



The Road to Autonomous Patching

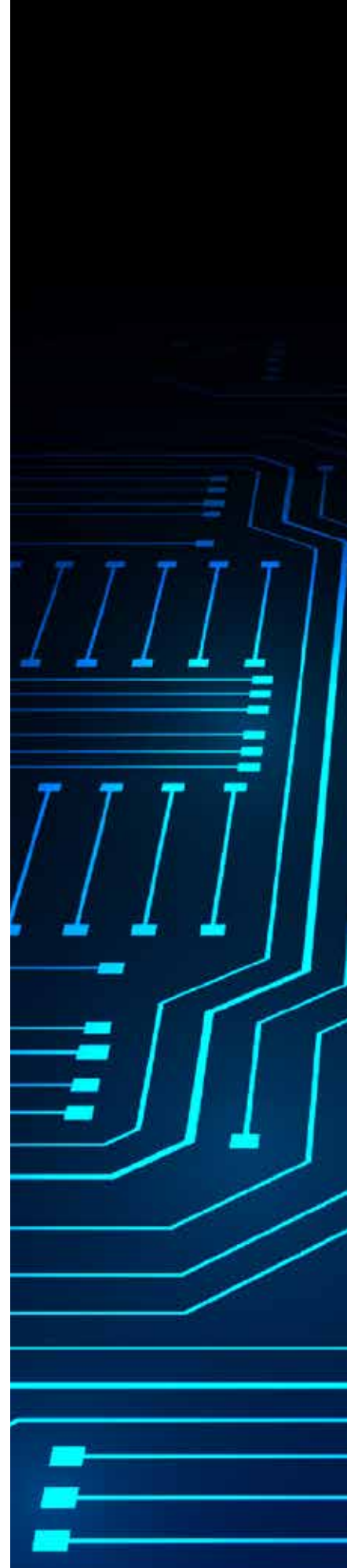
VISIT [ADAPTIVA.COM](https://www.adaptiva.com)
2023

Table of Contents

01	Introduction	3
02	Why Patching Sucks	5
	The Six Nightmares of Patching	7
	Overcoming Patching Nightmares	9
03	What's Wrong with Patch Management Today?	11
	Different Methods Same Results	13
	What's Next? The Future of Patch Automation	14
04	Using a Unique Platform	15
	Improving Reliability and Efficiency of Patch Deployments	16
	Keeping Up with the Speed of Patch Releases	16
	Overcoming Unmanageable Volumes of Patching 3rd Party Applications	17
05	Autonomous Patch Management for Modern Applications	18
	The Turning Point in Tech Utilization	19
	Cyber Threats and Vulnerabilities Make Their Move	20
	Endpoint Management Best Practices	21
	Limiting Factors in Patch Automation	22
	Endpoint Security, Patch Management, and Beyond	22
06	The Three Parts to Consider When Building Your Autonomous Patching Workflow	24
	Preparation, Execution, and Post Deployment	25
	Patch Automation to the Rescue	26
07	The Biggest Advancement in Patch Management Is Here	29
	Adaptiva's New Autonomous Patch Datasheet	31
	How Adaptiva's Autonomous Patch is Outpacing Every Patch Automation Vendor in the Market Today	35
	Automation Vendor in the Market Today	

01

Introduction



IT management is an inherently stressful job.

Teams responsible for the smooth operation of an organization's data and technology requirements are often under-resourced and overworked.



They are the first and last line of defense against software problems from bugs that can reduce company-wide productivity and the plague of malicious hackers looking to capitalize on holes in their security posture. However, they are often the first to be asked to “do more with less” and despite the lack of resources, they take all the blame when things go wrong. Third-party patching represents this wild west as well as any part of IT’s job. There are no clear rules or regulations for disclosure, patch availability, or deployment and IT teams cobble solutions together as best they can. In a world where 100% protection is an aspirational ideal, most look at 80% as good enough. Patching is flawed but solutions do exist to massively reduce the stress and burden.

This is a collection of our views on the Patch Management market – what’s broken, what needs to change, what’s in store for the future, and how Adaptiva can help.

02

Why Patching Sucks

THE 6 NIGHTMARES OF PATCHING

1. Overworked & overwhelmed employees
2. Remote work is the default
3. IT teams operate in silos
4. Long change management processes
5. Imperfect patches
6. A mountain of manual tasks

Is application security falling apart at the digital seams? There’s a patch for that—but by the time your IT teams put it in place, it may be too late. Try as they might, patch managers fail and fail again to apply needed repairs to third-party application vulnerabilities quickly enough to keep scheming hackers at bay.

Adding more people should help, right? Hiring or training staff doesn’t appear to solve the problem. It’s like adding traffic lanes to a crowded thoroughfare that inevitably fills up with more cars. Devoting more people and hours to patching doesn’t clear the ever-growing patch backlog. That’s because hackers work 24/7 and patches are released around the clock. Unfortunately, deploying those changes is a lot more complicated than deploying a quick fix and expecting all to be well.

Pressed by the need for speed but hindered by complex processes, IT workers might feel tempted to cut corners—with potentially disastrous results. Cybercriminals know almost before anyone else where software vulnerabilities lie and how to exploit them, and they will, given an improperly patched application or untimely delay.

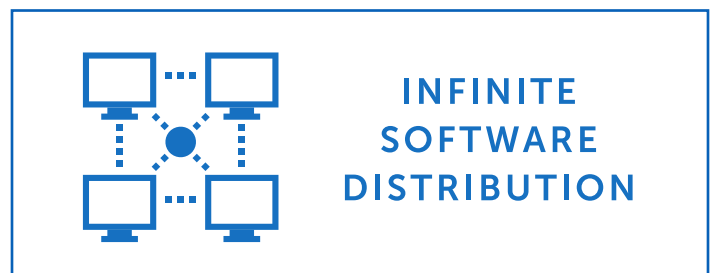
In fact, some 60 percent of data breaches over the past two years might have been avoided with timely patching.



With about half of companies reporting at least one breach during that time, we’re talking about a pervasive and systemic problem.

Companies know the dangers of falling behind. So do overwhelmed patching and deployment teams. Yet they still cannot keep up, costing enterprises money, customers, reputation, and legal exposure. Why is third-party patching so hard? The reasons are many, and inter-related. In the end, it all comes down to complexity.

