



PATCH MY PC

WHITEPAPER

The Application Iceberg: The Hidden 80% of Enterprise Risk

Vulnerability discovery lives above the waterline.
Remediation lives below it.

Why OS Patching Alone No Longer Reduces Enterprise Risk

Executive Summary

Most enterprise patching programs were designed for a different era.

Ten years ago, keeping your Windows operating system current eliminated a meaningful portion of enterprise risk. Today, the OS is only one component in a sprawling software ecosystem that includes browsers, collaboration platforms, document readers, file transfer tools, remote access software, developer utilities, and hundreds of other third-party applications.

Attackers have adapted accordingly.

According to Verizon's 2026 Data Breach Investigations Report, vulnerability exploitation was involved in 48% of breaches, making it one of the most common initial access vectors observed across the threat landscape¹. Recent breach investigations and exploitation reporting reflect this shift. Vulnerability exploitation continues to grow as an initial access vector while software products outside the operating system appear repeatedly in CISA advisories and the Known Exploited Vulnerabilities Catalog.^{2,3}

The same pattern shows up beyond the endpoint as well. Third party vendors, file transfer platforms, remote access tools, and supply chain software continue to show how quickly software exposure can turn into business risk.⁴

Advances in AI-assisted security research like we've seen with Claude's Mythos are exacerbating the situation by increasing the volume of vulnerabilities entering enterprise remediation pipelines. Security teams are identifying more vulnerabilities than ever before while many infrastructure teams continue operating with the same staffing levels, maintenance windows, and deployment processes they relied on several years ago.

The result is a widening gap between vulnerability discovery and vulnerability remediation. Organizations are getting better at identifying exposure. Attackers are getting faster at exploiting it. Many patching programs are still operating on timelines designed for a pre-AI threat landscape.

ENTERPRISE RISK BY THE NUMBERS

48%

of breaches involved
vulnerability
exploitation
(Verizon DBIR)

Hundreds

of third-party
applications per
enterprise
endpoint estate

**Weeks
to Months**

typical enterprise
remediation time for
critical vulnerabilities

429

security fixes in
one Chrome
Stable release

The Iceberg Beneath Patch Tuesday

Ask most organizations how they measure patching success and the discussion usually centers on Windows: update compliance, endpoint health, security baselines, and the percentage of devices running current security updates. These metrics matter, and mature IT organizations track them closely. The problem is that they describe only a fraction of the software environment they intend to protect.

The modern enterprise endpoint extends well beyond its operating system. It is defined by the applications running on top of it. A typical knowledge worker's laptop may run Chrome, Edge, Acrobat, Teams, Zoom, VPN clients, password managers, browser extensions, compression tools, developer utilities, along with a long list of business-specific applications. Across thousands of endpoints, that quickly becomes hundreds or thousands of unique software products requiring ongoing maintenance.

Operating system patching has benefited from two decades of investment in tooling, process, and reporting. Windows updates arrive on a predictable cadence, deployment workflows are well understood, and compliance reporting is readily available through platforms such as Intune, Configuration Manager, and Microsoft Update. Most organizations can determine their Windows patch status within minutes. Achieving the same level of visibility across hundreds of third-party applications is often far more difficult.

Sometimes nobody owns these apps, which can create long-tail gaps in patching cadence. Managing them is operationally messy. As application counts increase, visibility into third-party software tends to degrade, even in organizations with otherwise mature patching programs.

This creates a mismatch between visibility and risk. An endpoint may be fully compliant from an operating system perspective while still running multiple applications with known exploitable vulnerabilities. From a reporting standpoint, the device can appear healthy. From an attacker's perspective, it may still represent an attractive target.

The iceberg analogy is useful because it reflects how most organizations experience patching. The operating system sits above the waterline. It is visible, measurable, and generally well managed. Beneath it sits a much larger collection of third-party software that consumes the majority of teams' patching efforts, introduces a significant portion of vulnerability exposure, and often receives far less executive attention.

- Patch Tuesday
- Windows cumulative updates
- Server OS updates

- Browsers
- VPN clients/gateways
- Security tools
- Citrix
- Adobe
- Collaboration software
- Business applications
- Third-party libraries
- Edge devices



HOW THIRD-PARTY APPLICATIONS CREATE MORE RISK

- ✓ Different release schedules
- ✓ Different ownership teams
- ✓ Different installers
- ✓ Inconsistent deployment mechanisms
- ✓ Different packaging requirements
- ✓ Limited reporting
- ✓ Different testing processes

Result: Operational complexity slows remediation.

Attackers Follow the Path of Least Resistance

Security professionals often describe attackers as sophisticated, but most successful attacks are driven by practicality rather than technical elegance. Threat actors generally pursue whatever route offers the greatest probability of success with the least amount of effort.

