vicarius

Why traditional Vulnerability & Patch Management are broken and what to do about it

*Checklist included

If you read one thing this week about how we manage risk in cybersecurity, let it be this. The way most organizations handle vulnerabilities simply doesn't work anymore. We're still relying on outdated tools, slow processes, and false confidence in periodic scans while attackers move faster, exploit known issues, and cause real damage. This isn't just inefficient. It's dangerous. I wrote this because I believe we need to rethink everything: how we detect, how we prioritize, and most importantly, how we fix. Quickly. If your team is still stuck in the old model, this piece is your wake-up call.

The old ways of managing vulnerabilities aren't working. Software flaws are being disclosed at an overwhelming pace over 30,000 in 2023 alone, averaging one every 17 minutes. But organizations are still patching far too slowly, leaving wide gaps for attackers to take advantage of. The consequences are clear: more breaches caused by issues we already knew about but failed to fix. Exposure management isn't just about identifying risks anymore it's about how fast you can act on them. And the traditional approach, built on scheduled scans and manual patching, simply can't keep up with the speed and complexity of modern environments.

The Rising Tide of Vulnerabilities (and Attacks)

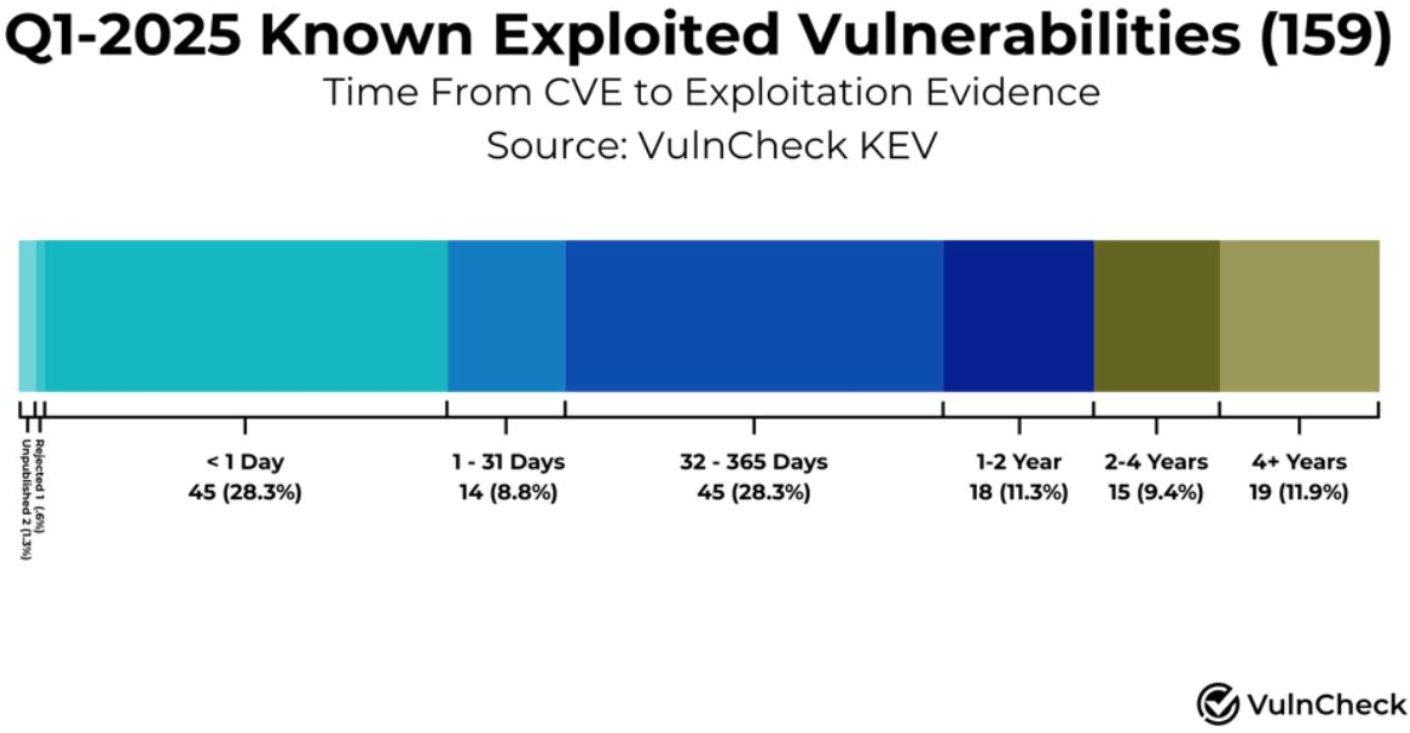
The volume of new software vulnerabilities has exploded. In 2024, over 40,000 CVEs were reported (a 17% jump from the year prior). We're on pace for nearly **50,000** in 2025, continuing an accelerating trend. This sheer volume creates an endless to-do list for security teams. It's simply unrealistic to "patch everything" when roughly a hundred new flaws emerge each day. In fact, one study found that half of businesses manage to patch only about 15% of their known vulnerabilities per month, a stark indication of how much falls through the cracks.

This wouldn't be so dire if attackers weren't quick to pounce on known issues. But they are. Analysts estimate that 60% or more of breaches involve known vulnerabilities that were never patched. Verizon's latest Data Breach report observed that attacks leveraging unpatched software nearly tripled in 2023, accounting for 14% of breaches (up from around 5% the year before). In other words, many threat actors don't need fancy zero-days, they simply exploit the lag in patching well-known flaws. We saw this vividly with the MOVEit file-transfer hack in 2023, where criminals exploited a published vulnerability faster than organizations could update their systems.

Why is this happening? Because **attackers have gotten faster, while defenders remain slow**. The industry used to talk in terms of weeks or months before a new vulnerability might be exploited. Now, that timeline has shrunk to days or even hours. Google's Mandiant team found that the average "time-to-exploit" a disclosed vulnerability plummeted from 63 days in 2018 to just 5 days in 2023. In early 2025, over a quarter of newly disclosed "known exploited" vulnerabilities showed signs of attack within 24 hours of publication. Some attacks have been observed **within minutes** of a CVE release. This is the reality: the moment a critical bug goes public (and especially once an exploit or proof-of-concept is released), the countdown is on.

By contrast, how fast do companies typically apply patches or mitigations? Sadly, much slower. **Average remediation times are still measured in months**, not days. For example, the median organization takes on the

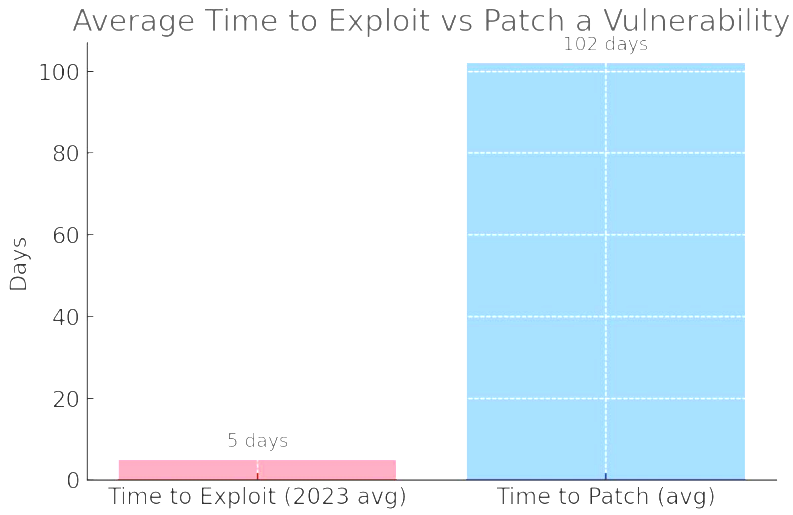
order of ~100 days to fully deploy a critical security patch. Even when glaring, high-severity flaws are known to be under active attack, most firms struggle to react quickly. A recent analysis of "known exploited vulnerabilities" (KEVs) found that even critical vulnerabilities that made it onto government alert lists still took a median of 137 days (4.5 months) to remediate. More than 60% of such known-exploited issues weren't fixed by the deadline set by CISA, the US cyber agency . These delays give adversaries a huge head start.