Fortunately, there are solutions that can save organizations the patching headaches they have been facing for years. Let’s first address the problems, and then what solutions to look for to help solve them.



Using software supplied by other companies has become the norm among businesses of every size. Third-party applications provide us with everything from email to endpoint management. As operating systems have become more secure, malicious actors are seeking other unlocked doors into enterprises and their data. A lot of the time they're finding ways in through unpatched apps. The consequences could be dire, even lethal. An attack on a healthcare provider, for instance, can paralyze systems and delay or interrupt critical patient services.

Scripps Health in San Diego had to take parts of its IT system offline for several weeks after a 2021 ransomware attack, and even sent some patients to other hospitals. Postponed surgeries and cancelled appointments also hit patients of the Waikato Hospital system in New Zealand as well as the Irish Health Service after ransomware attacks that same year.

If security isn't a great enough concern to cause your enterprise to find a solution to the patching problem, compliance might be.

These attacks haven't been definitively linked to patching fails. But healthcare organizations that fall behind in patching are seven times more likely to suffer a ransomware attack, one study shows.

Governments are snapping to and insisting on timely patches. Two examples: The U.S. Department of Homeland Security now requires federal agencies and contractors to patch critical vulnerabilities within 15 days and high vulnerabilities in 30 days. The UK's Cyber Essentials has a similar requirement for UK government contractors. Where the federal government leads, state and local governments as well as the private sector often follow.

The 6 Nightmares of Patching

Every company has its own reasons for poor patch management, and we've heard a lot of them. Between the many enterprise companies we have supported over the years at Adaptiva, here are six of the most common difficulties we've observed.

01 OVERWORKED AND OVERWHELMED EMPLOYEES

Unfortunately adding more employees won't necessarily help all problems. There is more to the solution than just hiring additional staff. IT professionals need better tools and training to do their jobs. Updating and patching external applications is in itself a Sisyphean task given that these patches come in faster than they can be applied. By the time a patched version of an application is fully deployed it might already be outdated, supplanted by another new version with more patches.

The only tenable way to handle the backlog, for most, is to prioritize according to (1) how many people in the company use the app in question

and (2) how severe the security vulnerability is. Hackers will often target little-used applications for this reason: they tend to fall lower on the priority list, which increases the likelihood that intruders will be able to sneak in before the patch gets applied.

02 REMOTE WORK IS THE DEFAULT

As enterprises know, the move to remote work has caused a lot of security headaches, in part because employees often prefer to use their personal devices for work. Even where companies discourage BYOD people do it, anyway, if it's more convenient—and who's to stop them?

Undetected, unprotected and even unmonitored by corporate security, these off-premises devices are much easier for hackers to breach—you can't patch what you can't see. And with IT staff also working remotely, they're almost certainly going to have a harder time collaborating, which is essential for patch deployment.

03 IT TEAMS OPERATE IN SILOS

The team responsible for flagging software vulnerabilities may not be the same team that will patch that software. Vulnerability management typically is an IT security task; patching desktop computers might be the job of the desktop team, IT operations, or IT service management.

These disconnects can interrupt workflow, hinder effective communication, and cause even more friction and delays in the patching process.

04 LONG CHANGE MANAGEMENT PROCESSES

We've seen large organizations go through a change process with as many as 42 different approvers – all of whom had to sign off on the change before the product could go live. When a critical issue poses an immediate threat to your enterprise, this type of delay could be disastrous. And it may not even be necessary: the policies slowing you down may be outdated.

You may be required to consult with the technology team before installing security updates, for instance, an edict hearkening back to a time when IT approval was necessary for your company's security. Now the technologies your company uses would validate the update, allowing your teams to do this job without IT approval, but the old rule still stands. Timely patches face delays for no good reason except that, "It's always been done this way."

05 IMPERFECT PATCHES

The corrected software you receive may, itself, be flawed. Maybe, as happened in the now-famous SolarWinds hack, the update has already been compromised and waits for your deployment for criminals to gain access to your systems.

Knowing the potential risks in each patch and update, many IT teams are loath to simply "plug and play", even if it saves them time. They want to check each patch for safety, which usually involves observing it on several systems and testing for bugs before putting together a patch status report manually. All this checking, testing, and report-compiling requires precious time.

06 A MOUNTAIN OF MANUAL TASKS

Patching can take a lot of time to complete. A company might use multiple applications and need to apply many patches daily—hundreds, in the case of larger organizations. Not only are there security concerns as noted above, but compatibility tests can take days, as well.

And then, because some companies release patch after patch after patch, your teams must determine whether the metadata they're looking at applies to the patch they're wanting to apply, or to a different version. All told, a single patch can require as many as two weeks to deploy—and that's if all goes smoothly.

With all these twists, turns, hoops, and obstacles, it's a wonder that patching happens at all. As technologies proliferate—along with the software to run them—the problems with patching multiply, as well.

Patching endpoints is a critical component of every successful IT team. Installing the latest security updates is an easy way to ensure bad actors stay out of their networks.

Overcoming Patching Nightmares

Patching endpoints is a critical component of every successful IT team. Installing the latest security updates is an easy way to ensure bad actors stay out of their networks.

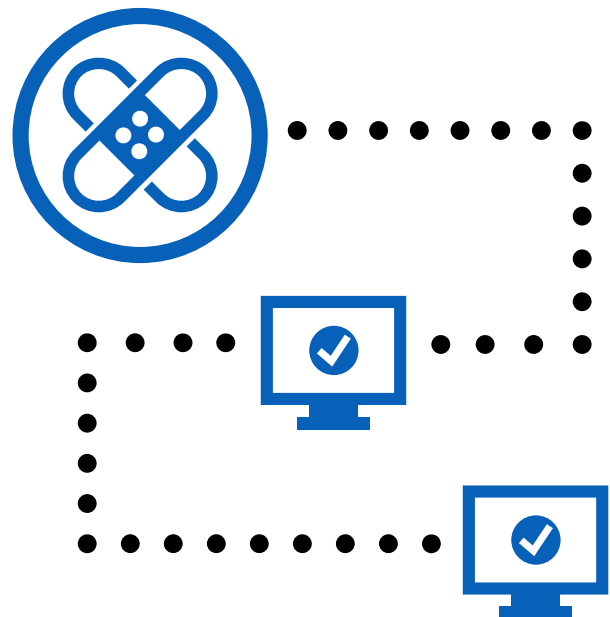
It's important to keep operating systems up to date, which Windows is getting better at on its own, but third-party applications provide the greatest opportunity for hackers and remain the hardest type of patches to distribute. There are thousands of third-party applications, and the list is growing, which makes patching them one of IT's most manual, time-consuming, and laborious tasks. It must feel like Sisyphus for the folks in IT; constantly pushing that boulder up the hill only to see it roll back down when the next batch of application patches drops.



A patch's lifecycle is not trivial for IT to contend with. Each application has its own unique release schedule and timeline; once a new patch is released, IT needs to test it to ensure it doesn't break anything in the environment. Then the patch goes through a phased deployment until it's successfully installed enterprise-wide, which can take weeks. Now multiply that process by the number of 3rd-party applications your organization uses, and it will make your head spin.

Ultimately, the goal is to manage risk.

Properly patching as many endpoints as possible and establishing an automated way to patch as much as you can is your best defense against people looking to exploit your network for their own gain.



03

What's Wrong with Patch Management Today?



Despite a renewed focus on security to bolster networks against cyberattacks, a main entry point for hackers remains unresolved for many large organizations. The way we patch third-party applications is fundamentally problematic. Several factors play a part including visibility into application installs, time, and legacy solutions that can't handle the complexity of modern work environments.

A new study from Ponemon Institute sponsored by Adaptiva surveyed 663 enterprise IT professionals across the United States from organizations with an average headcount of over 30,000. Sixty-nine percent believe that patching 100% of all applications is impossible. With widespread pessimism of what's possible, it's no wonder over-worked IT administrators feel defeated by the monumental task before them. They've tried and failed to successfully patch time and again.

Off the Radar: You Can't Patch What You Can't See

What, where, and how many apps are central to this dilemma. Visibility into what applications are on an organization's endpoints continues to be a major barrier to successful patching according to over half of those surveyed. Further, 69% of respondents have no idea how many distinct applications are on their endpoints.

How can they be expected to shore up holes in their network if they have no idea what needs their attention in the first place? The numbers are eye opening. The average organization has over 3,000 applications to manage and 54% say the number has only increased in the past two years.

Due to typical infrastructure obstacles such as low bandwidth, remote endpoints, and backlogs of other remediations, it can take an average of 12 hours just to determine if a patch has been deployed to impacted endpoints.



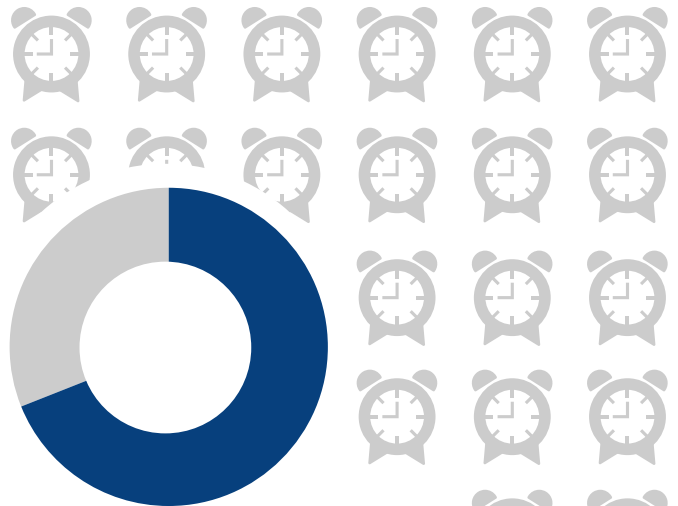
The Ticking Clock: Closing the Time in Between a Patch's Release and its Deployment

When IT falls behind on patches or spends too much time in the validation phase of the process, networks are exposed to bad actors who continuously scan potential targets for vulnerabilities. But the reality is that once a third-party application vendor makes a patch available, it takes an average of two weeks or more to begin deployment (according to 59% of respondents).

Due to typical infrastructure obstacles such as low bandwidth, remote endpoints, and backlogs of other remediations, it can take an average of 12 hours just to determine if a patch has been deployed to impacted endpoints. The timeline stretches another two weeks on average for patches to be deployed across an entire organization according to 48% of respondents. This gives hackers an entire month to find their way into a network and access sensitive data or gain control before anyone even knows they were there.

Zero-day patches, which by nature should be deployed immediately to prevent cybercriminals from taking widespread advantage of these vulnerabilities take a minimum of two weeks on average for 60% of respondents. Staying on top of even the most serious and widespread vulnerabilities remains a major challenge. Over a year after the widely publicized Log4j vulnerability, most enterprises remain vulnerable. How is staying this wide open to an attack still acceptable?

65% of patching teams spend between 10-25 hours a week on deployment.



Further, 69% of respondents have no idea how many distinct applications are on their endpoints.

Different Patching Methods, Same Results

No two organizations approach patching the same way. Decisions ranging from who is responsible for the process to methodologies and tools, regimented best practices do not exist. Those surveyed had varying responses regarding the responsible party for patch distribution.

Knowing how complex and burdensome patching is, it is concerning that more enterprises are not leaning on automation to take pressure off their employees.

Application owners drive the process for 25% of organizations with IT security (24%) and CSIRT teams (23%) close behind. Regardless of who drives the patching process, organizations should not adopt a one-size fits all approach to patching applications. According to respondents, different characteristics should be weighed with function (68%), risk (62%), and business unit (53%) as the most influential in deployment decisions.

Knowing how complex and burdensome patching is, with 65% of patching teams spending between 10-25 hours a week on deployment, it is concerning that more enterprises are not leaning on automation to take pressure off their employees. Of those surveyed, only 31% use automation in their patch strategy despite its ability to speed up deployments and reduce time spent on the process. By staying vigilant and proactively patching vulnerabilities, companies can better protect themselves from cyber threats and safeguard their sensitive data.



What's Next: The future of patch automation

Patching automation is a rapidly evolving field, and there are several best practices that organizations can adopt to improve their patching processes. By utilizing these technologies, organizations can improve their ability to identify and prioritize vulnerabilities, as well as streamline the patching process. Adaptiva's Autonomous Patch enables teams to set their patching strategies once and have confidence that patches, from regular releases to zero-day, will reliably deploy without human intervention.

04

Using a Unique Platform

A NOVEL APPROACH

1. Improving reliability and efficiency of patch deployments
2. Keeping up with the speed of patch releases
3. Overcoming unmanageable volumes of patching 3rd party applications



In 2023, it's difficult to comprehend any organization not leveraging edge computing to solve the daily challenges of IT teams.

Since edge computing processes data as close to the data source as possible, it comes with apparent benefits like low latency, improved scalability, increased security, and lower cost of maintenance. And much like seasoning to a dish once, you apply edge computing to certain processes - it can completely transform.

Edge computing can be broadly applied to a multitude of industries such as retail, IT, or even manufacturing. And within every vertical specific challenges. Even the most disparate industries share common challenges like 3rd party Windows patching, which is what we'll be exploring here.

Improving Reliability and Efficiency of Patch Deployments

Patch deployments are a critical aspect of IT operations and are essential for maintaining the security, stability, and performance of your systems. But they can also be a significant source of frustration and downtime for IT teams – especially ones that are already overworked and understaffed. Since patch deployments are used to address security vulnerabilities, fix bugs, and add new features to your systems. Without regular deployments, your systems could be exposed to security threats.

The lack of comprehensive monitors and controls doesn't alleviate the sheer volume of 3rd party applications.

Patching itself is already a process in which deployments can fail if there aren't solid steps in place; such as areas to approve deployment, notify of a patch failure, or alert key stakeholders. Improving the reliability and efficiency of patch deployments means there's a comprehensive feedback loop in place from start to finish in all regards to successful patch deployments. a patch failure, or alert key stakeholders. Improving the reliability and efficiency of patch deployments means there's a comprehensive feedback loop in place from start to finish in all regards to successful patch deployments.

Keeping Up With the Speed of Patch Releases

Many organizations struggle to keep up with the pace of patch releases and may fall behind on applying the latest updates. The sheer volume and complexity of patches can be overwhelming as significant testing and validation are required. Couple that with the

layers of patch interdependencies and lack of visibility and the overall challenge of keeping up with the speed of patch releases becomes a multi tenet issue.

This is where having sufficient coverage makes a massive difference. On average, an enterprise organization can expect to use roughly 2,908 applications across all departments - that means that you'll have one or two applications that'll need to be patched every day. That's a tremendous amount of manual effort pushed on to IT teams to manage on a regular basis. This is where having visibility into your applications goes hand in hand with proper coverage. You won't know what to patch if you don't know the full breadth of your current environment. Visibility is a consistent challenge.

Overcoming Unmanageable Volumes of Patching 3rd Party Applications

As technology continues to advance more organizations and their employees will become distributed and introducing additional endpoints and applications will become the norm in order to scale and conduct business regularly. However, with so many applications comes the challenge of patch management. Keeping all of these applications up to date can be a time-consuming and overwhelming task.

IT teams are more than aware of the planning and preparation it requires to be able to keep every 3rd-party application consistently updated with the latest patches. Which is why it's incredibly common to see those same teams finagle a product like SCCM in order to patch 3rd-party applications on Windows. But SCCM isn't good enough and you deserve better.

The lack of comprehensive monitors and controls doesn't alleviate the sheer volume of 3rd party applications. Having the right controls and monitors means certain functions like automation don't run rampant and administrators can set the rules. There is a risk of business disruption that can occur without consistent successful patch deployments. What you really need to overcome unmanageable volumes of patching 3rd party applications, the speed of 3rd party patch releases, and lack of reliable and efficient patch deployments is a solution that has true automation, one that's rooted in edge computing so it'll have all the inherent benefits of it, and the genuine functionality and autonomy to set-it-and-forget-it with full process control thereby eliminating tedious manual patching altogether.

You won't know what to patch if you don't know the full breadth of your current environment. Visibility is a consistent challenge.

05

Autonomous Patch Management for Modern Applications

ENDPOINT MANAGEMENT BEST PRACTICES:

1. Know what's in your environment
2. Be able to scan for vulnerabilities
3. Create a scalable patching policy
4. Have an Autonomous Patching Solution in Place













Patch management is a foundation of keeping your environment safe and secure. Updating your applications to the latest versions ensures functional bugs are fixed along with remediating potential security threats. It all sounds easy on paper - but in practice, patch management is a deluge of processes and challenges that can easily pose a larger problem for IT teams.

According to a recent survey from Ponemon Institute, enterprises run an average of 2,908 applications on their endpoint devices. The trend of continued application deployment isn't slowing down. Fifty-four percent said the number of applications has increased in the past two years. Additionally, the proliferation of endpoints at these companies require increases in data usage and infrastructure to support them. More applications and endpoints mean more patches to deploy which signals

more work for an already overworked and understaffed IT & Security teams. 54% of IT professionals consider endpoint patching a priority, so what's being done to ensure that it remains a priority? In a sea of zero-day threats, bugs, and vulnerabilities; it's essential to include endpoint patching as a central process pillar from the start.

The Turning Point in Tech Utilization

Endpoints have always been a staple of conducting modern business. Today, the sheer number of endpoints and types have massively expanded since the 1980s when computers started to gain popularity in the workplace. Forty years later computers are joined by smartphones, cloud-based applications, laptops, servers, IoT devices, and more. All this new technology has expanded the reaches of how and where organizations can conduct business like never before. Employees are

	SERVERS		PRINTERS
	MOBILE DEVICES		WEARABLES
	LAPTOPS		CLOUD-BASED APPS
	DESKTOPS		CLOUD-BASED SERVERS
	NETWORK DEVICES		SMART SYSTEMS
	IOT DEVICES/SENSORS		POS DEVICES

dispersed, applications are in the cloud, and sensitive data has spread throughout every corner of every business.

According to SpacelQ, “coming off a decade of technologies designed to help employees work outside the traditional workplace, this most recent decade was cathartic for those who prefer to work in an office.

Workplace technology solutions of the 2020s came in the form of IoT devices. Beyond connecting laptops, tablets, and smartphones to the cloud, we’ve now connected anything and everything!” This begs the question, at what point does security become part of the conversation? Having so many devices connected and exchanging data presents its own unique set of challenges. Most critically from a security standpoint, how do you keep your endpoints safe?

Cyber Threats and Vulnerabilities Make Their Move

Similar to the advancements of endpoints, cyber threats and vulnerabilities have also become increasingly sophisticated since the 1980s. New endpoints provided hackers new avenues to attack. And according to Embroker, the 10 most popular cybersecurity threats are:

■ **SOCIAL ENGINEERING**

A manipulation technique that exploits human error to gain private information. In cybersecurity, this lures unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.

■ **THIRD-PARTY EXPOSURE**

Attacks that occur on external third-party software, devices, or applications.

■ **CONFIGURATION MISTAKES**

An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.

■ **POOR CYBER HYGIENE**

Cyber hygiene is a set of habitual practices for ensuring the safe handling of critical data and for securing networks.

■ **CLOUD MISCONFIGURATIONS**

A catchall term used to describe common vulnerabilities that can lead to attacks such as unrestricted ports, storage access, lack of validation, and more.

■ **RANSOMWARE**

A type of malware that prevents or limits users from accessing their system, either by locking the system’s screen or by locking users’ files until a ransom is paid.

■ **MOBILE DEVICE VULNERABILITIES**

Exploitable software or hardware flaws in the network interfaces of a device or its applications that make a mobile device vulnerable to a network.

■ **IOT**

The Internet of Things describes physical objects with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.


■ **POOR DATA MANAGEMENT**

The practice of collecting, keeping, and using data securely, efficiently, and cost-effectively.

■ **INADEQUATE POST ATTACK PROCEDURES**

Taking the incorrect steps to evaluate a cyber-attack after it's occurred to avoid future attacks.

Your endpoints are exposed to a laundry list of cyber-attacks. One essential aspect of keeping your environment safe against vulnerabilities is to have a comprehensive patch management strategy in place.

	
BAD GUYS	3RD PARTY BUG HUNTERS / RESEARCHERS
	
IN-HOUSE TESTING AND RESEARCH	DHS RESEARCH

Endpoint Patch Management Best Practices

Creating, evaluating, and iterating on a patch management strategy shouldn't be an arduous process. The ability to have a procedure in place of regularly applying patches (fixes, updates, improvements, etc.) to software to prevent vulnerabilities from being exploited by cyberattacks takes precedence.

Patch management offers many inherent benefits that trickle from the IT team to the business at large. The Log4J exploit that occurred in early 2022 allowed malicious hackers to drop malware or ransomware on a target system. Log4J could easily wreak havoc on an environment - especially one that didn't have the proper patches in place.

To ensure you're prepared for what's looming around the corner, here're some **best practices for mapping out your endpoint patch management strategies.**

KNOW WHAT'S IN YOUR ENVIRONMENT

Do you have a comprehensive asset inventory? How many endpoints do you have? Do you know what third party applications are used across the organization? Do you know where to find the answers to all of these questions? It's impossible to patch an application that you never knew was being used - so ensure you have a complete understanding of all the systems and applications in your environment so you're always able to stay aware of vulnerabilities and available patches.

BE ABLE TO SCAN FOR VULNERABILITIES

You don't know what you don't know. Without the capability to scan endpoints and the applications they're running, it leaves you wide open to an attack. So ensure that you're one step ahead of the latest hack, zero-day vulnerability, or attack.

CREATE A SCALABLE PATCHING POLICY

This will be the how and when patching occurs. This includes the ability to keep track of patch release schedules (think of patch Tuesdays) and the timelines you'll need to test then deploy the patches. Whatever process you create needs to be able to be standardized and scalable as the company grows.

HAVE AN AUTONOMOUS PATCHING SOLUTION IN PLACE

An application like Adaptiva's Autonomous Patch fully automates the patching the process. Keep an eye out for features that include autonomy, robust reporting, applications supported for patching, and fast deployment.

Limiting Factors in Patching

Automation is an interesting word, it's representative of the future and what we come to expect from things we do or use to make our lives easier. But unlike a robot vacuum cleaner that continuously learns the layout of your living space, autonomous endpoint patching is a monumental task. It needs to learn your system, possess the ability to scan it, model your patching process for repeated success, prioritize different patches based on risk, support a list of 3rd party applications, and more.

Automating the patching process is a huge order and requires time and advancements in tech to run successfully. Many vendors will promote "true automated patching" but that isn't a standardized definition, so they can put out a subpar product that ultimately just provides a list of tasks for a person to take on and tack on automation without the necessary capabilities to back it up. Just up until the past year, that statement remained true.

IT teams are understandably hesitant to introduce new solutions into their tech stack because of the impact they could have on their environment and whether it can be well integrated without breaking anything. Imagine a scenario where an automated patching solution is brought into an environment where it's not able to perform as expected. The environment would remain vulnerable and the organization will have allocated resources for nothing. The technical limitations of autonomous patching have been overcome. Now, adoption remains the biggest hurdle in its implementation.

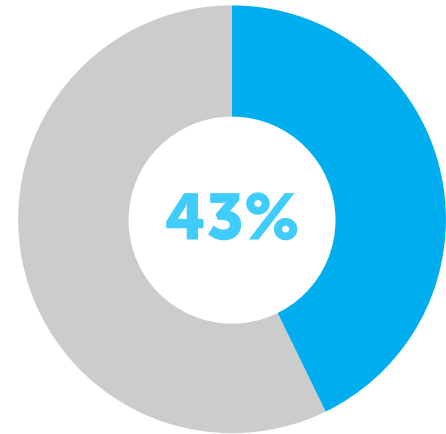
Endpoint Security, Patch Management, and Beyond

While creating an endpoint patching strategy will take time and effort - its importance can't be overstated. As we move into a workplace where in office, remote, and hybrid are all viable options - the increased flexibility applies both to the company and the malicious actors who seek to take advantage of any vulnerability.

