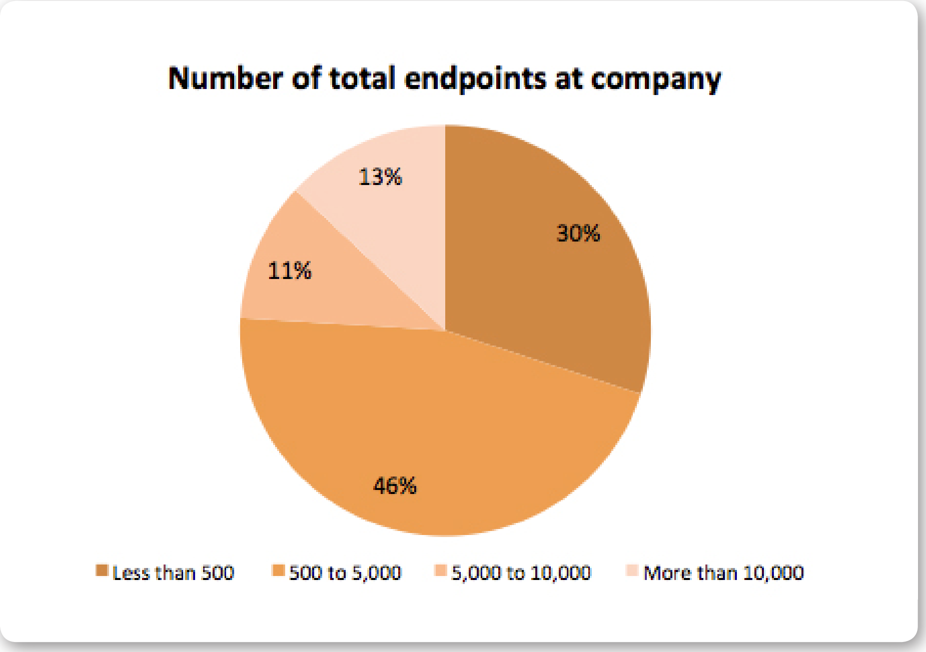
Number of total endpoints at company
13%
30%
11%
46%
Less than 500
500 to 5,000
5,000 to 10,000
More than 10,000

Fig. 22

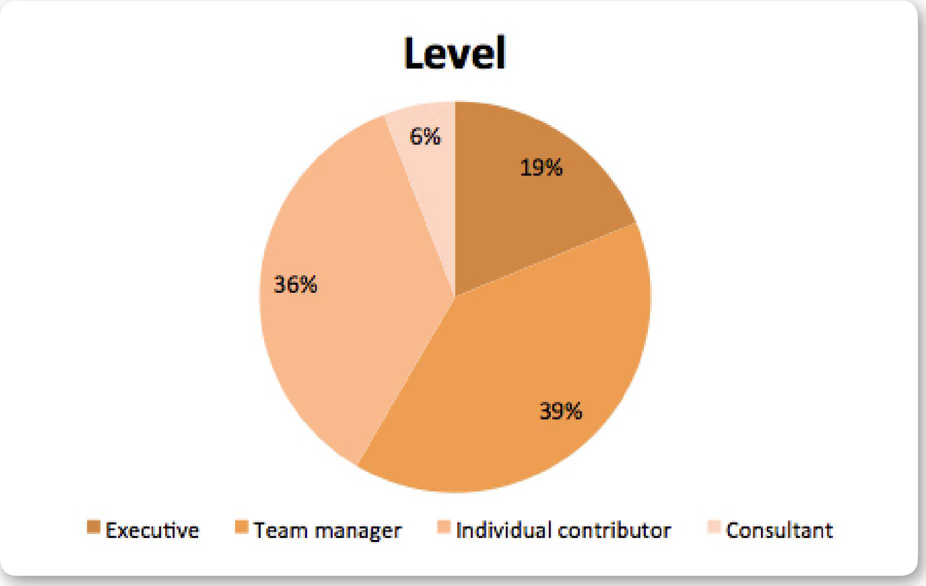
Level
19%
39%
36%
6%
Executive
Team manager
Individual contributor
Consultant

Fig. 23

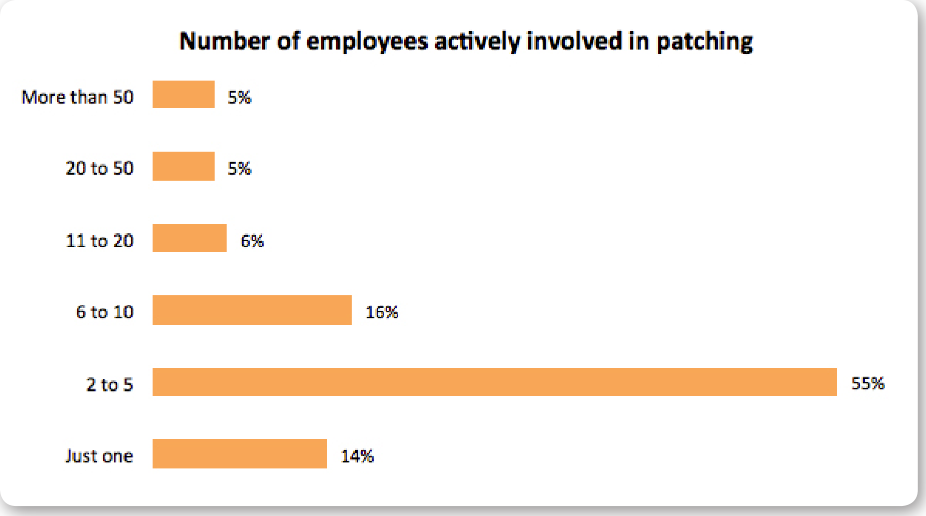
Number of employees actively involved in patching
More than 50
5%
20 to 50
5%
11 to 20
6%
6 to 10
16%
2 to 5
55%
Just one
14%

Fig. 24

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

The State of Security: **News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook