2025 Exposure Management Index

Breaking down trends in cybersecurity exposure management with insights from 3,000 organizations and our team of security experts.

intruder

Introduction

For everyone but the largest, most well resourced of enterprises, the security challenge is often structural. They face the same vulnerability landscape as expansive multinationals but with fewer resources, smaller budgets, and leaner teams. Growth often takes precedence over governance, leaving leaders forced to balance the pressure to scale with the risk of exposure.

2025 has shown how exposure emerges from multiple fronts. AI-assisted development has created new risks as engineering teams rush vibe coded outputs into production without sufficient review. Rapid cloud adoption continues to deliver agility but also introduces a host of new potential attack vectors for bad actors to exploit. Shadow IT – unapproved or unknown tools and services that exist without security oversight – can expose sensitive data and expand the attack surface. And small vendors, often part of critical supply chains, remain attractive entry points for attackers seeking leverage over larger organizations.

These risks are made evident by the September 2025 European airport disruptions and the attack that brought Jaguar Land Rover's production lines to a standstill. The RediShell vulnerability, meanwhile, highlights the risks of inadvertently exposing assets to the internet and underpins the necessity of attack surface reduction.

Cyber security is no longer a luxury reserved for large enterprises – access to effective solutions and actionable knowledge is essential for all. This first edition of the Intruder Exposure Management Index is part of that effort. By analyzing data from thousands of customers, Intruder aims to give small and midsize companies the threat landscape insights that have historically been locked behind enterprise budgets and external consultants.

While large enterprises have the scale to manage complex security stacks, smaller organizations often need unified, accessible platforms that bring essential security tools together. This report highlights where that need is most acute, where responses are improving, and where gaps remain.

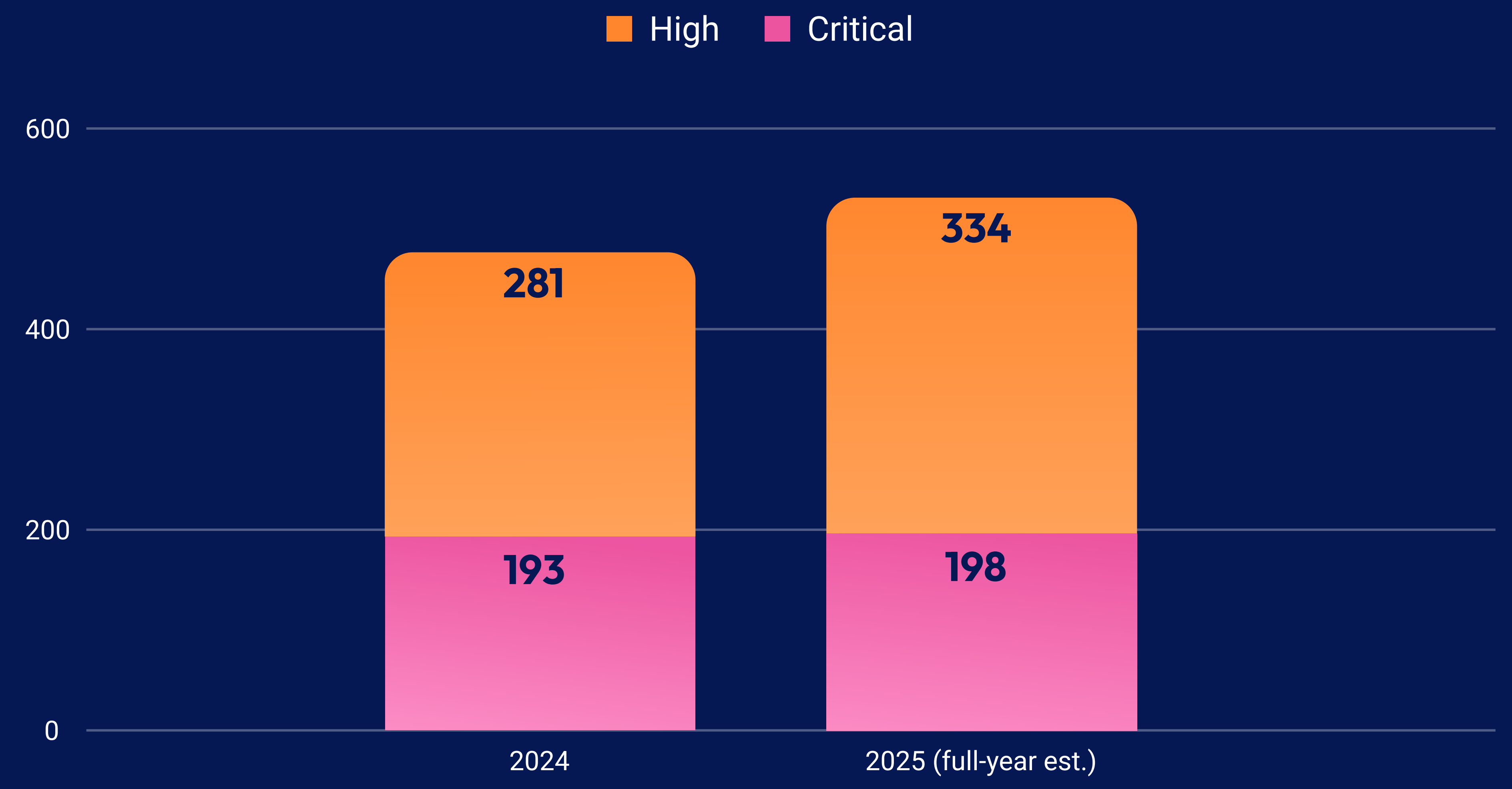
The 2025 Vulnerability Response Index tracks how 3,000+ small and midsize companies (1-2,000 employees) are exposed to security vulnerabilities, how and why their responses vary, and what can be learned from those patterns.

Trends in vulnerability detection & response

Criticals remain stable, but highs are on the rise

The average number of newly identified critical vulnerabilities per organization is trending on par with 2024, but the volume of high-severity issues is nearly 20% higher.

Average number of identified high and critical issues



A worsening threat environment.

While a stable number of criticals mean teams aren’t necessarily fighting more fires than they were a year ago, they are being forced to prioritize a meaningfully higher volume of high-severity issues. This expansion is no doubt influenced by attackers reaping the benefits of generative AI in developing exploits. In the wider threat landscape, volumes of both critical and high severity CVEs have surged year-on-year, and are on track to finish the year 28% and 34% higher respectively.

More pressure on already stretched teams.

19% more high-severity vulnerabilities mean that security and engineering teams have 19% more things to worry about, but chances are headcount isn’t keeping up with the expanding threat environment. Scalable security solutions are needed to help lean security teams manage this gap.

AI-driven weaponization of "old" CVEs

Old CVEs are the new zero-days.

In 2025, attackers have increasingly focused on exploiting long-known weaknesses – vulnerabilities disclosed one, two, or even three years ago but still left unpatched in many environments.

AI is increasing attackers' pace.

Writing new exploits for older CVEs has become easier and faster, with AI-assisted coding lowering the technical barrier to developing reliable attack methods.

Beware of ghosts in your back catalog.

This acceleration means the "back catalog" of vulnerabilities is being weaponized at a rate not seen before. For defenders, the effect is that yesterday's weaknesses remain today's active threats, and a failure to remediate older issues continues to present a real risk.

Exposed infrastructure remains especially attractive.

Security appliances such as SSL VPNs, firewalls, and identity providers are deliberately internet-facing and often central to access control. When these systems are vulnerable, exploitation is widespread and highly damaging.

> **We are seeing the back catalog of CVEs and vulnerabilities being weaponized with increasing frequency.**
>
> **Andy Hornegold,**
> VP of Product at Intruder

Critical issues are being fixed faster

Executive attention.

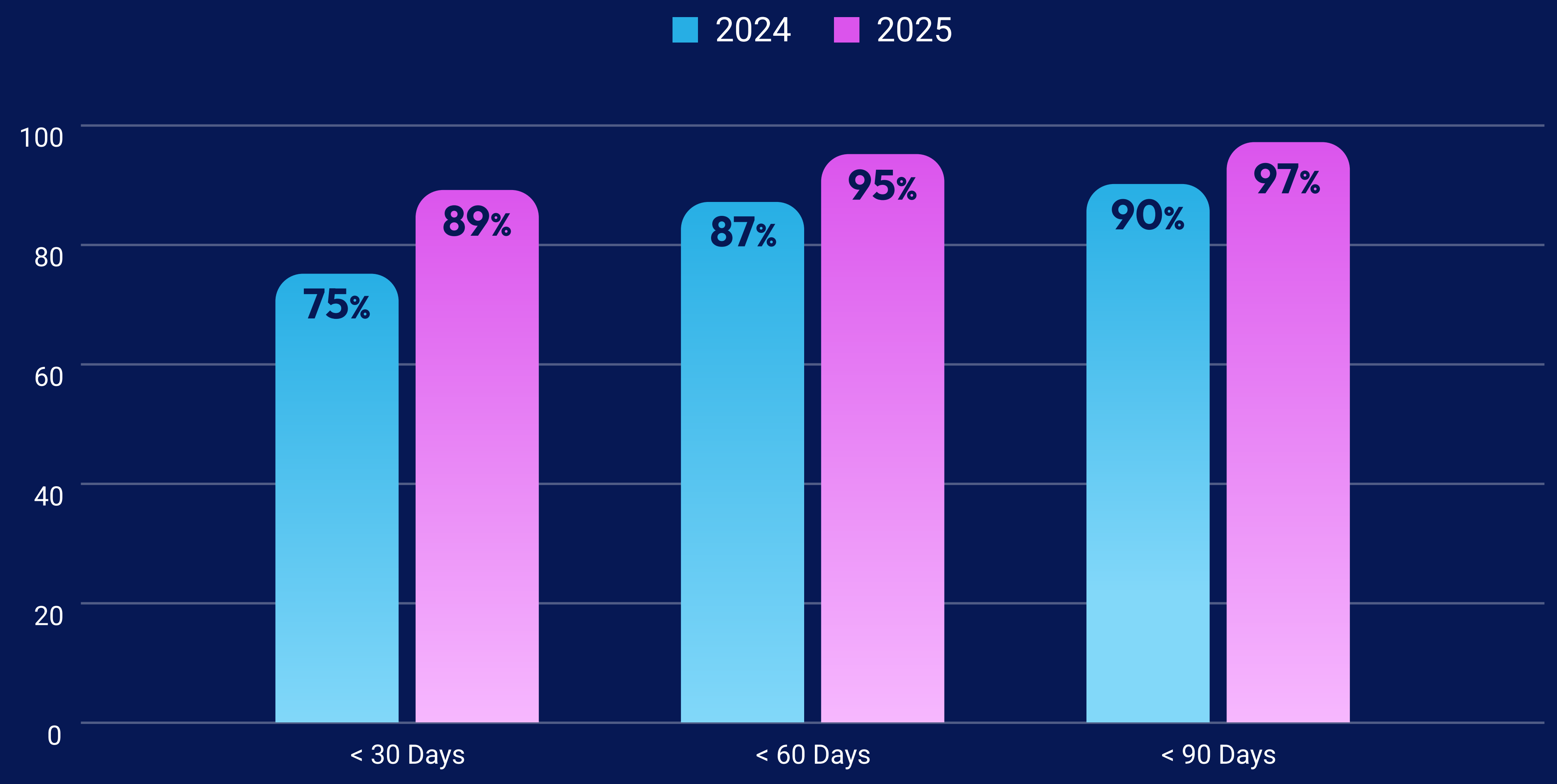
High-profile incidents in 2025 appear to have made the cost of delay harder for organizations to ignore. Disruptions to healthcare services, supermarket supply chains, and consumer brands in retail and automotive kept cyber security in the headlines and on boardroom agendas. When leaders see the impact of cyber risks clearly, remediation of critical issues tends to receive more focus.

Technology and process deliver speed.

Improved year-on-year remediation times suggest that as security processes and technology stacks mature, the organizational capacity to respond quickly to critical issues improves. Any good exposure management solution should provide actionable remediation advice that any engineer can follow and integrations with workflow tools that streamline processes and reduce time to fix.

In 2025, 89% of critical vulnerabilities identified have been remediated within 30 days, up from 75% in 2024. North America saw average remediation times improve from 37 to 16 days. High severity vulnerabilities are also being fixed faster.

