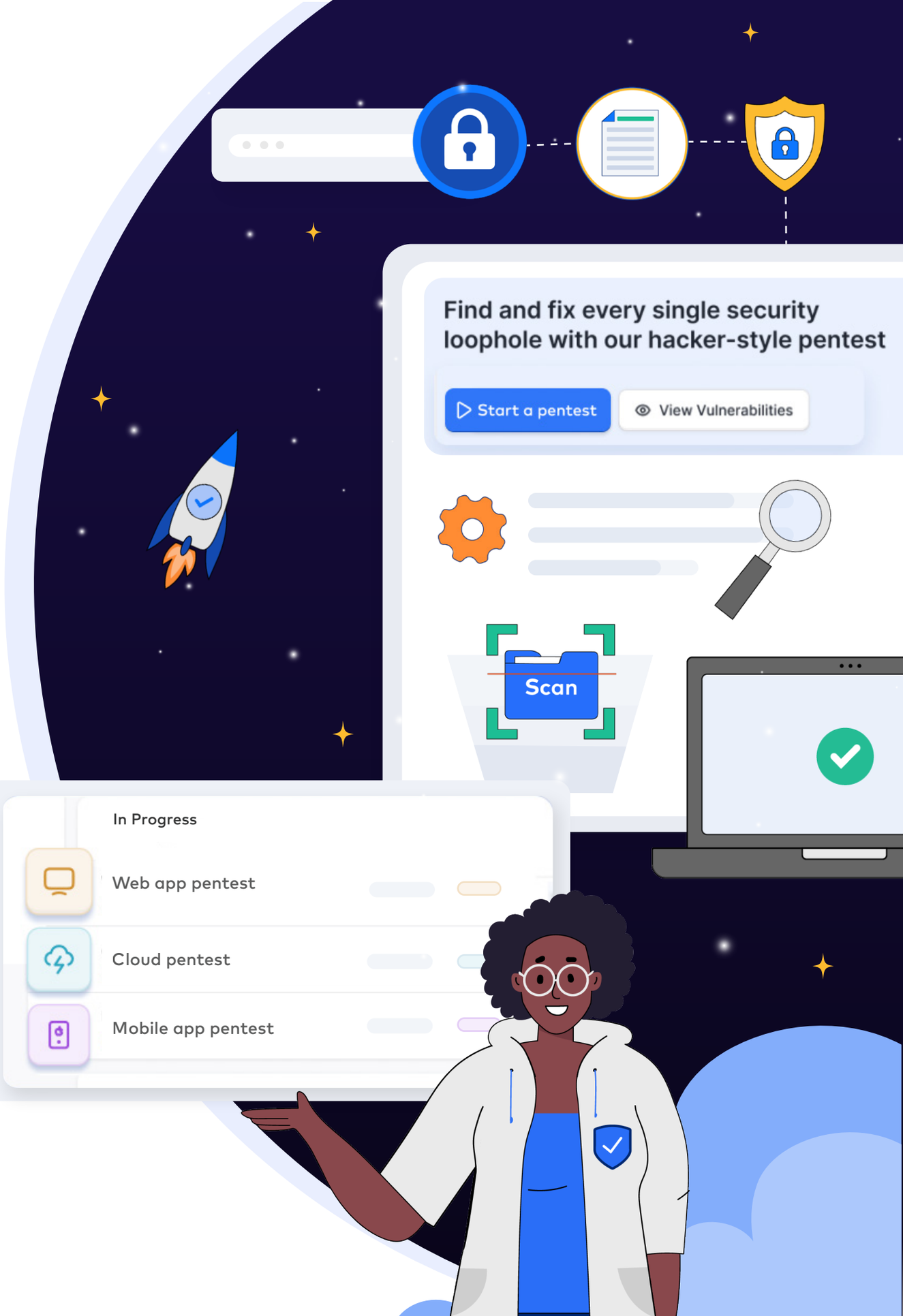
astra

State of continuous pentesting report 2025

Built in the trenches. Backed by data. For the boardroom.



Astra Security

Foreword

Security is no longer just about protecting assets but ensuring trust and continuity in a world of digital interdependence.

Rapid advancements in artificial intelligence, the growing reliance on third-party software, sweeping shifts toward cloud-first strategies, and an ever-expanding attack surface have created a perfect storm. Combined with persistent resource constraints, they have left CXOs grappling with difficult trade-offs between protection, progress, and shipping timelines.

While valuable, traditional penetration testing is no longer sufficient to address modern threats' scale, complexity, and velocity. The foundation of robust cybersecurity has evolved to prioritize proactiveness, continuity, and automation.

Emerging methodologies, such as CTEM and PTaaS, exemplify this shift by leveraging AI-powered insights to deliver round-the-clock visibility and operational scalability, focusing on safeguarding data, business continuity, and reputation.

While numerous reports and analyses exist, our unique vantage point as a trusted partner to over 800 companies offers invaluable insights and real-world lessons. Instead of reiterating existing information, we aim to add depth and clarity to the conversation.

We address critical areas such as the evolving threat landscape, the role of automation in modern defense, and balancing resource constraints with security priorities. Grounded in experience, we offer a practical, actionable lens to empower organizations to evolve from reactive defense to proactive resilience.

More importantly, this report is more than a data summary; it reflects our collective journey through an era of rapid transformation. By combining granular insights with a broad analysis of the SaaS security landscape, we aim to foster meaningful dialogue and drive informed decision-making. Let's build a more secure future together.

Cheers,
Shikhil and Ananda

Looking ahead

1 Introduction

It may be 2025, but cybersecurity is still stuck in a state of 'survival.' Over 62%[1] of professionals reported burnout last year—an unsurprising consequence of chasing zero-tolerance security in an environment that refuses to cooperate.

The sheer velocity of emerging vulnerabilities, magnified by automation, resource constraints, and the unpredictability of AI-driven threats, has stretched security teams to their limits. Yet, the fundamental question remains: Are we making meaningful progress, or are we just patching faster than we break?

Reflecting on the past year, the nature of cyber threats hasn't necessarily evolved—it has compounded. Attackers aren't reinventing the wheel; they're optimizing & automating it with persistent legacy vulnerabilities and/or escalating supply chain attacks while organizations remain locked in an exhausting cycle of reactive security.

Worse, security investments often follow the latest breach headline rather than grounded vulnerability intelligence with proper business-contextualized prioritization. This results in an ROI model that looks effective on paper but falls apart in practice.

Critical performance areas are either overlooked or misaligned, widening the gap between security efforts and actual risk reduction. Meanwhile, the financial impact of breaches continues to climb to several billion, challenging CTOs to justify security investments as tangible ROI rather than compliance checkboxes.

Thus, this report goes beyond summarizing breach statistics and vulnerability trends to examine the state of cybersecurity and pentesting as an industry—where it excels, where it falls short, and how security teams must recalibrate for the coming year.

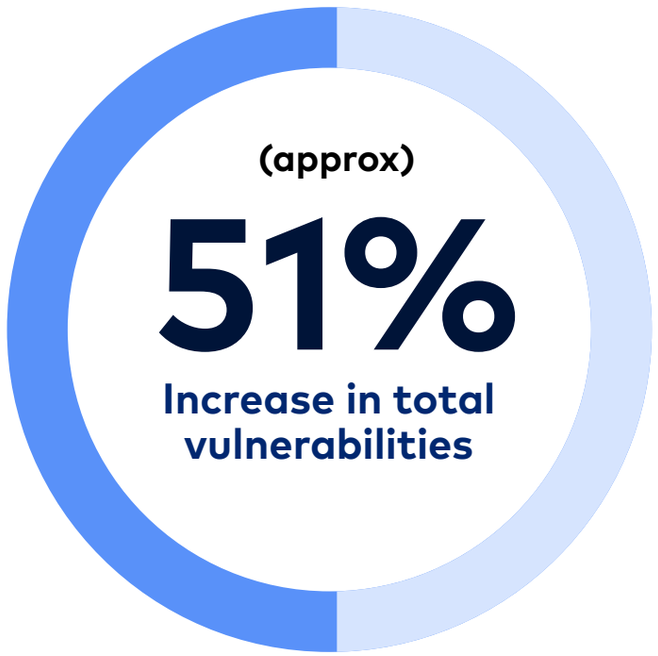
With Attack AI reshaping attack surfaces and defensive strategies, the road ahead demands a shift from traditional "point-in-time" security to an integrated, continuous approach. The goal is not just resilience but evolving, predictive, yet proactive security—a model where pentesting isn't a periodic audit but a living, breathing component of an organization's defense.

> *Security is increasingly shifting to the hands of developers, while security teams find themselves more overwhelmed than ever.*
>
> 
>
> Ananda Krishna, Co-founder and CTO, Astra.

1. *https://www.darkreading.com/cybersecurity-careers/persistent-burnout-is-still-a-crisis-in-cybersecurity*

2 Executive summary

01 Total vulnerabilities



02 Total CVEs reported in 2024

91

03 Manual pentest increase

48%

04 Automated web scans conducted in 2024

126%

05 Automated pentests surged

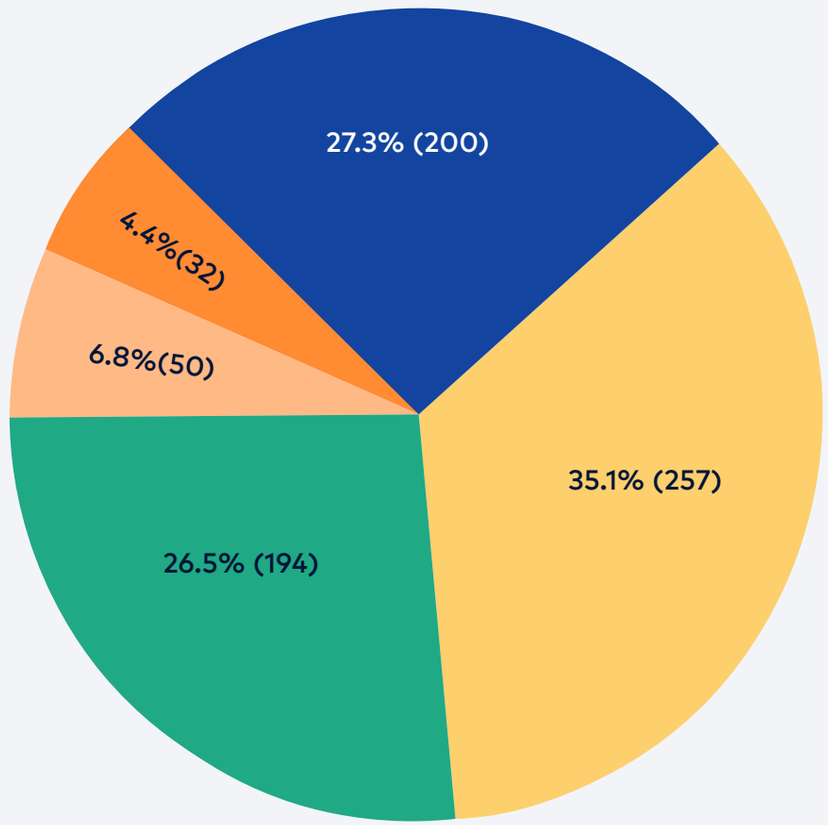
2.5x

06 Last year at Astra, we uncovered 5.33 vulnerabilities per minute across all tests

6a. 4.87/min via automated scanning

6b. 0.46/min through manual pentesting

07

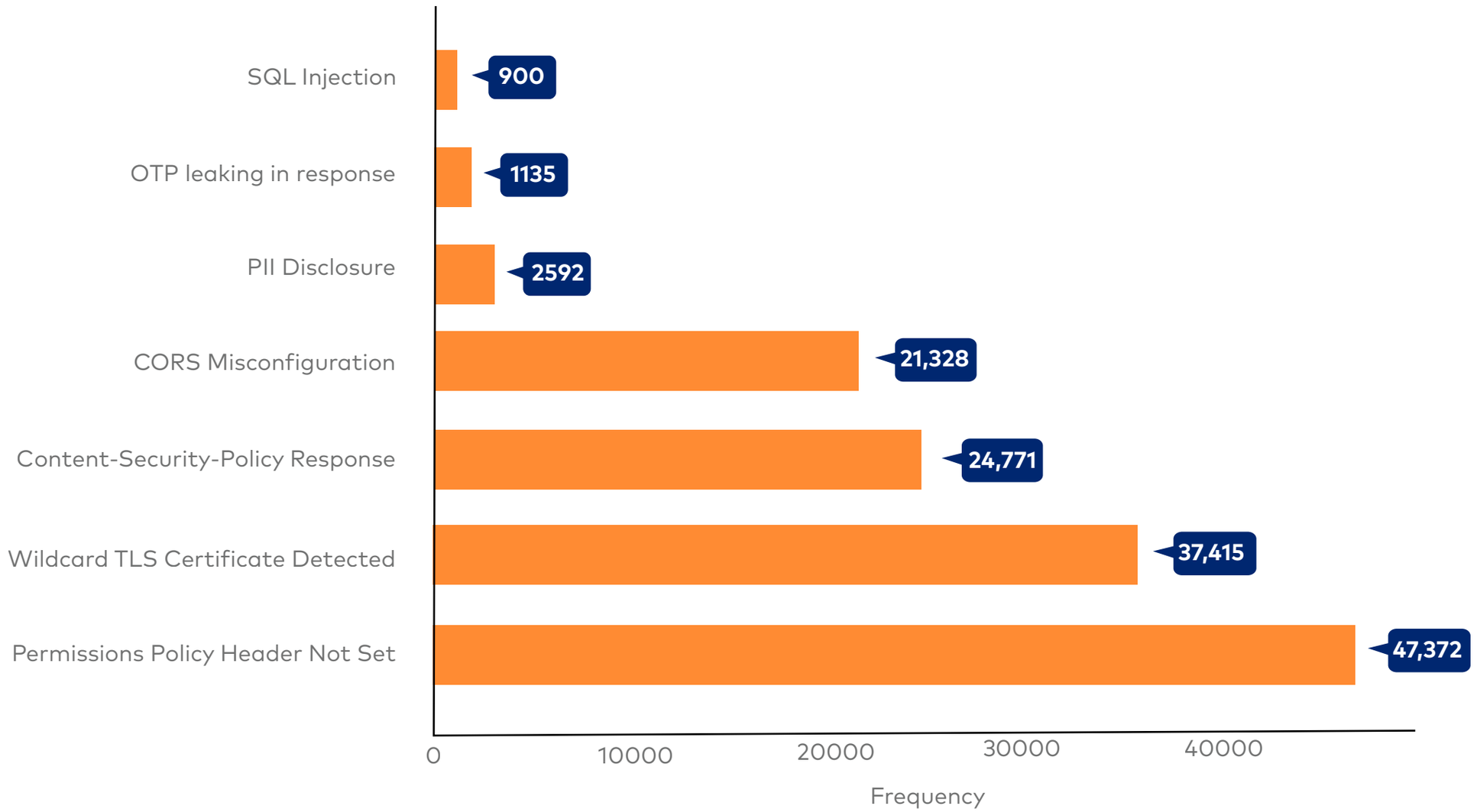


Market demand by company size (Last 30 months)

- Growing Business
- Small Business
- Mid-Market
- Large Company
- Enterprise

Executive summary

08 Most commonly recurring vulnerabilities



Executive summary

09 Potential losses saved

Asset Type	Number of Issues	Average Potential Loss	Total Potential Loss
Web	476,738	$ 1,212.36	$ 266,194,887
API	3,614	$ 1,444.06	$ 2,044,792

10 Total potential loss prevented by automated pentests

$2.89 billion

11 Cost saving 2023 vs 2024

2024	$ 1,677,512,914	Cost savings (automated)
	$ 105,511,606	Cost savings (manual)
2023	$ 473,098,791	Cost savings (automated)
	$ 53,630	Cost savings (manual)

3

The threat landscape - key learnings and outlook

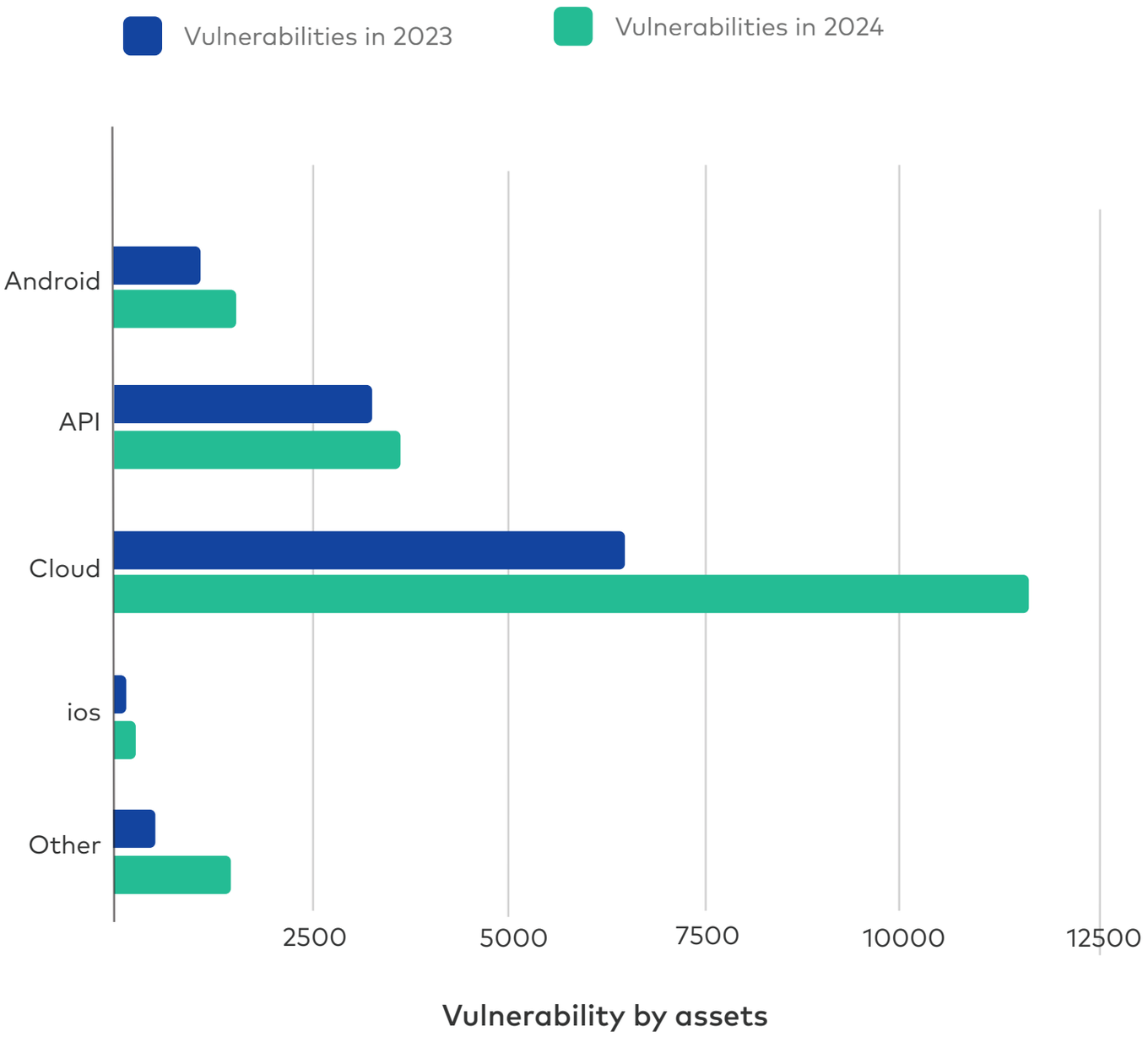
The cybersecurity threat landscape has undergone a seismic transformation, with 2024 marking a sharp rise in vulnerabilities - a 50.86% increase in vulnerabilities when compared to 2023 across automated vulnerability scans and manual pentests by security engineers.