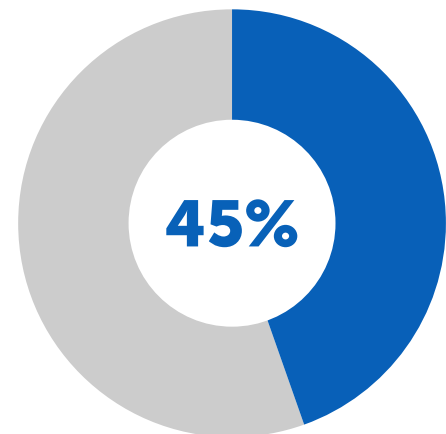
According to a recent Sophos report on the state of endpoint security, "IT security remains a highly challenging and complex area for organizations across the globe, fueled by the ever-increasing complexity of malware attacks and the financial incentives for attackers.

The gap is growing between the knowledge and skills of the attackers, particularly around the areas of ransomware and exploits, and that of the IT professionals charged with stopping them. Traditional security solutions are no longer enough to keep organizations ahead of today's complex threats." And that has given rise to the ever-popular growing trend of autonomous patching solutions.

Don't wait until it's too late. Create your patching strategy, purchase your patching software, and ensure the right steps are taken to secure your environment.



43% OF BUSINESSES TAKE AT LEAST A WEEK TO ROLL OUT THE MOST CRITICAL PATCHES



45% OF BUSINESSES SAY ZERO-DAY ATTACKS ARE THE BIGGEST THREATS TO ENDPOINT SECURITY

06

The Three Parts to Consider When Building Your Autonomous Patching Workflow



Patch management is a problem that every organization faces daily. And in 2022, there was no shortage of large well-known organizations that experienced security breaches. From Uber, Cash App, to Twitter - the common thread among all of these attacks was an unpatched vulnerability. Even if you have a patch management strategy in place, it's easy to miss a step and potentially leave your environment vulnerable. As more and more companies look to introduce autonomous patching solutions, it further highlights the challenge of adequately patching.

The difference between a successful patching strategy versus an unsuccessful one usually comes down to creating the best workflow for your environment. The best way to imagine how your workflow should work is a train system that is able to move at a sufficient speed, stop at each required station, and be able to have maintenance performed on it. When you consider your workflow, the easiest way to think about it is to break it into two parts: preparation, and execution.

The Three Things to Consider When Building Your Autonomous Patching Workflow

PREPARATION:

Consider your current environment setup. How many endpoints do you have, how many locations do you have, what applications are you using, etc.? Going blind with patching has a lot of potential negative implications. Imagine having a suite of security tools and only patching the one that notified you of an update and not doing the same for the other products —that means you're only partially protected.

- After getting a comprehensive asset inventory, start to catalog and scan for your current vulnerabilities.
- Start to group endpoints into logical groupings: geography, business unit, risk profile, etc.
- Have patching criteria in place. Prioritize things like your operating system and system tools first, but also be aware of applications that are high risk. The last thing you want to happen is a repeat of Log4J.

EXECUTION:

Once you validate the patches required, then it's time to deploy the patch itself. Whether that is a slow-phased approach or enterprise-wide will depend on the application and its risk level. If it's successful, then congratulations. If not, then you need to begin the troubleshooting process.

- Review the error you're receiving and consult documentation to fix the error and deploy again. Especially when it comes to manual patching. Failed manual patches are a regular occurrence.
- Document and monitor the changes and ensure your logs are kept up to date that the applications have been successfully patched.

- Autonomous patching solutions will provide reporting capabilities that allow you to review your patching in real-time, what failed, remediations for successful deployments, as well as control to stop or pause a deployment and roll-back capabilities.

POST DEPLOYMENT:

- Find opportunities to iterate on your patch deployment. What went right, what went wrong, and how can you make what went right repeatable and scalable. Were there endpoints that consistently failed to patch, users that postponed deployments and reboots? All essential points to consider to make your deployments go smoothly.
- Your patching workflow plays an important role in your endpoint patching process and needs to be handled with care from start to finish. Use the information outlined in this article to help build that roadmap and start successfully deploying your patches.

Patch Automation to the Rescue

So, what do organizations do? The answer shouldn't be overcoming this dilemma by skipping versions, bypassing testing, or employing a one-size fits all approach to all third-party applications. Sadly, IT teams often have no choice but to resort to cutting at least one of those corners if they're strapped for time, resources, or budget.

Enter patch automation software vendors. These vendors may be able to eliminate some of these burdens, helping turn third-party patching from a major hassle to a strategic business strength. But the problem is that all vendors in this space are not created equal. Some even make claims that their technology can't back up.

So, before jumping into a long contract with an Autonomous Patch Management vendor, make sure you consider these five things.

01 INTELLIGENT AUTOMATION THAT ENABLES TRUE AUTONOMY

Let's face it, IT teams have better things to do than constantly and repeatedly chase down third-party application patches. It's a time-consuming and manual job, but it's necessary. So, when looking for a vendor to help automate that process, ensure they can automate every step of the patching process. Unfortunately, many "Patch Automation" vendors claim true automation when they're just providing you patching metadata and a plug-in to Microsoft Endpoint Manager (MEM) or another UEM tool.

Look for the ability to create different patching automation strategies with varying testing thresholds, roll-out phases, configurations, and deployment options for various devices, user groups, or applications. Patching is not a one-size fits all problem, so make sure you don't sign up for a one-size fits all solution. Configurable out-of-the-box patching

templates should be available to use or modify to create any patching deployment model your business requires.

02 REAL-TIME VISIBILITY AND CONTROL

It's not enough to have pretty dashboards and customizable views. You should expect to be able to see the real-time status of patch deployments, successful installs, and failures. Vendors in the patching space should also be able to provide actionable insights through AI that provide you areas and opportunities to optimize your patching strategy further and create additional patching efficiencies.

63% of companies say that a lack of visibility over their endpoints is their most significant security risk. That percentage jumps when talking about an ever-growing library of third-party applications users adopt. It's impossible to keep up with all the different applications and versions. So having visibility not only into the endpoint but into the various applications and versions it's running is a must.