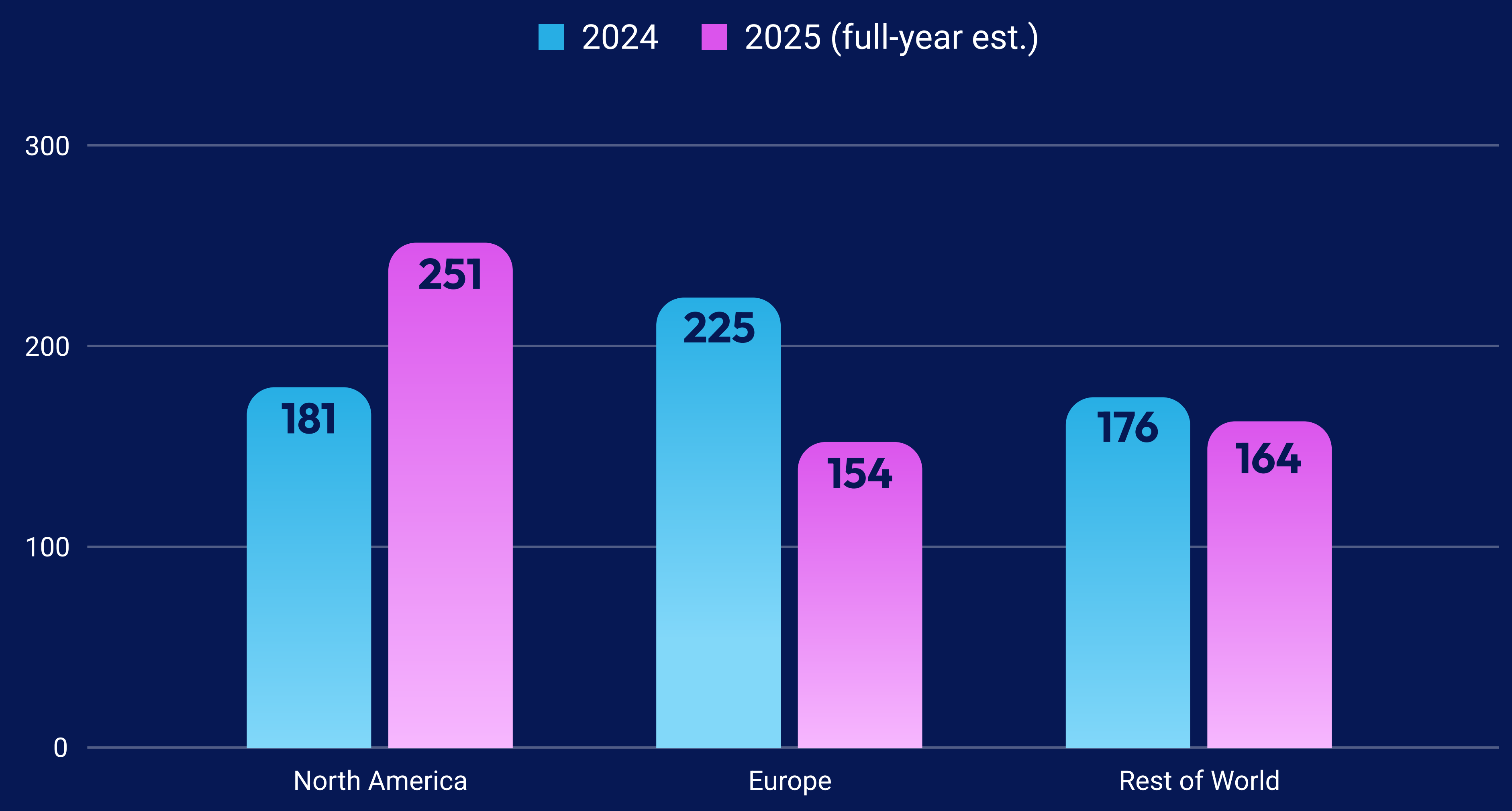
Critical vulnerability remediation times 2024 vs. 2025



Early signs of the regulatory impact in Europe

In a reversal from 2024, European organizations are forecasted to register an average of 100 fewer critical vulnerabilities than their North American counterparts this year.

Average number of identified critical vulnerabilities by region



Avoiding criticals.

European businesses are outperforming when it comes to avoiding critical vulnerabilities. The average European company is forecasted to have 100 fewer than their North American counterparts this year. While Europeans perform well on criticals, it's not all good news. They experienced considerably larger volumes of high-severity issues in 2024 (423 vs. 248), and the gap is widening further in 2025.

Regulation driving cyber hygiene.

Proponents of regulatory frameworks such as DORA, NIS2, and the Cyber Resilience Act are likely to be optimistic about the downward trend in identified critical vulnerabilities in Europe where the regulatory environment is most developed. While it is too early to declare a definitive trend, the data provides an indication that these regulations may be having the desired effect on cyber hygiene and resilience. The true impact remains to be seen in the months and years to come.

Size matters: large estates bring risk and delays

Small companies with less than 50 employees fixed issues nearly twice as fast as medium-sized business (51-2,000 employees) in 2024, but 2025 data shows this gap is closing.

Average critical vulnerability remediation time (days)

	2024	2025
< 50 employees	20	14
51-2,000 employees	38	17

Contending with complexity.