As the environment grows in complexity, the evolving interplay between attackers and defenders continues to reshape security strategies. The 50.86% increase doesn't merely illustrate an expanding attack surface but signals a deeper shift in adversarial tactics and defensive responses, setting the stage for what's to come in 2025.

Peter Merkert,
CTO, Retraced

With the rise of autonomous services and applications, security responsibilities are shifting further upstream in the supply chain. Similar to debates around regulating AI LLM creators rather than users, this trend highlights the need to secure foundational layers. While most cloud services are managed or even autonomous—often ensuring up-to-date security patches—this shift raises complex questions about accountability and risk ownership.

Emerging trends in the threat landscape



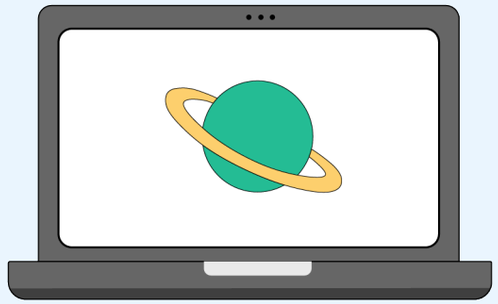
Web dominance: Still the largest target

Your security is only as strong as your weakest link—for most, that's their web application. In 2024 alone, web applications accounted for over 96% of all discovered vulnerabilities, with staggering security flaws.

As businesses increasingly adopt cloud-native infrastructures, microservices, and interconnected APIs, the attack surface today isn't just growing—it's introducing new layers of risk.

However, we often treat web security as a standalone concern instead of the **symbiotic relationship** with cloud infrastructure, APIs, and mobile services. In 2025, these boundaries are blurring even further, making security gaps more fluid across environments.

Simply put, weaknesses in one inevitably spill over to others, i.e., comprehensive vulnerability management will hinge on a deeper understanding of these interdependencies and a shift toward more unified security strategies.



A deep dive into assets

Cloud security: Growth and opportunity

Cloud vulnerabilities have surged nearly 1.8X in the past 12 months, yet their relative share remains modest at 2-3%. If this trajectory continues, we may see cloud vulnerabilities evolve at a similar pace, potentially reshaping the threat landscape further.

The current data hints at a future where, despite rapid cloud adoption, security measures—combining in-app tools and external pentesting—continue to mature. Though this signals progress, today's modest share of cloud CVEs shouldn't be mistaken for stability. Misconfigurations and weak IAM will likely remain significant threats in the year(s) ahead.

Simply put, providers like Amazon, Microsoft, and Google secure the underlying infrastructure under the shared responsibility model and offer robust security tools. Still, any rise in vulnerabilities in the coming years will fall squarely on users.

Ultimately, cloud security is not Amazon's, Microsoft's, or Google's problem—it is yours.

APIs: The unseen vulnerability

APIs are quickly becoming the new "**First Point of Failure**" in cybersecurity. While the overall number of vulnerabilities saw a slight uptick in 2024, their share of total CVEs dropped. But don't be fooled by the numbers; in 2025, **APIs are the backdoor to your data.**

Moreover, automated security tools often zero in on web applications, leaving APIs under-tested. Today, if you aren't rigorously testing your APIs, attackers will.

The rapid growth of microservices and serverless architectures continues to unleash a flood of APIs, increasing complexity and risk. **Broken object-level access control, exposed endpoints, and weak authentication** are emerging as hackers' preferred entry points in 2025.

Jayesh Singh Chauhan
Founder, Cloudurance Security & Cloud Village

Security is more of a people problem than a technology problem. Persistently creating a security culture within the org brings an amazing amount of long-term benefits.

Mobile security: Small, but growing

As mobile-first applications continue to grow in importance, mobile vulnerabilities are expected to rise in tandem. The 2024 surge in vulnerabilities —where Android apps saw a **45%** and iOS experienced a **110%** surge —is likely to be a precursor to a similar upward growth in the coming year as the reliance on mobile devices, particularly among younger generations, deepens.

Most importantly, applications today don't operate in isolation; they rely on cloud infrastructure and APIs, which means a vulnerability in a mobile app can quickly escalate into a larger security issue or vice versa.

The Automation Factor

Not all vulnerabilities are equal

Remember, much of the vulnerability discovery process is driven by automated tools focusing primarily on web applications. While these tools are invaluable for scaling vulnerability discovery, they tend to miss vulnerabilities in other asset types, particularly mobile and API.

Simply put, though the number of web vulnerabilities is overwhelming, the vulnerabilities in other areas—fewer in absolute terms—should not be underestimated.

The severity factor

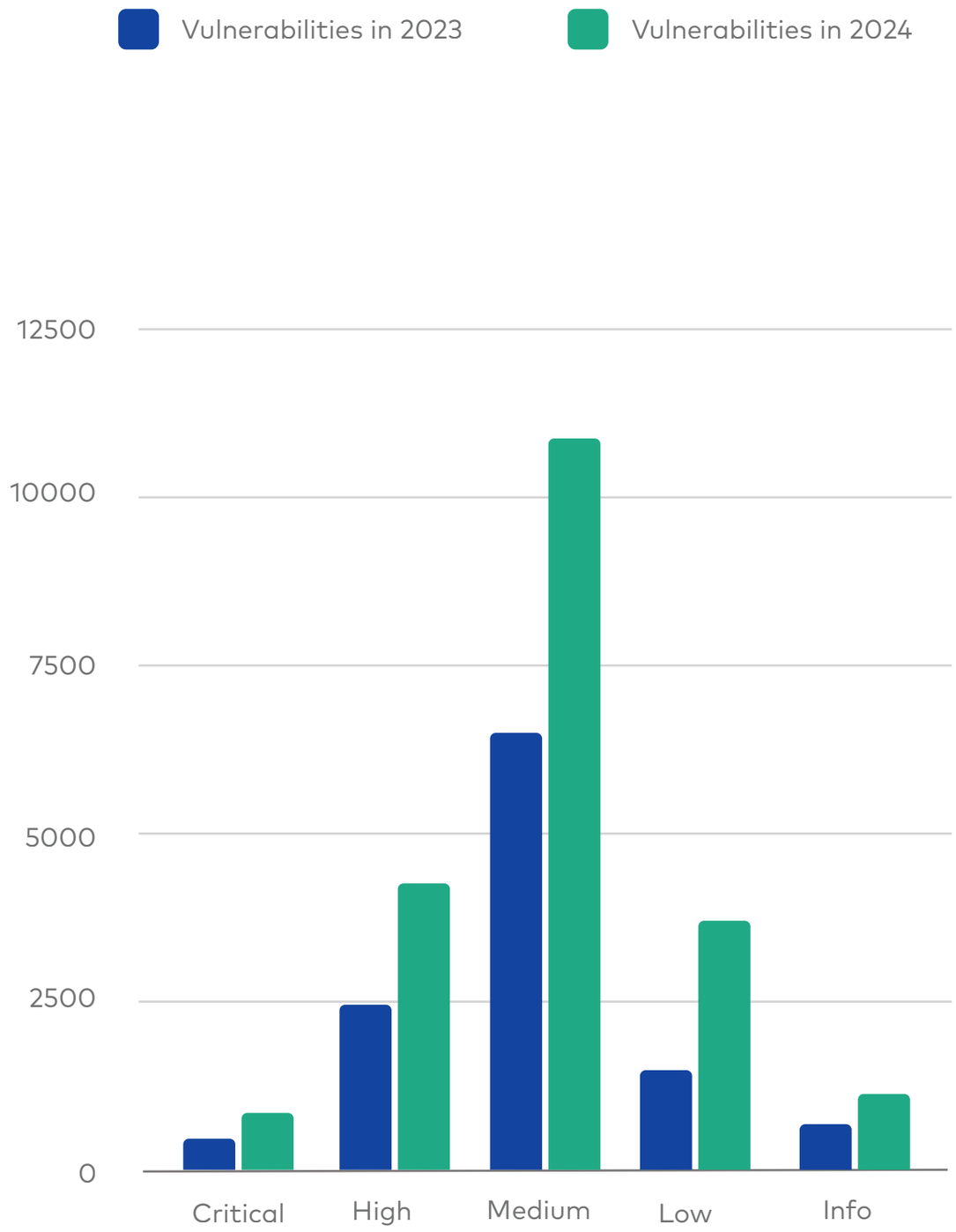
The **83% surge in critical vulnerabilities** in 2024 signals a clear trajectory: Attacks are becoming more precise, opportunistic, and damaging. Authentication failures, misconfigurations, and poor access control aren't just security lapses—they are now core attack vectors shaping the next wave of breaches.

Despite making up only 5.34% of total vulnerabilities, these high-impact flaws will disproportionately drive security incidents in 2025—faster, more catastrophic ones. The reality is simple: Attackers aren't just finding vulnerabilities but refining their approach to maximize impact.

The growing tension between speed and security is now a critical fault line. A **66% rise in high-severity vulnerabilities** in 2024 wasn't an anomaly—but the result of rushed deployments, insecure APIs, and poor patching hygiene. Organizations continue to scale without security-first thinking, and that gap is widening. If the same pattern persists, 2025 will be the year when poor security debt finally comes due, with costly consequences.

Medium-severity vulnerabilities, up 80% in 2024, remain the most common foothold for attackers—they don't trigger panic, which makes them perfect for long-term exploitation. The industry's habit of de-prioritizing these vulnerabilities has already proven risky. In 2025, expect attackers to double down on chaining these flaws together for deeper access and prolonged system compromises.

The 158% jump in low-severity vulnerabilities is, perhaps, the most underestimated risk. Security teams often dismiss these flaws, but attackers don't. Combined—like a weak input validation flaw with improper session management—they create attack chains capable of full-scale exploitation. If organizations keep ignoring the compounding impact of these "low-risk" issues, 2025 will be the year those small cracks become massive breaches.



The CVE breakdown

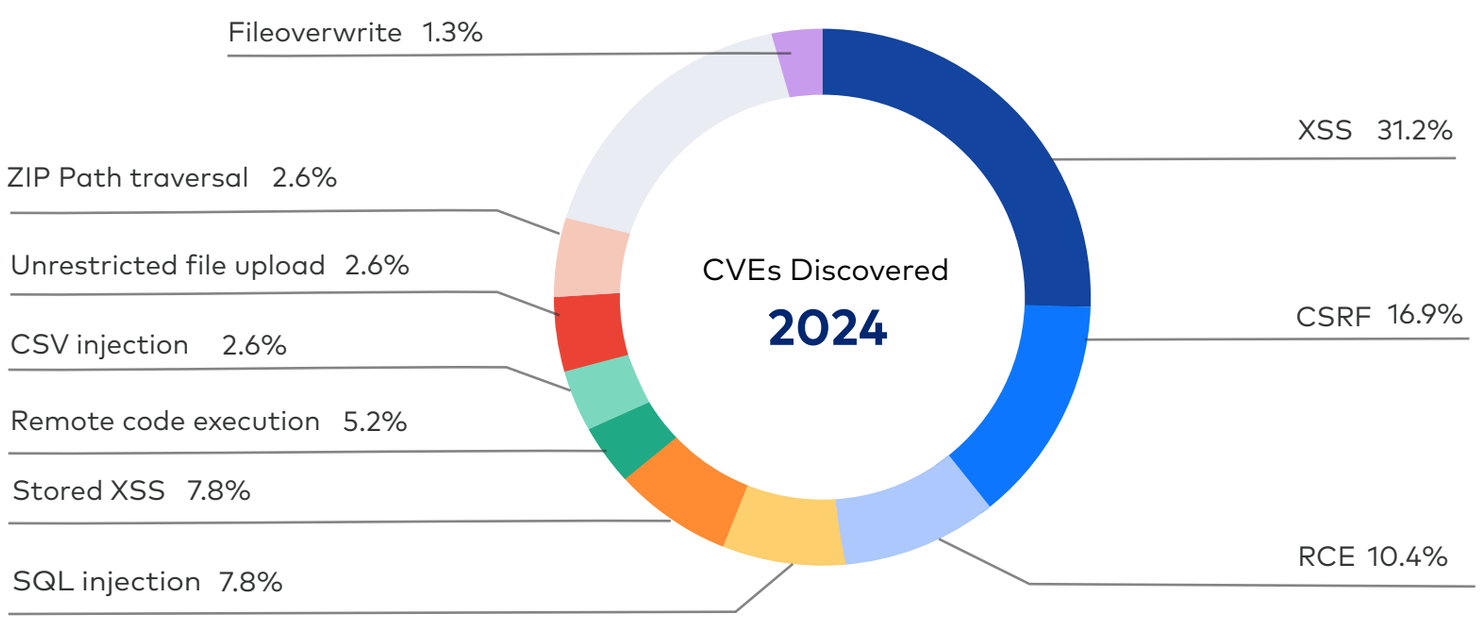
The CVE data from the past year signals a clear trajectory—attackers are becoming more precise, targeting high-value weaknesses with increasing sophistication. **Astra reported 90+ CVEs** in the last 12 months alone, which, while modest compared to the sheer volume uncovered through pentests and automated scans, highlights the vulnerabilities attackers are actively exploiting.

WordPress plugins and CMS were at the center of these attacks, particularly as chained exploits became more prevalent. **Cross-Site Scripting (XSS) led with 31%**, a stark reminder that user input fields remain a persistent weak spot despite years of mitigation efforts.

CSRF and RCE followed with nearly 17% and 10%, respectively—trust vulnerabilities that continue to offer attackers a direct route to manipulating user actions and executing remote code on critical systems.

SQL Injection and stored XSS remained stubbornly challenging to eradicate, exposing persistent gaps in secure coding and vulnerability management. Defenses that rely on legacy best practices alone are proving insufficient; attackers aren't slowing down, and if businesses don't catch up soon, the gap between offense and defense will only widen.

Even at the current rate, 2025 won't just see more of the same; it will demand a shift in how security teams approach prevention.



Reading between the numbers

Your security is only as strong as its weakest link—and attackers exploit the gaps defenders overlook. While security teams categorize risks into web, API, and cloud, attackers chain them. A misconfigured API can expose cloud data just as a weak web app can open doors to an entire infrastructure.

Thus, web apps dominate reports, but are they the biggest risk or just the easiest to find?

- **96%** vulnerabilities in web apps, **$266M losses**
- **$2M+** API vulnerability losses, BOLA a top threat
- Cloud threats up to **1.8X,** IAM misconfigurations lead
- ‘Permissions Policy Header Not Set’ a widespread CVE in web apps

“

There is an alarming rise in API-related breaches, mainly because APIs are now at the core of modern applications. Security teams struggle to keep pace with engineering velocity, especially where shift-left security is not well integrated. Discovery and API inventory of both exposed and internal APIs continues to be a persistent problem. Web apps remain a primary attack vector, especially with the increasing complexity of single-page applications and third-party integrations.
In fact, in the SaaSified world, integration is becoming a crucial trust boundary.

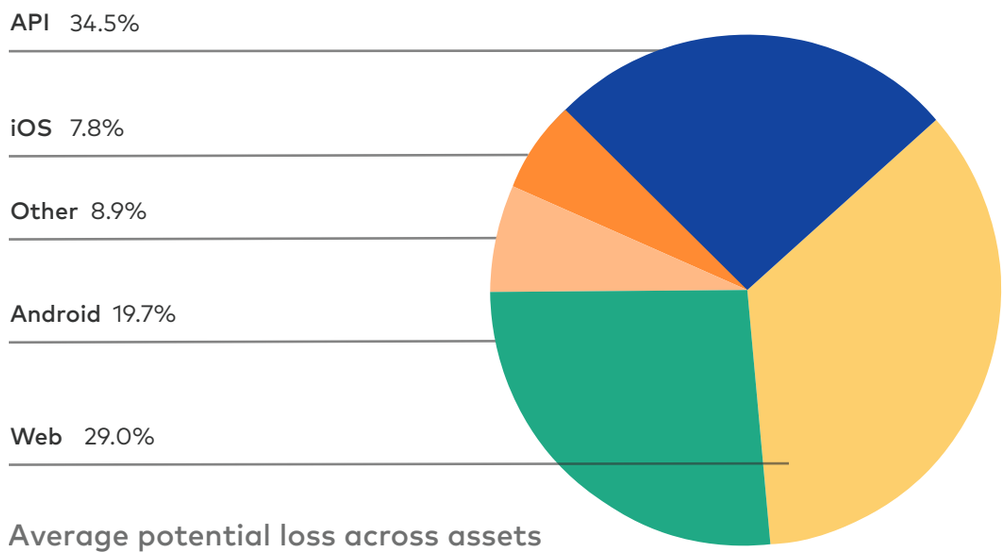
Cloud misconfigurations continue to be among the top 3 vectors of breach, as per the IBM Cost of Data Breach report.
The common thread across all three planes is the need for hygiene/foundational engineering practices, the need for a 360-degree observability stack, and the need for continuous security testing & monitoring.

Suhel Khan, Head of Cyber Security, Chargebee

4 Rise in vulnerabilities: The numbers that matter

Among the vulnerabilities detected, the **nearly 2000x** rise in those found through manual pentests highlights both the evolving sophistication of cybercriminal tactics and the advancing depth of defender detection capabilities. If the past 12 months are any indication, two undeniable forces will shape the cybersecurity landscape in 2025:

- **Advanced Attack Techniques**—Attackers now leverage sophisticated methods, such as exploiting zero-days or targeting intricate misconfigurations. This indicates a shift toward more complex and nuanced attack strategies that chain existing attacks.
- **The Crucial Role of Manual Testing** – The rise in unique vulnerabilities emphasizes the necessity of human-driven testing. Manual pentests remain essential in identifying context-specific vulnerabilities that automated tools often overlook.



Average potential loss across assets

Cost savings

The economics of VAPT are shifting fast. In 2024 alone, automated testing delivered **$1.68 billion in cost savings**, proving how much these tools have advanced efficiency and impact. Manual pentests, while narrower in scope, still **saved over 19 times** more than the previous year, reinforcing a critical truth: Automation is scaling, but human expertise remains indispensable for exposing high-risk vulnerabilities, especially in cloud and API security.

This isn't just about hypothetical risk; the financial stakes are real. The most expensive breaches prevented last year stemmed from persistent vulnerabilities like AWS Access Key exposure, where a single leak could cost **$100,000**, and SQL Injection, a top-tier critical threat. (Explored further in The Financial Impact.)

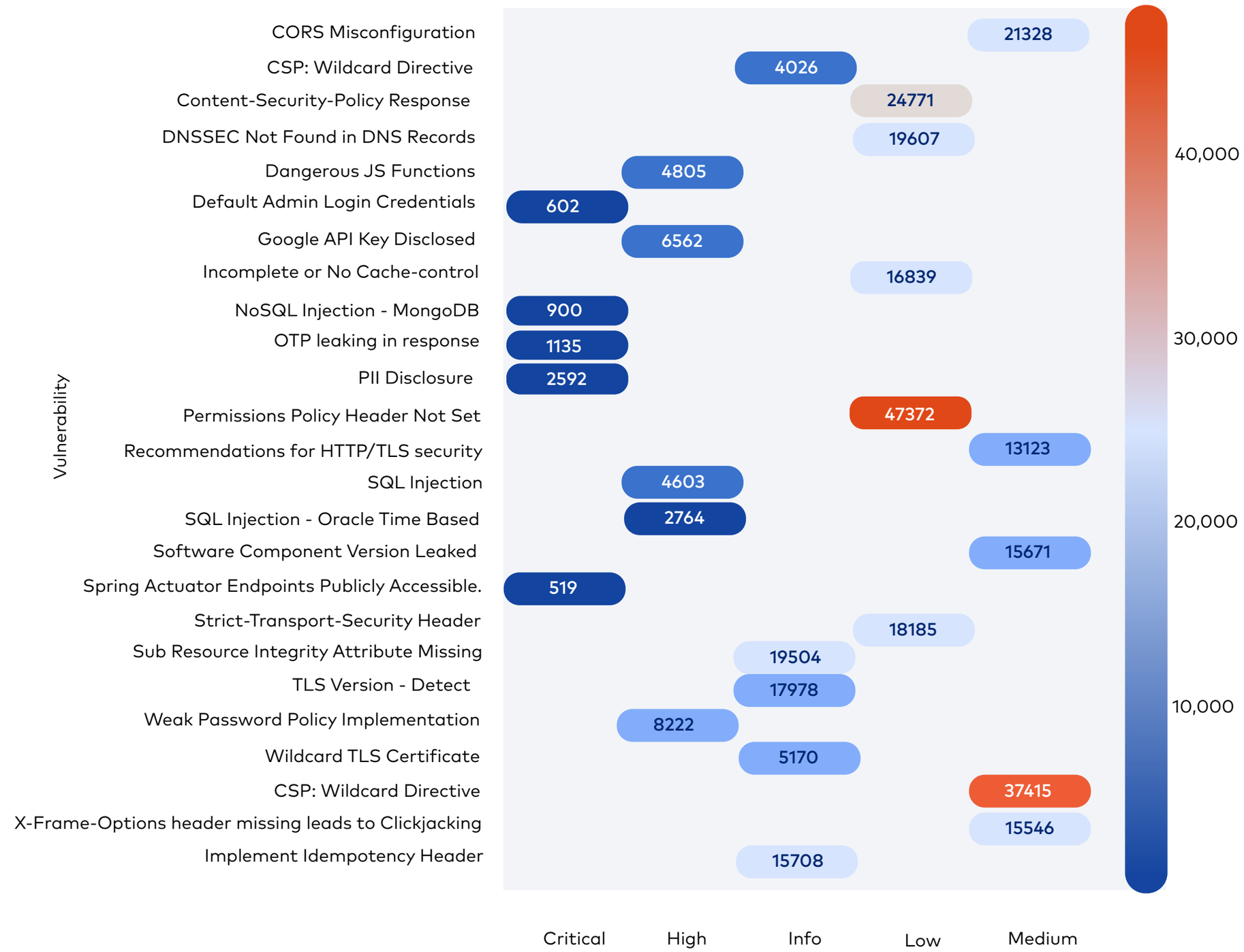
Zoom out, and a pattern emerges—web vulnerabilities continue to dominate, accounting for $266 million in potential losses, while APIs contribute another $2 million. If 2024's trajectory continues, these numbers won't plateau, and businesses relying on outdated or one-off security checks will set themselves up for failure.

In 2025, the organizations that prioritize continuous testing will be the ones that stay ahead—both financially and defensively. Security isn't just a cost center; it's a strategic investment. The alternative? Mounting financial risk and reputational fallout.

Scaling detection in a complex environment

The **219.41% surge** in automated web scans in 2024 isn't just a response to expanding attack surfaces—it's a shift in how security is approached. Continuous monitoring is no longer optional; it's the new baseline. If vulnerabilities keep emerging at the same pace, 2025 won't be about finding gaps but keeping up with them.

With vulnerabilities already uncovered in millions, the sheer scale of exposure is impossible to ignore. Permissions Policy Header Not Set and Wildcard TLS Certificate Detected dominated in volume (nearly 85K+ instances), while critical flaws like PII Disclosure, OTP leaking in response, and NoSQL Injection - MongoDB highlight an unsettling reality: security debt isn't shrinking but accelerating.



Reading between the numbers

Your vulnerabilities aren't new—attackers just wait for you to ignore them. The data doesn't just show growth; it shows intent. While security teams debate testing frequency, attackers have become more strategic.

Instead of flooding networks with low-hanging exploits or lasering in on high-severity CVEs, they are chaining overlooked low and medium-severity vulnerabilities into pathways for high-impact breaches. If this continues, the challenge in **2025** won't be foreseeing an attack—it will be recognizing the groundwork for the one already in motion.

- Vulnerabilities discovered in **2024** grew by **50.86% YoY**
- Manual pentests saw a nearly **2000% increase**
- Automated web scans surged **219%**
- **High-severity vulnerabilities are up 83%**, signaling a focus on critical exploits

> *Although, open-source tools support testing various types of assets, choosing the right paid vulnerability scanners in combination with open-sources tools for your asset goes a long way in helping you stay ahead of vulnerabilities and be compliant towards various standards.*

Prateek Kuber, Information Security Analyst, Astra Security

5 AI, automation, and pentesting

AI in cybersecurity is an enigma wrapped in a hype. Vendors promise next-generation automation, and threat actors allegedly use AI-driven attacks. Yet, when you strip away the marketing, one truth remains: breaches keep happening.

Security teams continue to struggle, not because they lack AI-powered tools but because they lack certainty about which threats matter, which vulnerabilities pose a real risk, and which remediation strategies will withstand evolving attack techniques.

Attack AI represents a critical evolution in offensive security whereby artificial intelligence moves beyond defense and becomes an active asset in attack tooling —to autonomously identify vulnerabilities, generate exploits, and scale social engineering with speed and precision.

While they may be leveraged ethically by red teams or maliciously by threat actors, the outcome is the same: increased complexity and urgency for defenders. Attack AI isn't just accelerating threats—it's reshaping them; its dual-use nature is forcing all stakeholders to revisit foundational assumptions around detection, response, and resilience.

As such, the promises of Attack AI are vast, but the data tells its own story. Automated scanners efficiently flag web app and API issues **(126% increase compared to last year)**. However, manual pentesting continues to uncover critical weaknesses that necessitate in-depth analysis and contextual understanding, such as payment gateway escalation.

Thus, Attack AI models don't eliminate the need for expertise but amplifies the need for more profound validation. The **38.67%** increase in vulnerabilities detected by automated scans reflects this capability, i.e., defining its role in handling the volume, while manual testing delves deeper into specific areas of concern.

The real challenge isn't automation versus manual testing—it's navigating the gaps between detection, prioritization, and meaningful remediation. This section explores those gaps, uncovering what today's automated security tools are catching, what they're missing, and what security leaders must do to bridge the divide.

Industry-Wise Security Priorities in 2025: Are Companies Protecting the Right Assets?

Cyber threats may be universal, but security priorities in 2025 are anything but. Each industry faces its own evolving risk landscape—what keeps a SaaS leader on edge isn't the same as what a fintech powerhouse fears most. Yet, security strategies often remain overly generic, relying on one-size-fits-all approaches that fail to address the industry-specific threats organizations actually face.

Despite growing awareness of cybersecurity risks, many companies are still misaligned in their defense strategies—focusing on known vulnerabilities while overlooking emerging attack vectors. Security audits remain standard practice, but the patterns reveal a concerning reality: protection efforts don't always match real-world threat exposure.

Looking ahead, businesses must shift toward smarter, risk-driven security approaches tailored to their industry's unique challenges. This section examines the top five industries investing in security audits—what they prioritize, why it may not be enough, and how their current focus could expose them to the evolving threat landscape of 2025 and beyond.

Furthermore, cloud infrastructures experienced a **65.7%** increase in security assessments, following, though with a significant margin at **285**, as the second most requested asset after web apps.

Asset-Specific Targeting: A shifting focus

As the threat landscape evolves, attackers are broadening their focus, leading to a sharp rise in security assessments across key digital assets. Web applications saw the most significant surge in pentesting demand, growing at more than double the rate compared to the previous year. This trend aligns with the increasing number of vulnerabilities identified in CVE data, reaffirming web apps as high-value targets for attackers.

APIs also experienced a substantial rise in security assessments, reflecting their expanding role in modern architectures and the heightened risks associated with their widespread adoption. Meanwhile, cloud infrastructures, though trailing behind web apps in total demand, continued their steady growth, emphasizing the industry's deepening reliance on cloud environments and the associated security concerns.

Pentesting requests for mobile platforms, including Android and iOS, also climbed noticeably, underscoring how attack surfaces are expanding into areas once considered relatively secure. The upward momentum across all these categories signals a clear shift in how businesses prioritize

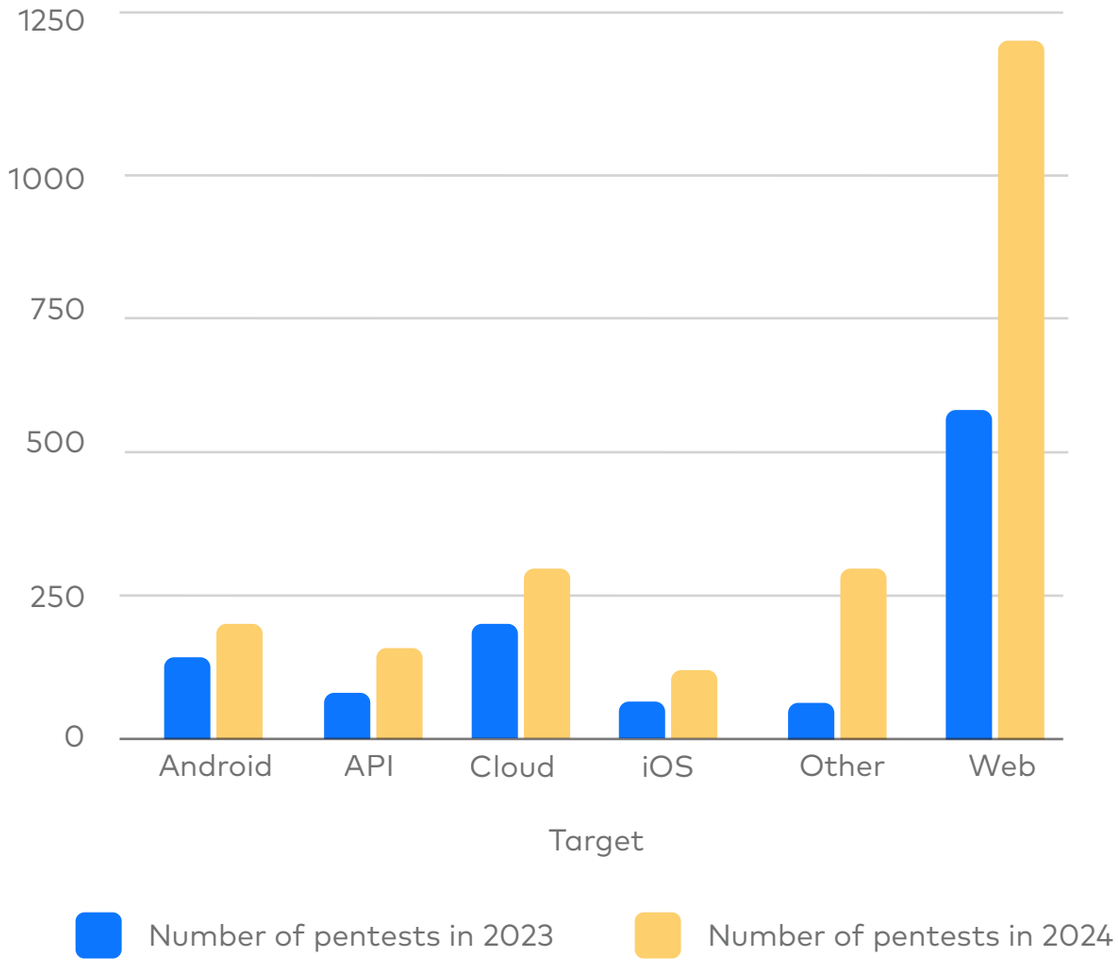
While the YoY growth here is lower than that for APIs, the numbers are a stark reminder of the undeniable shift toward cloud reliance, making these environments prime targets for cybercriminals.

Why is demand shifting now?

The surge in security assessments isn't just a response to evolving threats—it's a direct consequence of how organizations operate today. The rapid expansion of online assets, fueled by remote work and cloud adoption, has significantly widened attack surfaces, making regular security testing more critical than ever.

At the same time, tightening compliance mandates drive companies to conduct deeper, more frequent assessments, uncovering vulnerabilities that might have previously gone unnoticed. But beyond regulatory obligations, this shift signals a deeper change in mindset—businesses are moving beyond a checkbox approach to security, recognizing the real and rising risks across industries.

Attackers, too, are adapting. With AI/ML accelerating the sophistication and scale of cyberattacks, adversaries are diversifying their methods, exploiting weaknesses across an ever-growing range of assets. For security teams, the priority is clear: protecting high-risk environments like web applications, APIs, and cloud infrastructure—now at the forefront of cyber threats.



Astra's efficiency in numbers

Web App **60.5** Days to patch

- Astra delivers results at the **lower end of the industry range** despite web applications being the most frequently targeted.

API **43.9** Days to patch

- Astra's platform reduces API remediation times to **well below the industry average**, offering organizations a faster and more secure response.

Cloud **48.4** Days to patch

- Astra accelerates the security of cloud environments, delivering fixes in **far less time** than the broad industry range.

Mobile Applications **Under 50** Days to patch

- Astra empowers organizations to address vulnerabilities on emerging platforms at a pace that significantly outperforms traditional timelines.

Peter Merkert,
CTO, Retraced

AI is a double-edged sword, benefiting both red and blue teams. On defense, AI enhances detection, response, and proactive threat prevention. On offense, it enables more unique and sophisticated attacks. Social engineering, the top attack vector, will likely become even more dangerousas AI amplifies attackers' ability to craft hyper-personalized exploits!

Time-to-remediate: Setting a new industry standard

Time is critical in cybersecurity. Industry data shows that the average time to remediate vulnerabilities ranges between **60 and 150 days**, depending on the asset type and severity. Astra has consistently outperformed this benchmark, delivering significantly faster remediation times across all major assets.

Astra's impact

By consistently delivering faster remediation timelines than the typical industry averages, Astra empowers organizations to:

Reduce risk exposure: Narrowing the window of opportunity for attackers.

Boost operational efficiency: Minimizing disruption to teams and systems.

Ensure compliance: Meeting security standards within shorter timeframes.

Why it matters

Faster remediation is more than a statistic—it's a competitive edge. By closing vulnerabilities swiftly, organizations mitigate the risk of exploitation, protect customer trust, and ensure compliance with regulatory standards. Astra's approach demonstrates how proactive vulnerability management translates into tangible security and operational benefits.

In a world where the cost of a data breach averages millions of dollars, cutting remediation times by even a few days can save organizations from catastrophic losses. With Astra, it's not just about finding vulnerabilities but fixing them faster than ever before.

Reading between the numbers

As Attack AI evolves, its role in cybersecurity becomes more apparent—it's a force multiplier, not a replacement for human expertise. In 2025, automation is accelerating vulnerability detection like never before, but identifying a risk isn't the same as understanding its real-world impact. A flagged issue doesn't always translate to an actual threat, and an exploit isn't just about exposure—it's about consequence.

AI redefines how security teams operate, enhancing speed and scale, but the critical aspects of context, prioritization, and strategic response still depend on human insight. In an era where attackers also leverage Attack AI to refine their tactics, intelligent automation and human expertise remain the most powerful defense.