03 ZERO-DAY SUPPORT

The Cybersecurity Insiders 2022 Endpoint Security Report shows that companies are historically slow to react to the most critical patches. 43% of businesses take at least a week to roll out the most critical patches. When the next zero-day exploit pops up, a patch automation vendor is worth its weight in gold and goes from a "nice-to-have" to "kept our business out of the headlines."

45% of businesses say zero-day attacks are the biggest threats to endpoint security and that the average cost of an endpoint attack is \$1.8 million annually. Patch automation vendors allow you to react the second a new threat is discovered – you can pause everything else, automatically push out the patch via your preferred patching strategy and ensure a 100% successful installation rate. As a result, you stay one step ahead of the bad actors and ensure your business's security and compliance.

04 EFFICIENT SOFTWARE DISTRIBUTION

A massive problem with patching is that despite IT's best efforts to find, test, and distribute the patch - the larger the enterprise gets, and the further the endpoints move toward the edge, the less reliable legacy content distribution methods become. Whether it's Patch Tuesday or just a standard security update, distributing that content across the globe to each endpoint can be a headache and often very unreliable. Some vendors in the space plug into and rely on MEM for patch distribution, but even still, completion rates rarely hit 100%.

Look for an automated patching solution that is compatible and improves upon your UEM investments but is not reliant on it and won't break your current workloads.

05 SET IT AND FORGET IT

Automating the 3rd-party patch process will somewhat reduce the need for human intervention. If you're ready to eliminate the need for human intervention in the entire

endpoint patch process, then look no further than an Autonomous Patch Management solution. With this type of solution, you can express how you want your patching handled by business unit, application, and user. Then the patching tool will automatically execute your strategies repeatedly without requiring you to do a single thing. The moment a new patch version is available, the autonomous endpoint patching tool will find it, check which deployment strategy you have chosen, and execute it across your enterprise automatically, with zero human intervention. Set it and forget it; allow your IT team to spend their time working on core business strategies and let Autonomous Endpoint Management handle the patching.

Patching 3rd-party applications can seem like an insurmountable task, but there is help out there. Autonomous endpoint patching vendors can help take this manual task and turn it into a business strength. Now you are equipped with the right questions to ask when evaluating these solutions.

Clearly, the exigencies of patch management are too complex for manual processes. Your IT people only have so much capacity to juggle a dizzying and even befuddling array of tasks. But for every problem technology creates, technology also tends to provide a solution—and patching is no different.

Advances in technology such as artificial intelligence and machine learning make patch automation faster, smoother, and easier than ever. In fact, using automation to investigate and remediate vulnerabilities and attacks could reduce the average cost of a breach by 25% – some \$450,000 a year – a recent Ponemon Institute-survey shows.

A true autonomous patch management solution can move you through the many steps of patch management with almost no human intervention. It can even deploy multiple patches simultaneously, and in a fraction of the time manual processes require—shaving the time to deployment from weeks to minutes, letting your teams focus on more strategic tasks.

It just so happens that we offer these capabilities in Adaptiva Autonomous Patch, which will take the manual work and the conjecture out of third-party application patching. For once, you'll get to focus on strategy while Autonomous Patch keeps the applications running on Windows devices in any location up to date.

A true autonomous patch management solution can move you through the many steps of patch management with almost no human intervention.

07

The Biggest Advancement in Patch Management is Here





Patching 3rd Party Applications Is a Never- Ending, Unwinnable Game of Tetris –Until Now.

Tetris shapes seem to come completely at random, at varying speeds, and you never get what you're looking for when you need it. It's a never-ending roller coaster of stress as the shapes drop at inexplicable rates as you scramble to make them fit before "topping out" and being overrun. The object of the game? Survive. There is no real way to win (yes, it's been proven) – success is determined by how long you can stay ahead before you lose.

Tetris is a fun game, and a great distraction from the stress of everyday life. After all, there is only one way to lose and there are no real stakes in the game - you run out of space to place a shape before a new one appears, the game ends, and you then you just start over. Now, imagine if there were more ways to lose, the game moved faster, was even less predictable, and if you lost you could lose millions of dollars. But, like the real game of Tetris, the longer you play the harder it gets. Would you still consider it fun? While that might sound like a cruel concept in a science fiction novel – it's a vivid allegory to the everyday reality for IT keeping systems and endpoints patched.

Third Party Patching is Just Like Tetris

The tetrominoes (or small Tetris shapes) represent new versions of an application that needs to be deployed. And instead of only six variations in shapes, there are hundreds of variations. Each time a new patch is available, it must be deployed, and placed in the perfect spot before another patch is available –

ensuring that all the pieces fit together, and, in turn, systems don't break. They also don't come in sequential fashion – many patches could be released at once, or in rapid succession. Further, not every patch is equal in severity. You may have started to deploy one patch, but a more severe one was since released and needs to be at the front of the deployment line. It's no wonder this has never been a game; it's the undeniable, very consequential reality of most IT teams.

Patches keep coming, and regardless of how many times IT has patched an application before, the work will repeat. They will go through the same motions of finding the metadata, prioritizing the patch based on severity, test the patch, deploy it, test more, fully deploy. This multi-step manual process has no multiplicity. Patch Management software treats all patches as one size fits all, with no ability to repeat work automatically.

And while we wish Tetris would gamify the patching process, IT unfortunately must rely on Patch Management software rather than video games to patch systems. Yet, every Patch Management tool on the market today promises automation upfront and then severely underdelivers requiring highly specialized scripting and coding skills; and those skills are in short supply.

Every patch automation tool on the market today promises automation upfront and then severely underdelivers.

Introducing Adaptiva's Autonomous Patch

Introducing a radical new approach, Autonomous Patch – the first truly autonomous endpoint patching software for third-party Windows applications.

Gone are the days of painful manual tasks, of doing the same thing over and over, or of cutting corners. By schematizing strategic intent and combining it with sophisticated models of enterprise business units and patching processes built by the administrator, the work is done, and patching will

simply happen. Metadata will stream down from Adaptiva CDNs, and patches will be deployed at a steady pace and according to the unique patching strategy for that application. Like all Adaptiva applications, Autonomous Patch is built to excel at enterprise speed and scale and will thrive in the most complex and bandwidth-limited environments.