Q1 2025 data shows that nearly one-third of exploited vulnerabilities had evidence of attack less than 1 day after disclosure, emphasizing how quickly threat actors strike . Meanwhile, many organizations take months to roll out patches for critical flaws, highlighting the dangerous exposure gap.

The Remediation Gap: Attackers vs. Defenders

The sobering truth is that there is a **yawning gap between how fast attackers exploit and how slow defenders remediate.** Think of it as a race: today's hackers sprint ahead while many organizations are still stretching at the starting line. On average, cybercriminals begin exploiting a new vulnerability in a matter of five days or less. Yet the average enterprise doesn't patch that vulnerability for about three months. In effect, the bad guys have a 90+ day free window to do damage before the fix is in place.



*The typical timeline difference between exploitation and patching is staggering. Research shows attackers start exploiting a vulnerability within days , whereas organizations often need **~100 days** on average to fully deploy the patch . This "exposure window" is when breaches happen.*

Several data points illustrate this dangerous gap:

⚠ Mean time to exploit vs. patch

Qualys observed a mean time-to-exploit of ~44 days in 2023 , but newer intel from Mandiant showed many cases exploited in <1 week. By contrast, one analysis pegged average time-to-patch at 102 days for critical vulns . In other words, it can take **10× longer to patch than to exploit** a vulnerability. Little wonder that some exploits succeed before a patch even reaches all systems.

⚠ Exploitation often beats SLAs

Many organizations set internal SLAs of 30 or 60 days to patch critical issues. Unfortunately, attackers aren't so patient. A 2024 study found **75% of new vulnerabilities were exploited within 19 days of disclosure**, well before a 30-day patch cycle would even elapse. And **25%** of vulnerabilities were attacked on **Day 0** (the very day details became public) . Clearly, a monthly patch cadence leaves you exposed for weeks.

⚠ Slow detection and response

Even when attacks occur quickly, many firms don't notice or react until it's too late. Verizon's data shows the median time for organizations to even detect widespread exploitation of a known vulnerability is 5 days . That's five days the attackers have free rein. Meanwhile, the median time to remediate 50% of critical vulns (once a patch is out) was 55 days. These numbers paint a stark picture: by the time half your systems get patched, the adversary has likely already hit you (and moved on).

This "Remediation Gap", the delta between threat actors' speed and defenders' response is the heart of why traditional vulnerability & patch management is failing. It's not that security teams lack awareness of vulnerabilities; it's that the **process of fixing them is too slow and fragmented** to effectively reduce risk. Every extra day a known flaw remains open is a day it can be used against you. As one cybersecurity CEO put it bluntly: most vendors and programs focus on finding bugs, but "remediation...presents an even bigger challenge, since most teams are not well equipped to fix vulnerabilities quickly." Attackers have figured this out and are taking full advantage.

Why Traditional Approaches Fall Short

If we know the problem, why haven't organizations closed the gap? The issue isn't ignorance or apathy, it's that legacy vulnerability management practices weren't built for this level of speed and scale. Here are several ways traditional vulnerability & patch management is coming up short:

Siloed Tools “Find” vs “Fix”

Classic vulnerability management uses one set of tools to discover and assess vulnerabilities (network scanners, agents, etc.), and a completely separate set of tools to remediate (patch management software, scripting, manual ops). For example, a scanner like Tenable or Qualys might dump a report of thousands of findings, which then gets handed to IT to address with Windows Update, WSUS, SCCM, or other patch utilities. This handoff is where things break down. Security teams often **drown in scanner alerts and spreadsheets of CVEs,** while IT teams face an overwhelming patch queue without context of which issues truly matter. The result is alert fatigue on the one side and patch fatigue on the other, plenty of vulnerabilities identified, but far too many left lingering unaddressed.

Point-in-Time Assessments

Traditional vulnerability scanning is typically done periodically, perhaps weekly or monthly scans of the environment, or quarterly external scans for compliance. Patching is also often done in **fixed cycles (e.g. the infamous “Patch Tuesday” monthly routine)**. This made sense a decade ago, but it’s dangerously out of sync with today’s 24/7 threat landscape. A critical flaw disclosed right after your last scan might not be detected for days or weeks until the next scheduled run. Likewise, waiting for a monthly maintenance window to push critical patches gives attackers a huge runway. As one security analysis noted, attackers now operate at “breakneck speed, not in days or weeks, but within minutes” of disclosure . A weekly scan or a 30-day patch policy simply can’t keep up. Any approach that isn’t **continuous** leaves blind spots in the interim.

Lack of Risk Context

Legacy programs often prioritize purely by severity (CVSS scores) or by vendor advisories, without considering the real-world risk in your specific environment . This leads to misallocation of effort, teams scrambling to fix high-CVSS vulnerabilities that may not actually be exploitable, while overlooking lower-severity issues that are actively being used by attackers. for example, only a fraction of “critical 10/10” CVEs ever get weaponized. Conversely, many breaches start from vulns rated medium or low that were ignored. Traditional vulnerability & patch management often lacks intelligent **prioritization**. It doesn’t integrate threat intelligence (e.g. is there an exploit in the wild?), asset context (is this server business-critical or internet-facing?), or the likely impact. Thus, overwhelmed teams may fix a lot of “noise” and still miss the needle-in-haystack that becomes a breach.

Coverage Gaps

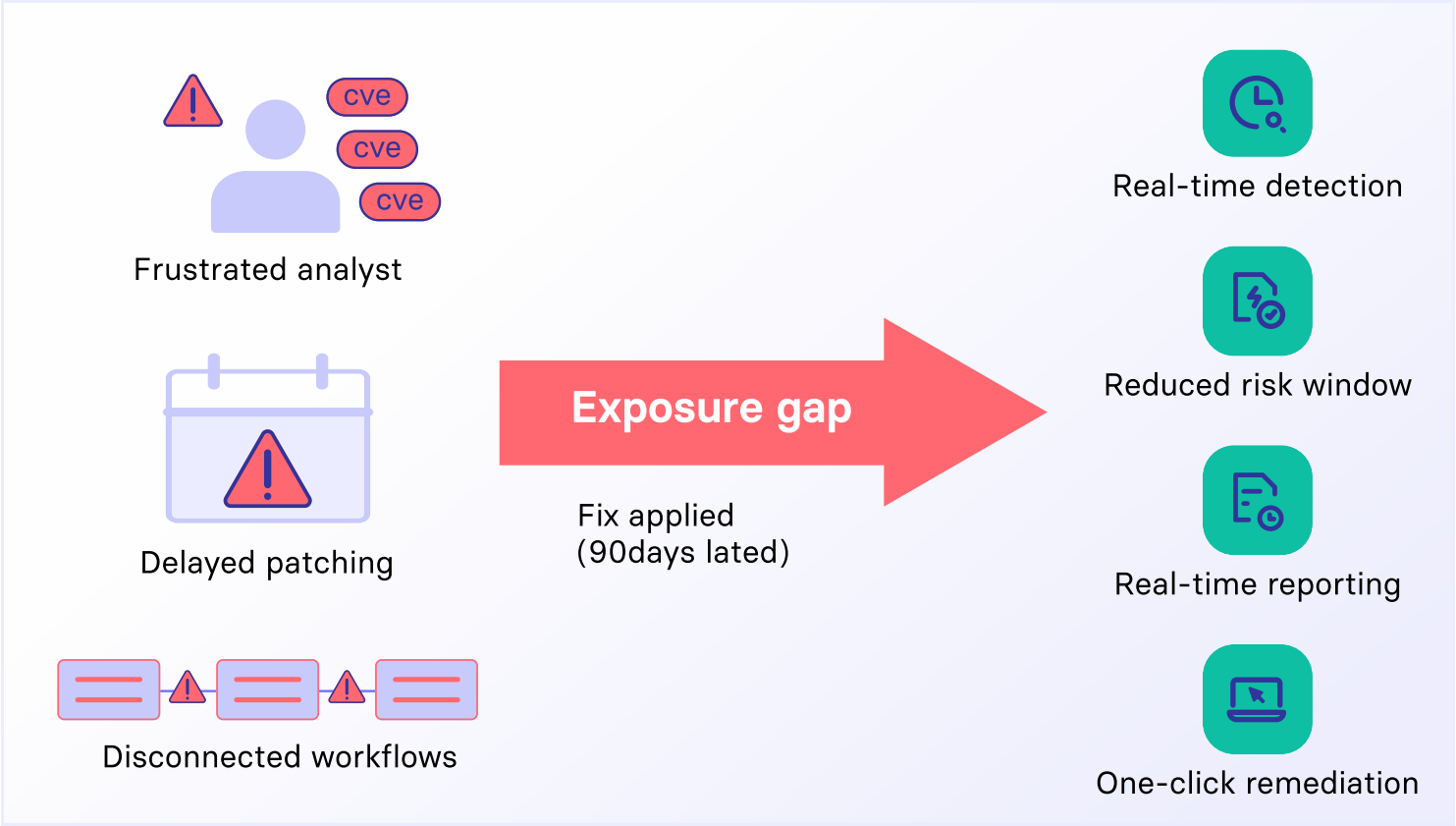
Another limitation is that older patch tools focus heavily on operating systems and maybe Microsoft applications, but leave **third-party and non-Windows software** under-patched. Many organizations have dozens of third-party apps (browsers, PDF readers, developer tools, etc.) that are full of vulnerabilities, yet their patch management might not handle those automatically. Similarly, if you have Linux, Mac, or IoT devices, legacy solutions might not support them fully. These gaps mean some systems stay outdated by default. Attackers will find those weak links. A single unpatched component (say, a VPN appliance or an open-source library) can provide a foothold for an entire network compromise.

Complexity and Process Bottlenecks

The traditional approach is **too manual and complex**. Coordinating between security (who finds issues) and IT (who applies fixes) introduces communication delays and sometimes politics ("can we take this server down for patching?"). Change control processes can stretch out the timeline. In many cases, organizations delay patches out of fear of downtime or breaking things in production, ironically accepting security risk to avoid operational risk. Some critical systems might be deemed "too important to patch" promptly, or teams insist on lengthy testing cycles. These real-world constraints mean even when a patch is available, organizations often **postpone it**, giving attackers a free pass . All of this adds friction and **inflates the mean time to remediate (MTTR)**.

The upshot is a perfect storm: more vulnerabilities than ever, faster attacker exploitation, and a legacy patch process that is too slow, siloed, and inconsistent. **Traditional vulnerability & patch management is like trying to fill a bucket with a huge hole in it**, no matter how many vulnerabilities you find, if you can't remediate them quickly and holistically, the risk keeps pouring out. As experts have noted, it's not the lack of scanning that's killing us, it's the lack of **rapid, orchestrated response**.

From Detection to Remediation: Closing the Exposure Gap



So what's the solution? The path forward is to fundamentally rethink vulnerability management as an end-to-end, continuous remediation process, rather than a periodic find-and-fix exercise. In practice, this means adopting new approaches and tools that emphasize speed, integration, and automation. Industry leaders and analysts are increasingly calling this model "continuous exposure management", a program that identifies exposures in real-time and rapidly addresses them to shrink that dangerous window of opportunity for attackers.

Key principles of a modern approach include:

Continuous Visibility

You can't remediate what you don't know about. Rather than relying solely on occasional scans, organizations need real-time asset and vulnerability visibility. This often involves lightweight agents or sensors that continuously monitor systems for new software, new vulnerabilities, and configuration changes. The moment a new critical CVE is disclosed (or a new app version is installed on a device), the team is alerted, not weeks later, but right away. By maintaining an up-to-date inventory of all assets and their exposure status, you ensure there are no blind spots or forgotten systems sitting unpatched . Continuous attack surface monitoring is the foundation for speed.

Integrated Prioritization

Modern exposure management flips the script from patch-everything to patch the right things first. This requires smarter analytics that weigh multiple factors: How critical is the affected system? Is the vulnerability being actively exploited or mentioned on exploit forums? Is there a known ransomware campaign targeting it? Is a patch available, and how easy is it to apply? Using such context, advanced platforms produce a risk-based ranking of vulnerabilities so teams can focus on the top threats that genuinely endanger the organization. This risk-centric approach cuts through the noise. It acknowledges that, with finite resources, speedy remediation of the riskiest 5% beats sluggish attempts to boil the ocean. Indeed, companies that implement risk-based vulnerability management have reported significant improvements, fixing high-risk issues faster while avoiding wasting effort on unlikely-to-be-exploited findings.

Unified Detection & Remediation Workflow

Perhaps the most transformative shift is moving away from separate scanning and patching silos to a unified workflow. In practice, this could mean using a single platform (or tightly integrated solutions) that identifies a vulnerability and allows one-click or automated remediation of that issue. For example, when a new critical vulnerability is discovered on a server, the system can immediately recommend the appropriate fix (patch, config change, script, etc.) and execute it or schedule it all within the same interface. This closes the loop instantly, without the delay of handoffs. Security and IT teams share one "pane of glass," seeing the same data and remediation status in real time . No more export to Excel, import to another tool, and hope for the best. By streamlining the process from detection to fix, organizations can shrink that exposure window from months to days or even hours.

Automation & Orchestration

With the volume of vulnerabilities and the speed required, automation is your friend. Leading organizations are implementing automated remediation playbooks policy-driven actions that trigger as soon as certain conditions are met. For instance, you might set a policy: “If a vulnerability with a known exploit is detected on an internet-facing system, auto-deploy the patch immediately (or isolate the system)”. Another example: “Auto-update any software that falls below a certain version with critical vulnerabilities.” This kind of automation ensures critical fixes aren’t waiting for the next weekly meeting or a human to click a button . It’s like having an extra team member who works 24/7 and never procrastinates. Of course, automation should be used judiciously with testing and fallbacks to avoid disruption but the technology today (from configuration management tools to modern patch platforms) makes safe automation very achievable. Some organizations have seen their mean-time-to-remediate drop by 50-80% after automating routine patching and deployment tasks.

Flexible Mitigation (“Virtual Patching”)

What about cases where you can’t patch immediately say, a vendor hasn’t issued a fix yet for a zero-day, or a critical system can’t be taken down right away? This is where virtual patching (a.k.a. vulnerability shielding) comes in. Virtual patching involves deploying a temporary security control that blocks exploitation of a specific vulnerability, buying you time until a permanent fix is in place . This could be a web application firewall rule that blocks malicious payloads targeting a web app flaw, or an endpoint security tool that detects and stops the exploit pattern in memory. Essentially, it’s a “shield” around the vulnerable component. Virtual patches don’t change the vulnerable code; they just prevent attackers from reaching it . This technique has become a crucial part of modern exposure management. For example, during the Log4j (“Log4Shell”) crisis, many organizations applied virtual patches via their IPS/WAF to fend off attacks while testing the official patches. **Patchless Protection** ensures you’re not defenseless during those gap periods when a fix isn’t yet available or can’t be rolled out instantly . It’s a key tool for resilience in a world of surprise zero-days.