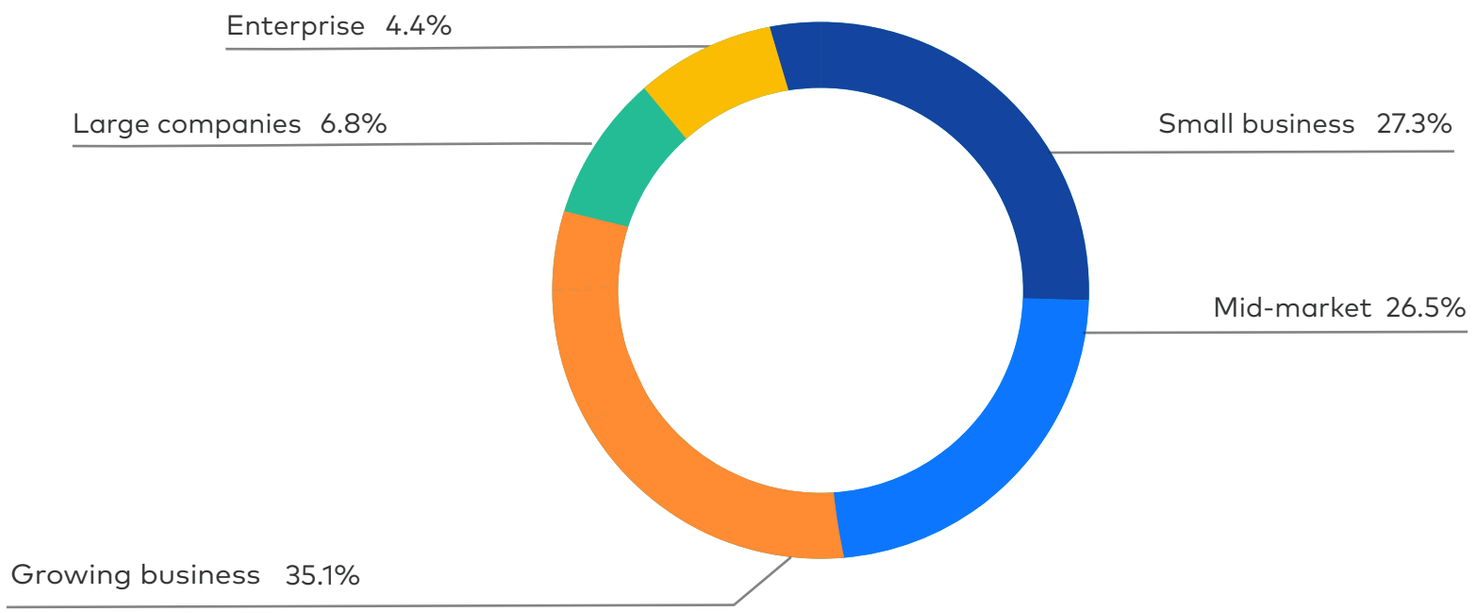
- **AI-powered web app pentests surged 219.41%,** signaling a sharper attack focus.
- **Automated scans detected 38.67% more vulnerabilities**, proving AI's growing role in scaling security.
- **Industry remediation time remains 60-150 days**—Astra is faster.
- **API pentest demand jumped 90%,** reflecting heightened security concerns.

State of cybersecurity teams

The last 30 months of security data make one thing clear: cybersecurity isn't just evolving—it's becoming an operational cornerstone for businesses of all sizes. The shift is most evident in **growing companies (50–200 employees)**, which now account for **35%** of overall pentesting demand. This isn't just a phase; it reflects a fundamental restructuring in how businesses perceive security.

Long underrepresented in security discussions, **small businesses** accounted for **27.29%** of pentesting activity in 2024. That alone signals a breaking point in the outdated assumption that only large enterprises need robust security programs. The surge in ransomware-as-a-service and highly targeted phishing attacks has forced even the most minor players to take security seriously—or risk being easy prey.

Meanwhile, **enterprises (4.37%) and large companies (6.82%**) continue to build sophisticated in-house security programs, reducing their reliance on external pentesting. But make no mistake: this isn't a sign of fewer attacks. It's a shift toward internal control, where security isn't outsourced but embedded within engineering workflows.

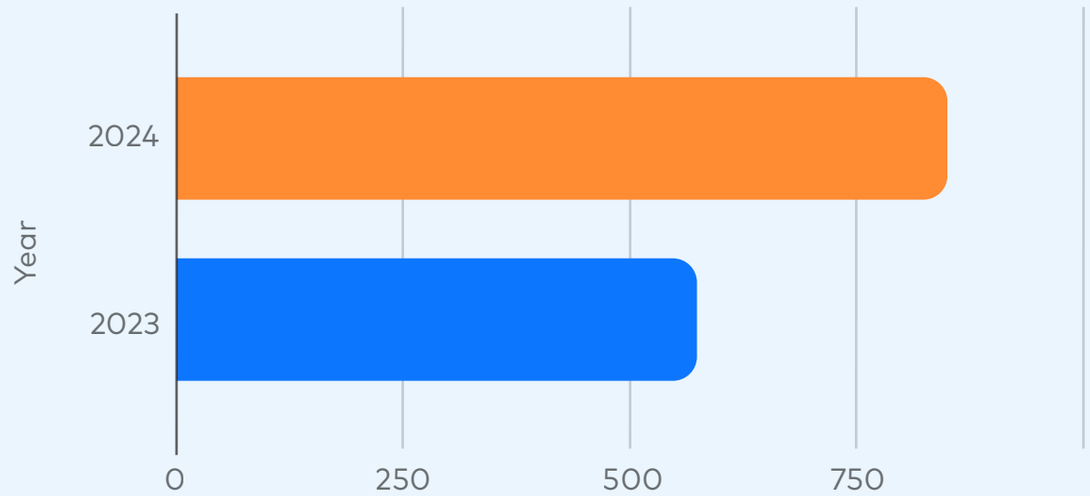


Automated pentesting isn't just gaining ground—it's becoming the default security layer for fast-scaling businesses. In 2024, **automated pentests surged 2.5X**, restructuring how security is managed with the ability to complete a scan in **1 hour and 10 minutes** now, allowing companies to enforce routine security checks at unprecedented speed, closing gaps before attackers can exploit them.

But automation alone has limits; the uptick in manual pentests proves that human-led security remains essential. When infrastructure is highly sensitive, compliance-driven, or vulnerable to complex exploits, a **16-day deep dive isn't a luxury**—it's the difference between surface-level validation and actual risk mitigation. Security-conscious organizations aren't replacing manual testing; they're using it where it matters most.

Simply put, efficiency has become the defining factor. Automated scans wrap up in 1 hour and 10 minutes; even vetted tests, which took nearly six days, now finish in just over one. The conversation is no longer about whether testing should be faster—2025 is proving that speed is non-negotiable. The real challenge ahead? Ensuring that as security validation accelerates, it doesn't lose depth.

Pentests resolved (with certificate) per year



Pentests resolved (with certificate)

Jayesh Singh Chauhan
Founder, Cloudurance Security & Cloud Village

Enterprises will be moving away from annual or quarterly pentests toward continuous pentesting models. Traditional pentests often give a snapshot in time, but security threats evolve daily. With rising API and cloud security concerns, organizations want ongoing visibility into vulnerabilities. A lot of organisations are integrating automated vulnerability scanning tools alongside manual testing to keep up with the pace of change. Gen AI shall play a pivotal role in advancing this forward, especially the limitation on human dependence for understanding logical context & building test cases for automated repeatability.

A **48% increase in pentests performed and completed**, with several hundred still underway, isn't just a reflection of rising security investments—it signals a structural shift in how security is embedded into business operations.

This goes beyond the familiar narratives of "increasing threats" or "regulatory pressure." It demonstrates a growing divide between companies treating security as a strategic enabler and those still reacting to incidents. If this continues, the gap in security maturity will only widen. Some emerging patterns include:

The 'good enough' mindset is fading

Compliance-driven, annual security checks give way to continuous validation, reinforcing security as an ongoing process rather than a box to check.

Pentests as a competitive edge, not a cost center

Forward-thinking companies aren't just testing more; they're integrating security into their core business strategy, using pentesting as a driver of resilience and trust.

Security teams are gaining leverage

The rise in pentests doesn't equate to instant security; instead, it reflects how security leaders are quantifying risk in ways that demand action—though remediation bottlenecks remain challenging.

The growing divide in security maturity

Faster scans mean little without efficient remediation. Companies embedding security into development pipelines accelerate risk reduction, while others risk accumulating security debt until breaches force a response.

This shift isn't a temporary surge; it's a transformation in security strategy. As security debt remains unchecked, it will quickly become a business liability rather than a technical concern. Signs already point toward the next phase—one shaped by continuous validation, security-driven engineering, and automated risk reduction.

Reading between the numbers

Technical debt in security doesn't disappear—it just changes shape. Early-stage companies wrestle with web app vulnerabilities, scaleups inherit API and cloud risks, while enterprises contend with sprawling networks and mobile threats. The 2025 challenge isn't just keeping up with new attack surfaces—it's ensuring past risks don't quietly resurface in the gaps.

- Web app security remains the top concern, driving **35% of pentest demand** from growing businesses.
- **Enterprises** increasingly prioritize **network & mobile security**, while scaleups focus on **API & cloud.**
- **Automated pentests surged 2.5x**, while manual pentests remain vital with a 16-day average.

> *One of the biggest shifts has been how organizations rethink security as a continuous process rather than a one-time checkbox. With evolving threats and regulatory pressure, security teams now focus more on proactive security through real-time threat monitoring, automated testing, or red teaming. Another major shift is the rise in supply chain attacks, which has forced companies not just to secure their systems but also to scrutinize vendors' security more closely. Organizations should take a data-centric approach to implement security controls*

Bhavesh Kumar, Chief Information Security officer and DPO, SK Finance Ltd

6 Financial impact

The business case for pentesting: a deep dive into cost savings

For security leaders, justifying cybersecurity investments is rarely straightforward. Unlike traditional business expenses with clear returns, security spending is inherently preventative, making its financial impact harder to quantify.