Historically, operating systems were prime targets because a single compromise could unlock broad access and elevated privileges across the enterprise. Over time, however, operating systems became more resilient. Patch management improved. Endpoint protection matured. Security teams built repeatable processes around operating system updates. While organizations focused on the tip of the iceberg, adversaries shifted their focus to the layer below the waterline.

Third-party applications did not benefit from the same degree of standardization applied to the OS. For attackers, the messiness of the workflow creates opportunity.

This evolution should not be surprising. Security investments tend to raise the cost of attacking a particular layer of the technology stack. Attackers, like water over a patched leak, reroute elsewhere.

Most organizations already understand this risk conceptually. The operational challenge begins after a vulnerability is identified. Knowing which applications are exposed is one issue. Performing discovery, packaging, testing, deployment and exception management can consume weeks to months when combined with disruption mitigation and compliance verification. Doing all of this safely, consistently, and at scale is something most teams are ill equipped to accomplish.



AI is being leveraged by threat actors to accelerate the time to exploit known vulnerabilities, shrinking the window for defense from months to mere hours.”

– Verizon 2026 Data Breach Investigations Report (DBIR)

Security's New Scaling Problem

Over the last two decades, the cybersecurity industry made enormous investments in visibility. Vulnerability scanners became more sophisticated, asset inventories became more accurate, threat intelligence became more accessible, and organizations gained significantly better insight into the software running across their environments.

By most measures, those investments paid off.

Modern vulnerability management platforms:

- ✓ Continuously inventory software
- ✓ Prioritize findings based on exploitability
- ✓ Correlate assets against vulnerability databases
- ✓ Alert teams as new exposures emerge



The remediation engine is running at the same RPM. The load has increased nearly eightfold.”

– Qualys Threat Research

Enterprise organizations are identifying vulnerable software more efficiently than they could ten years ago. However, these operational gains have not been matched by equivalent improvements in remediation. Metaphorically speaking, the iceberg gets wider the deeper we go.

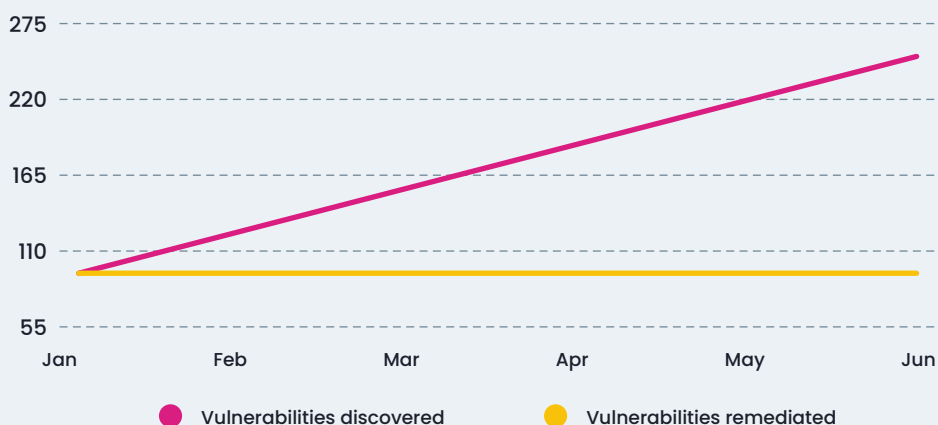
Applications still need to be evaluated, packaged, tested, approved, deployed, and verified. Those activities still require people, maintenance windows, and change management processes, no matter how quickly a vulnerability appears in a dashboard.

Take Chrome as a simple example. One stable release in June 2026 included 429 security fixes, including multiple critical vulnerabilities⁵. That is just one application adding real work to the same deployment pipeline. As software inventories grow and vulnerability volume increases, those workflows become harder to scale.

The pressure is intensifying. Advances in automation and AI-assisted security research

When Discovery Outpaces Remediation

Illustrative example showing how vulnerability backlogs grow when discovery exceeds remediation capacity.



Illustrative example based on trends described in Verizon DBIR 2026 and Qualys Threat Research.

are increasing the volume of vulnerabilities entering enterprise remediation pipelines. Researchers can identify weaknesses more efficiently than before; vendors are releasing fixes at a faster pace, and security teams are processing larger volumes of findings than they were only a few years ago.

A simple example illustrates the challenge. An organization that receives 100 actionable vulnerabilities each month and remediates 100 remains relatively stable. If improved tooling, threat intelligence, or AI-assisted research increases that volume to 200 findings per month while remediation capacity remains unchanged, a backlog emerges immediately. If the imbalance persists, vulnerability accumulation becomes a structural characteristic of the environment rather than a temporary operational issue.