Larger, older estates contain more heterogeneous systems, legacy applications, and bespoke integrations. More infrastructure means more to patch, and older systems add layers of complexity and risk.

Agility wins.

Smaller organizations can act with agility, whereas larger enterprises must often navigate organizational structures, ticketing systems, approvals, and testing cycles before a change can be made. The result appears to be slower remediation even when vulnerabilities are well understood.

Separation of “find” and “fix”.

Security teams can discover and triage issues but cannot patch them. Remediation depends on infrastructure, DevOps, or product engineering teams, and each handoff introduces friction. The larger the organization, the more these bottlenecks slow remediation.

Software sector remediates fastest

Buyer pressure.

Enterprise customers often require evidence of security maturity before purchasing, such as regular penetration tests, SOC 2 certification, and SSO aligned with zero-trust policies. SaaS vendors adapt early to meet these expectations.

Modern infrastructure.

Cloud-centric environments, particularly common amongst software startups, can rollback and redeploy more quickly, reducing the friction of patching and configuration changes. This makes remediation easier than in some other sectors.

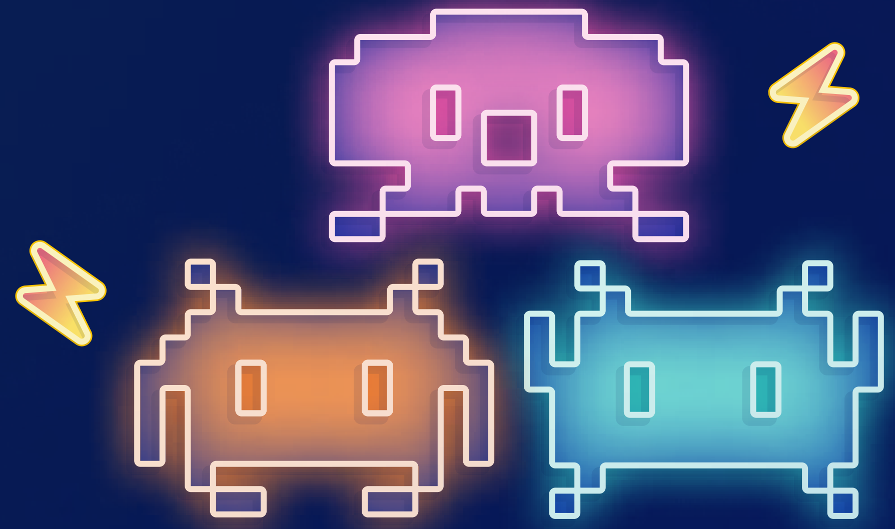
Sector specific realities.

It's no surprise to see financial services and healthcare near the top of the industry ranking table given the sensitive data being processed by these organizations, the associated compliance requirements and high security expectations of customers.

In 2024, financial services led the way with an average 14-day remediation time for critical vulnerabilities, however this has risen to 22 days in 2025. Software companies are showing strong year-on-year improvement, reducing average fix times from 24 to 13 days.

Average critical vulnerability remediation time (days)

Industry	2024	2025
Diversified financials	14	22
Software	24	13
Healthcare services	20	22
Professional services	29	21



Vulnerabilities of the year

Not every vulnerability is equal

Thousands of CVEs are published each year, but only a fraction become the focus of widespread exploitation or present serious, real-world impact. Intruder's security team identified the five vulnerabilities that stood out most in 2025.

Selection was based on three factors:

1. **Prevalence across environments**
2. **Likelihood of exploitation**
3. **Real-world impact**

In some cases, these were weaknesses with high technical severity and mass exploitation. In others, they represented recurring patterns of vendor error or categories of exposure that defenders consistently struggle to address.

This is not an exhaustive list of every high-profile CVE, but a view of the issues that shaped the threat landscape most for small and midsize organizations.

> **Assessing the threat environment is not just about what vulnerabilities are most common. The probability of exploit and potential consequences are equally important factors to consider.**
>
> **Dan Andrew**
> Head of Security

5. Apache Tomcat RCE

(CVE-2025-24813)

What it is:

A remote code execution flaw in Apache Tomcat, rated CVSS 9.8.

Why it mattered:

This was the single most commonly occurring critical CVE across customer estates from 2025. Its high severity, combined with the broad prevalence of Tomcat, made it one of the top exposures of the year, affecting a wide range of organizations – a classic example of an impactful, widely distributed application vulnerability.