Custom Scripting & Configuration Remediation

Not all fixes come in a neat vendor patch. Sometimes reducing risk means editing a configuration, disabling a vulnerable feature, or running a script to update something. Historically, security teams would file a ticket and someone might manually perform these changes on each system, a slow and error-prone approach. The new wave of remediation platforms include scripting engines and repositories of remedial actions that can be executed at scale. If a vulnerability requires, say, a registry tweak or turning off a service, the platform can push that script out to all affected endpoints in one go. Some cutting-edge solutions even use AI to generate custom remediation scripts on the fly for novel threats , allowing teams to respond faster than ever. By sharing and reusing these scripts (often vetted by the community or vendor), organizations dramatically increase their fix coverage beyond what off-the-shelf patches offer. This capability addresses the long tail of exposures that aren’t patchable in the traditional sense.

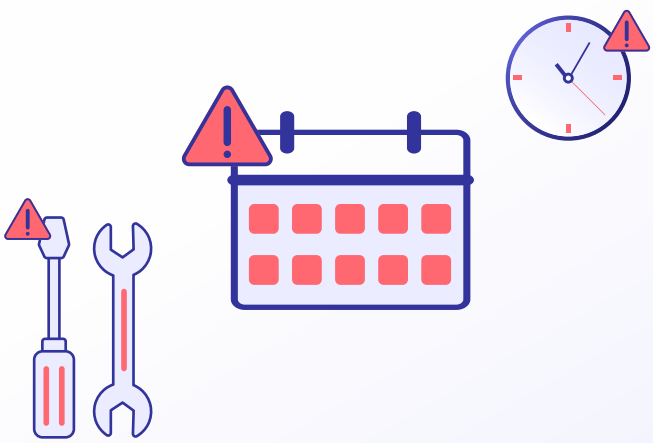
Real-Time Reporting & Metrics

Lastly, modern exposure management provides real-time insight into risk reduction. Instead of static quarterly reports of "X vulns found, Y patched," stakeholders can see live dashboards of their current exposure score, how many critical vulns remain open, and how quickly the team is remediating. Metrics like MTTR (Mean Time to Remediate) and patch compliance percentages become key performance indicators. Tracking these focuses the team on not just finding problems, but fixing them promptly . Executives and boards are increasingly asking for this level of accountability, especially as regulations and cyber insurance scrutinize vulnerability management practices. A unified platform makes it easier to demonstrate improvements for example, showing that after adopting continuous remediation, your average critical patch time dropped from 90 days to 15 days, or that your organization has **zero** high-risk exposures unaddressed from the latest CISA alert (an attainable goal with the right approach). In short, visibility and measurement drive action.

All of these elements work together towards a singular goal: shrinking the "exposure window" to as close to zero as possible. If you can detect a critical vulnerability today and remediate it (or mitigate it) today, attackers lose their advantage. This is how we break the current paradigm where they have weeks or months of free reign. It's worth noting that this isn't merely a theoretical ideal; many forward-looking organizations are already on this path. They are adopting what might be called a "Remediation Cloud" or unified vulnerability management platform that embodies these principles. Early adopters report dramatically reduced breach risk and major efficiency gains; one security team noted that by automating third-party app patching and integrating it with their scanner, they saved hundreds of hours of manual work and cut down their backlog by over 80%. Another organization using continuous auto-remediation proudly achieved patching of critical vulns within 48 hours across thousands of machines, a turnaround time that was unthinkable with legacy processes. These are the kinds of outcomes that make CISOs (and insurers, and regulators) sleep better at night.

Fix Faster, Fix Smarter

Traditional (slow)



Fast & Smart

Traditional vulnerability & patch management isn't keeping us safe in the modern threat environment. The old model of "scan on a schedule, then patch eventually" is too slow and too fragmented to counter attackers who weaponize new vulnerabilities in a blink. The approach is broken but it can be fixed. We must shift focus from finding everything to swiftly fixing the most dangerous things, from siloed tools to integrated platforms, and from manual steps to automated workflows. By embracing continuous, unified remediation, organizations can collapse the months-long gap between discovery and patch down to days or hours, drastically reducing their risk.