Adaptiva's Autonomous Patch is the revolution in endpoint patching that the world has been screaming for, and we're just getting started.

TO LEARN MORE, VISIT US AT ADAPTIVA.COM/PATCH



Capabilities in our public preview include:

COMPLETE VISIBILITY

You no longer have to “click and hope.” Real-time reporting and monitoring dashboards show you real-time progress to help you achieve Patching Strategy goals. You will be able to see what is happening when it is happening.

SET AND FORGET PATCHING STRATEGIES

Pull together all components that define how you wish to handle the notification, approval, deployment, and configuration of applications upon the release of a patch. As soon as metadata is available, patches will be automatically deployed as dictated by patching strategies.

CONTINUOUS METADATA AND AUTOMATED PATCHING

All the required information for detection, applicability, installation, severity, customization of software, along with over 100 other fields to determine the importance of a given patch. When a request is received or a new release is available, the metadata will be published to the feed system and automatically streams down to your Adaptiva server, and from there, it streams down to all endpoints that need it according to your patching strategies.

NOTIFICATION BOTS

Administrators will receive an automatic notification the moment an update is released. Notifications can be an email, text messages, Microsoft Teams message, a ServiceNow ticket, or any other kind of notification you wish to perform when an update is released.

DEPLOYMENT BOTS

When a release is available, deployment bots will trigger a workflow that will manage the initial deployment of that release. Within the workflow you can set whatever you want with that patch, such as approval processes, test deployments, service desk tickets, or any custom logic you want.

DEPLOYMENT CHANNELS

When a patch is ready for full deployment, it will be placed in a Deployment Channel. This acts as a queuing system for patches to aggregate patches based on their urgency and deploy them at a suitable time that won't disrupt the end user. For example, a company may create weekly, monthly, and quarterly channels. Patch deployment bots will examine each patch, and automatically route it to the most appropriate deployment channel.

CUSTOMIZABLE PRODUCTION DEPLOYMENT WORKFLOWS

Production rollout can take whatever form you like, with any phases, notifications, gates, and triggers you want. You can use a combination of waves and rings to decide what devices get the update and in what order. Within the workflow, you can control under what conditions a wave rollout should take place.

BUSINESS UNIT MODELS

Build models of logical grouping constructs for different classifications of devices. This can be defined by business function, or could be a grouping based on device type, hardware manufacturer, geography, or any other criteria you want to group machines. This allows you to apply similar characteristics to a group of

machines to define rollout behavior across the organization.

ROLLOUT MODELS AND AUTOMATIC INSTALLATION

Perform phased deployments within a business unit, depending on any criteria you have defined in the business unit models. Rollout can be as broad or granular as you like, and once the behavior is modeled for a business unit it will behave this way every single time. As soon as the rollout process begins, the actual device deployment takes place, and the right machines will perform the installation.

Model your strategies once

Now instead of these patches constantly raining down like the unpredictable game of Tetris, all you have to do is model your business and application patching strategies once, and then Autonomous Patch takes care of the rest. You won't have to scramble to figure out how to install all patches on all machines and make all the patches fit together before you lose the game. Autonomous Patch will assess each patch for importance, apply your strategic intent to the release and process it through your modeled business and devices.

Gone are the days of painful manual tasks, of doing the same thing over and over, or of cutting corners.

Humans shouldn't be patching computers. Technology should do that.

Deployments will simply happen, and you can sit back and watch as it does. Set it and forget it: as a new patch becomes available, and the metadata is fed to the system, it will apply those patches on the endpoints you have modeled, without having to lift a finger. Gone are the days of being stuck in a flood of backlog tasks that rip open holes in your cyber-defense walls opening the entire business to significant risk.

The simple truth is humans shouldn't be patching computers. Humans shouldn't have to waste their time babysitting technology problems – technology should do that. Humans shouldn't be patching computers. Technology should do that.

Adaptiva's Autonomous Patch is the only technology that requires no human intervention in the third-party patching process, thereby improving your cybersecurity posture and making it more difficult for bad actors to wreak havoc. Humans get to dictate the right strategy and then watch as technology patches itself.



Click the logos below to see how Adaptiva compares to



How Adaptiva's Autonomous Patch Is Outpacing Every Patch Vendor on the Market Today:

PATCH DISTRIBUTION

Distributes patches faster and more reliably with P2P Edge Cloud Platform. Powers all solutions.

PATCH CATALOG

Unlimited enterprise apps, any line of business app you need, and a dedicated metadata team adding to the ever-growing list.

AUTOMATION

Customize pre-built templates or build your own patching strategy models once, then Autonomous Patch executes your strategy over and over.

ZERO DAY

Vulnerabilities are addressed in real-time, so endpoints are always secure.

HUMAN INTERVENTION

Requires no human intervention.

FLEXIBILITY

Can define any patch model including ability to set urgency, individual departmental requirements, and testing for different applications, business units, and users.

DEPLOYMENT RATES

Meets or exceeds the most rigorous SLAs.

VISIBILITY

Fully customizable, real-time dashboards that include actionable insights with current state and historical views, plus suggested next steps to optimize your patching strategy.

CUSTOMER SUPPORT

4+ consecutive years with 100% customer satisfaction. Average response time is less than 25 minutes.

RESOURCES

1. **Adaptiva's Autonomous Patch**
2. **Adaptiva's Autonomous Patch Datasheet**
3. **Five Capabilities You Need in an Autonomous Patching Vendor On-Demand Webinar**
4. **World-Famous Hackers Exploit Common Enterprise Applications On-Demand Webinar**
5. **Request a demo of Adaptiva's revolutionary Autonomous Patch**

ABOUT ADAPTIVA

Adaptiva's autonomous endpoint management applications fill capability gaps of leading unified endpoint management platforms for Windows. Autonomous Patch intelligently automates the entire software patching process from identification to enterprise-wide deployment for first and third-party Windows applications. Endpoint Health's automated health checks and remediations maintain compliance and health of Windows devices in enterprise environments. OneSite Anywhere instantly distributes software and content to any Windows device in any location with a single server. Learn more about how Adaptiva's applications ensure your Windows devices remain healthy, productive and secure at adaptiva.com.