Many security teams are already experiencing this dynamic. Visibility continues to improve while remediation queues continue to grow. Quarterly reports contain more data, more findings, and more prioritization logic than ever before, yet many organizations still struggle to reduce the number of outstanding vulnerabilities in a meaningful way.

The industry's ability to generate vulnerability intelligence has advanced rapidly. The workflows responsible for turning that intelligence into completed remediation have evolved much more slowly.

The Packaging Bottleneck

This is where vulnerability management becomes endpoint management.

The moment a vulnerability is identified, the work shifts from the security team to the teams responsible for deploying software updates. In theory, the next step sounds straightforward: install the fix.

In practice, that fix often travels through a surprisingly long chain of operational dependencies.



Multiply that process across dozens or hundreds of applications and the scale of the challenge becomes apparent.

This is particularly true for third-party software because every vendor ships updates differently. There is no universal patching standard. Each application introduces its own packaging requirements, testing considerations, and deployment risks.

As a result, remediation speed is frequently governed by packaging capacity rather than security priorities.

Security teams may identify a critical vulnerability in minutes. Remediation may still take days or weeks simply because the deployment pipeline cannot move any faster.

The Scanner-to-Fix Gap

The cumulative effect of these operational constraints is what many organizations experience as the scanner-to-fix gap.

Most enterprises already possess mature vulnerability discovery capabilities. They maintain scanners, subscribe to threat intelligence feeds, and invest heavily in exposure management programs. In the best-case scenarios, security teams have a clear understanding of where vulnerabilities exist, but often, even with scanners and threat reports, long tail software and background utilities can hide issues that linger long past when updates are published.

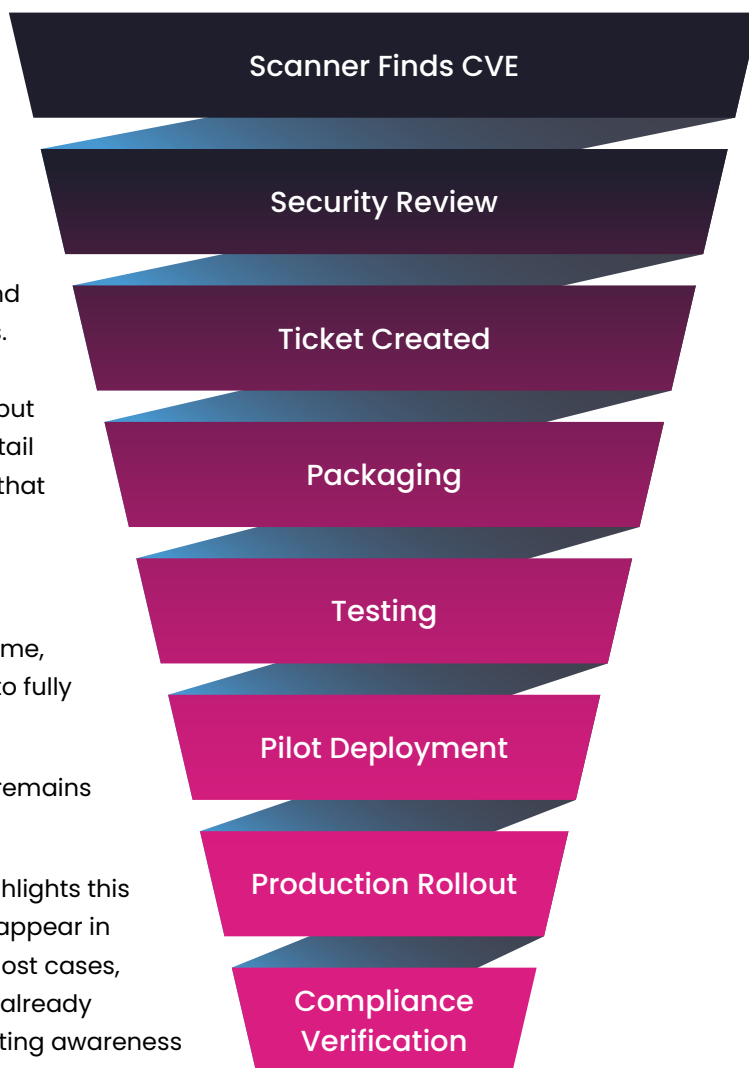
More bottlenecks appear further downstream.

According to Qualys, while detection is near real-time, critical vulnerabilities often take weeks to months to fully remediate in enterprise environments.

Throughout that process, the vulnerable software remains in production.

CISA's Known Exploited Vulnerabilities program highlights this reality repeatedly. Many of the vulnerabilities that appear in the catalog are neither obscure nor unknown. In most cases, organizations are aware of them and patches are already available.³ The difficulty lies in consistently translating awareness into action across hundreds of applications and thousands of endpoints.