4. Fortinet Perimeter Vulnerabilities

(CVE-2024-55591 & CVE-2025-32756)

What they are:

An authentication bypass in FortiOS (CVE-2024-55591) and a critical flaw in FortiVoice (CVE-2025-32756). Both affect internet-facing Fortinet appliances.

Why they mattered:

Fortinet has seen a string of critical vulnerabilities across multiple product lines over the past 18 months. These incidents underscore why edge appliances remain such high-value targets: they are internet-facing, widely deployed, and hold the keys to network access. For most enterprises, changing vendors in response isn't realistic – the cost and disruption are too high – leaving fast patching and compensating controls as the only viable defenses.

Fortinet was not the only major edge device vendor to be hit by a wave of vulnerabilities in 2024 and 2025. It would be remiss not to mention Ivanti, who was also affected by numerous critical vulnerabilities over the same period.

3. Apache mod_rewrite RCE (CVE-2024-38475)

What it is:

A vulnerability in Apache HTTP Server's mod_rewrite module (versions 2.4.59 and earlier) caused by improper output escaping. It allows attackers to map URLs to filesystem locations that should not be directly accessible, leading to potential code execution or source code disclosure.

Why it mattered:

Despite being disclosed in 2024 – and our most commonly observed CVE of that year – the number of vulnerable instances still present highlights the continued relevance of this threat in 2025. Its persistence shows how widely deployed web server modules remain attractive targets, and how quickly attackers incorporate reliable application-layer bugs into their exploitation toolkits.

2. Palo Alto Auth Bypass

(CVE-2025-0108)

What it is:

An authentication bypass in the web management interface of Palo Alto Networks' PAN-OS firewall.

Why it mattered:

This vulnerability was actively exploited in the wild and highlights a recurring theme: incomplete fixes. Protections introduced after a prior authentication bypass (CVE-2024-0012) proved insufficient, and attackers found new ways to abuse how different technologies (Apache, Nginx, PHP) process requests. When authentication controls on management interfaces fail, attackers gain an immediate foothold in security-critical devices.

1. ToolShell (CVE-2025-53770)

What it is:

A critical remote code execution flaw in Microsoft SharePoint, exploitable without authentication.

Why it mattered:

ToolShell stood out in 2025 because it was a perfect storm. It offered reliable, unauthenticated remote code execution on systems that are often perimeter-exposed and tightly integrated with Active Directory. Exploitation required little sophistication, and Microsoft releasing details on a Saturday left teams without an out-of-hours SOC at a disadvantage. To make matters worse, there was a gap between disclosure and patch availability – a window attackers quickly took advantage of. For many organizations, failing to patch within days meant they were already in a post-exploitation scenario. Vulnerabilities this impactful, reliable, and easy to exploit don't come along often!

Looking forward

Remediation improves when accountability is shared across teams, and when engineers - not just security teams - have the tools to act.

The 2025 data underscores a consistent theme: speed matters, but so does focus. Attackers are exploiting older vulnerabilities with new efficiency, while defenders are learning to act faster when exploitability is clear.

For small and midsize organizations, the lesson is not to chase every CVE, but to prioritize the ones that matter most: internet-facing systems, older flaws with fresh exploit code, and vulnerabilities flagged as likely to be targeted.

External pressure has proven effective, whether from regulators in the EU or enterprise buyers demanding stronger controls. But urgency does not need to wait for mandates. The organizations reducing risk fastest are those that embed exposure management into their normal operations, shorten the path from detection to validated fix, and ensure responsibility sits with those who can remediate directly.

The vulnerabilities highlighted in this report are not outliers – they are representative of the pressures all defenders face. Closing the gap between exposure and remediation is possible if defenders focus on context, collaboration, and continuity.

About Intruder

Intruder's exposure management platform helps lean security teams stop breaches before they start by proactively uncovering attack surface weaknesses. By unifying attack surface management, cloud security, and continuous vulnerability management in one intuitive platform, Intruder makes it easy to secure your entire infrastructure — from apps and APIs to cloud accounts and employee devices. Designed to cut through the noise and complexity, Intruder enables teams to discover exposed assets, detect misconfigs, prioritize real risks, streamline security workflows, stay compliant, and fix issues fast.

Founded in 2015 by Chris Wallis, a former ethical hacker turned corporate blue teamer, Intruder was selected for GCHQ's Cyber Accelerator and is now protecting over 3,000 companies worldwide.

Start a free trial or book a call with one of our experts at intruder.io

★★★★★

Read our reviews on G2.com