In essence, it's time to close the remediation gap. The organizations that do so will drastically limit the window of opportunity for attackers, turning what used to be an easy shot (a well-known unpatched flaw) into a much harder target. Those that cling to the old ways endless vulnerability scanning without rapid action will continue to play catch-up and suffer the consequences. The writing is on the wall, backed by hard metrics: speed is the new frontier in cybersecurity defense.

To protect our systems and data, we must make "Day Zero" patching a realistic objective, not an oxymoron. We need to empower our teams with tools that act like a tireless teammate, working 24/7 to remediate exposures as soon as they're found. By doing so, we flip the script on attackers. Instead of us racing to catch up with them, we force them to struggle against an environment that is self-healing, adaptive, and far less forgiving of their tricks. In the end, the organizations that fix faster and fix smarter will win and that is why the status quo of vulnerability & patch management must evolve, now. The cost of inaction is simply too high, and the attackers are not waiting.

Bottom line: It's not what you discover that matters most it's how fast you can remediate it. In cybersecurity, resilience comes not from avoiding every vulnerability (an impossible task), but from rapidly closing the window of exposure so threats have little room to operate. By reimagining vulnerability management with that end-state in mind, we can finally get ahead of the onslaught of vulnerabilities, instead of forever falling behind.

The Ultimate Checklist to Fix Traditional Vulnerability & Patch Management

Continuous Visibility

- [ ] Enable real-time discovery engine across endpoints, servers, cloud, OT
- [ ] Maintain auto-updating inventory of hardware, OS, apps, configs
- [ ] Stream CVE feeds directly into the live inventory for instant mapping
- [ ] Alert on any asset or software that drifts from approved baselines

Contextual Risk Analytics

- [ ] Correlate each CVE with exploit-in-the-wild and ransomware intel
- [ ] Tag assets by business impact, internet exposure, and owner
- [ ] Re-score risk daily so teams always see the critical top five percent
- [ ] Surface single-click risk overviews for executives and auditors

Policy-Driven Remediation & Patching

- [ ] Define policies such as critical internet-facing flaw → patch within 12 h
- [ ] Automate OS and third-party patch deployment with rollback safeguards
- [ ] Verify fixes through post-patch scans and close the loop in one console
- [ ] Track Mean Time to Remediate (MTTR) for every policy in real time

Shielding & Zero-Day Mitigation

- [ ] Apply virtual patching controls when vendor fixes are unavailable
- [ ] Document compensating controls and set expiry reminders
- [ ] Validate shield effectiveness with exploit replay or red-team tests

Custom Script Automation

- [ ] Maintain peer-reviewed remediation script library under version control
- [ ] Use the platform's scripting engine to auto-generate or run fixes at scale
- [ ] Capture success and failure metrics for every script rollout

Integrated Telemetry & Health Monitoring

- [ ] Monitor agent health, patch status, and policy compliance continuously
- [ ] Alert on failed deployments, drift, or rising MTTR before SLAs slip

Unified Analytics & Reporting

- [ ] Track MTTR, exposure windows, compliance drift, automation ROI live
- [ ] Auto-generate executive, auditor, and tenant-level reports on schedule
- [ ] Expose analytics via open API for BI and board dashboards

Seamless Integration & Orchestration

- [ ] Sync vulnerability and patch data with SIEM, ITSM, SOAR, and CMDB
- [ ] Trigger tickets or playbooks automatically when remediation policies fire
- [ ] Feed closed-loop status back to asset and configuration databases

Governance, Process, and Culture

- [ ] Set 24-hour triage and seven-day remediation SLAs for critical CVEs
- [ ] Embed emergency change paths for hotfixes without red tape
- [ ] Run monthly tabletop exercises simulating Day-Zero disclosure
- [ ] Tie team incentives to risk-reduction metrics, not ticket volume