As vulnerability volumes continue to increase, the efficiency of that remediation process becomes increasingly important. Organizations that reduce risk most effectively are not necessarily the ones with the largest teams. They are the ones that are able to minimize organizational friction to move updates from identification to deployment quickly.



CISA continues to emphasize that many of the most dangerous vulnerabilities are already known, already patched by vendors, and remain exploitable primarily because organizations have not completed remediation.

– Verizon 2026 Data Breach Investigations Report (DBIR)

Beneath the Surface

- Investments in vulnerability scanning tools over the past decade has produced better visibility, richer reporting, and more accurate risk assessments.
- As the visible layer of risk has become more manageable, **attackers have shifted toward software layers that remain difficult to patch consistently at scale**. At the same time, AI-assisted research is fueling a growing volume of vulnerabilities entering remediation pipelines.
- Lack of visibility is not the problem. Many **organizations are better at finding exposure than they are at remediating it**.
- The challenge is operational. IBM security research has shown that **delays are rarely technical – they are process and coordination driven**. Vulnerabilities move through packaging queues, testing cycles, deployment rings, maintenance windows, and change management processes before they ever reach an endpoint.
- Operating system patching represents only a fraction of the work required to reduce enterprise exposure. The **larger challenge sits beneath the surface in the sprawling ecosystem of third-party software** that powers modern business operations. That is the iceberg.

The Solution

The challenge is not what organizations can see, it is what they can act on. Vulnerable software is largely visible within modern environments. What remains difficult is moving from identification to remediation quickly, consistently, and at scale across the operational iceberg. This is where automation becomes valuable.

Organizations that rely on Microsoft Intune, WSUS, or Configuration Manager already possess the infrastructure required to deploy updates across their environments. What they lack is an efficient way to deliver those updates without increasing risk exposure or breaking production in the name of compliance.

Patch My PC — Designed to Close the Gap

Rather than replacing existing Microsoft management tools, Patch My PC operates within them. It identifies newly available third-party application updates quickly, downloads and tests content centrally, and automates the packaging and deployment tasks that create bottlenecks for endpoint management teams.

Instead of manually chasing installers, rebuilding packages, and maintaining update workflows for every application, endpoint teams can automate much of that effort and focus on higher-value activities that require experience and judgment.

The result is a dramatically shorter path from vulnerability disclosure to remediation.

Organizations can then use the deployment controls they already trust to determine how updates move through the environment. Pilot groups, validation rings, phased deployments, maintenance windows, and production schedules remain under the customer's control. The deployment strategy adapts to the business rather than forcing the business to adapt to the tool.

Visibility Improves As Well

Patch My PC Advanced Insights for Intune and Configuration Manager provides reporting and compliance visibility for managed and supported third-party applications. Security teams can quickly determine which applications are current, which devices remain exposed, and if remediation efforts are stalled. Instead of manually assembling reports from multiple systems or validating patch status application-by-application, administrators can generate the evidence they need in minutes.

For many teams, that means spending less time proving that remediation occurred and more time focused on reducing risk. When leadership asks whether a critical vulnerability has been addressed, the answer no longer requires a spreadsheet, a ticket review, and a conference call. It requires one report.

The organizations most likely to succeed in the years ahead will not be the ones that discover the most vulnerabilities. They will be the ones that can consistently move software updates from identification to deployment without adding friction, administrative overhead, or unnecessary delay. Closing the scanner-to-fix gap requires more than visibility. It requires the ability to operationalize remediation at the same scale modern security programs identify risk.

References

¹ Verizon. 2026 Data Breach Investigations Report (DBIR). <https://www.verizon.com/business/resources/reports/dbir/>

² CISA. Known Exploited Vulnerabilities Catalog. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

³ CISA. Reducing the Significant Risk of Known Exploited Vulnerabilities (AA23-278A). <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>

⁴ SecurityScorecard. Global Third-Party Breach Report 2025. https://securityscorecard.com/wp-content/uploads/2025/03/SSC-Third-Party-Breach-Report_031225_03.pdf

⁵ Google Blog – Chrome Releases <https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html>



PATCH MY PC

About Patch My PC

In the age of artificial intelligence, attackers move faster than ever. Legacy patching processes can't compete. Patch My PC helps organizations automate third-party application patching in Microsoft Intune and Configuration Manager, so devices can be protected within hours of updates becoming available—not weeks or months later. Our curated catalog supports more than 3,300 apps, with white-glove PSADT support for custom and paywalled applications. Patch My PC works natively within your Microsoft environment, reducing manual effort, improving compliance visibility, and giving IT teams back thousands of hours each year without compromising security or operational stability.

Visit patchmypc.com to see how automated application updates can make your life easier.