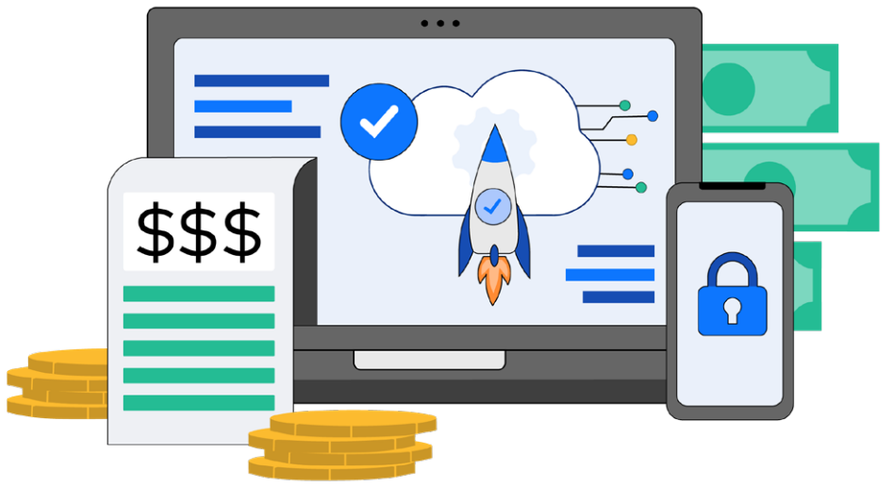
Organizations know that breaches are costly, but estimating potential losses, understanding risk exposure, and translating cybersecurity into boardroom language remain persistent challenges. The most important fundamental truth - security isn't an expense but an investment.

Every undetected vulnerability carries a price tag, and every missed remediation opportunity is a future financial liability. This section breaks down the cost of cybersecurity inaction, the ROI of automated and manual pentesting, and the economic risks organizations mitigate when taking security seriously.

How pentesting directly translates to cost savings

The cost savings from VAPT in 2024 are undeniable: **Automated testing alone saved $1.68 billion**, up from $473 million in 2023, reflecting such tools' increased efficiency and sophistication.

While more limited in scope, **manual pentests saved $105 million**, a sharp rise from $5.4 million. This shows that human expertise still uncovers critical vulnerabilities that automation might miss, particularly in high-risk areas like cloud and APIs.



Top 3 vulnerabilities with most financial impact prevented

Certain vulnerabilities have the potential to inflict significant financial damage. Through proactive pentesting, these threats were identified and mitigated, saving our clients from substantial losses. Here are the top 3 breaches we helped prevent in 2024 based on their **risk score and potential loss:**

01 AWS access key ID and secret access key exposed

Risk Score 10

Potential Loss $100,000

Exposing AWS credentials in any system can lead to severe financial losses, making it critical to identify this vulnerability early.

CWE: Exposure of Sensitive Information to an Unauthorized Actor

02 Insecure Direct Object Reference (IDOR)

Risk Score 9.9

Potential Loss $50,000

This flaw could allow **unauthorized access to sensitive data**, resulting in a significant breach and financial loss.

CWE: Improper Access Control

03 2FA Bypass via Response Manipulation

Risk Score 9.7

Potential Loss $27,000

A vulnerability like this **compromises the security of user accounts**, putting valuable data and resources at risk.

CWE: Authentication Bypass

The real cost of inaction: how fixing vulnerabilities saves millions

In today's cybersecurity landscape, a breach can have a devastating financial impact. However, identifying and fixing vulnerabilities before they are exploited can save organizations millions. By analyzing the potential loss associated with detected vulnerabilities, we can estimate the financial savings realized by organizations when vulnerabilities are remediated proactively through Astra's pentesting services.

Average Potential Loss vs. Actual Cost of Remediation

Vulnerabilities exist across multiple environments, but the financial risk varies significantly. Here's how different asset types contributed to potential financial exposure:

iOS

Number of Issues	359
Average Potential Loss ($)	325.62
Total Potential Loss ($)	71,310

Web

Number of Issues	476,738
Average Potential Loss ($)	1,212.36
Total Potential Loss ($)	266,194,887

Android

Number of Issues	1,542
Average Potential Loss ($)	824.96
Total Potential Loss ($)	666,566

Other

Number of Issues	1,409
Average Potential Loss ($)	373.94
Total Potential Loss ($)	280,453

Cloud

Number of Issues	11,560
Average Potential Loss ($)	1.55
Total Potential Loss ($)	6,840

API

Number of Issues	3,614
Average Potential Loss ($)	1,444.06
Total Potential Loss ($)	2,044,792

ROI of manual vs. automated pentests

In 2024, Astra Security conducted many automated and manual pentests. The ROI of both methods can be evaluated based on the vulnerabilities detected, their potential financial impact, and the time saved in detection and remediation.

The financial benefit of vulnerability detection & patching

Most organizations view cybersecurity spending through the wrong lens, focusing on cost instead of consequence. But security isn't about how much you spend but what you prevent. A single AWS Access Key exposure could cost **$100,000, and SQL Injection**—still a critical threat—remains one of the most financially devastating vulnerabilities.

The actual financial impact of pentesting isn't in the number of vulnerabilities detected; it's in the losses avoided. Web vulnerabilities alone accounted for **$266 million** in potential losses, while APIs added another **$2 million** to the risk pool. These aren't abstract figures—they represent the cost of inaction.

The takeaway? Security teams aren't just fighting attackers; they're fighting assumptions—assumptions that compliance is enough, that automation catches everything, and that breaches happen to other companies. However, as the data shows, companies prioritizing continuous testing don't save money; they stay in business.

Web

Vulnerabilities Detected	13107
Avg Potential Loss per Vulnerability ($)	1,212.36
Total Potential Loss Prevented ($)	15,890,403

Android

Vulnerabilities Detected	1699
Avg Potential Loss per Vulnerability ($)	824.96
Total Potential Loss Prevented ($)	1,401,607

iOS

Vulnerabilities Detected	371
Avg Potential Loss per Vulnerability ($)	325.62
Total Potential Loss Prevented ($)	120,805

API

Vulnerabilities Detected	726
Avg Potential Loss per Vulnerability ($)	1,444.06
Total Potential Loss Prevented ($)	1,048,388

Cloud

Vulnerabilities Detected	218217
Avg Potential Loss per Vulnerability ($)	1.55
Total Potential Loss Prevented ($)	338,236

Other

Vulnerabilities Detected	8122
Avg Potential Loss per Vulnerability ($)	373.94
Total Potential Loss Prevented ($)	3,037,141

Total	242242		21,836,579

Automated pentests: vulnerabilities detected & potential loss prevented

In 2024, automated scans identified **2,558,317 vulnerabilities** across various asset types. The total potential loss is calculated based on the number of vulnerabilities detected and their corresponding average potential loss values.

Asset Type	Vulnerabilities Detected	Average Potential Loss	Total Potential Loss Prevented
Web	2365691	1,212.36	2,868,069,141
API	12185	1,444.06	17,595,871
Cloud	180441	1.55	279,684
Total	2558317	-	2,885,944,695

Total Potential Loss Prevented by Manual Pentests: $21,836,579

Reading between the numbers

Security isn't just a bottomless cost center—it's a financial strategy. Every breach that didn't happen, every exploit neutralized before execution, represents millions saved in damages, downtime, and reputational loss.

More importantly, the real question isn't whether security testing saves money but whether your spending matches your risk appetite. Are you staying ahead of threats or silently accumulating risk, hoping it won't materialize? Security isn't about endless spending but knowing how much risk you can realistically afford to take.

> *I constantly push developers to understand the business side, because that's where things start. Learn why you're doing things, ask questions, push back when needed, don't code until you truly believe.*

Aditya Anand, Co-founder & CTO, ZenAdmin.ai

$2.88B

Potential losses prevented through automated pentests.

$21.8M

Losses averted by manual pentests.

$1.68B

Saved through automated security testing in 2024 ((up from $473M in 2023)

7 Industry-wise security priorities in 2025: are companies protecting the right assets?

Cyber threats may be widespread, but security priorities in 2025 are far from uniform. Each industry faces distinct risks—what keeps a SaaS leader on edge differs from the top concerns of a fintech giant. Yet, many security strategies still take a one-size-fits-all approach, overlooking different industries' specific threats.

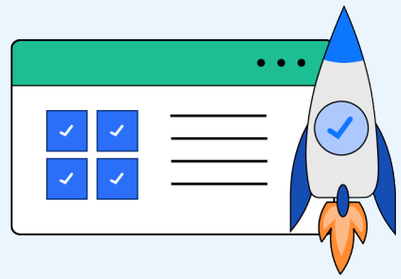
Despite increasing awareness of cybersecurity risks, many companies struggle to align their defenses with real-world threats, focusing on familiar vulnerabilities while missing emerging attack vectors. Security audits remain a standard practice, but the data reveals a critical gap: what businesses choose to protect doesn't always reflect where they are most exposed.

Looking ahead, organizations must adopt risk-driven security strategies tailored to their industry's evolving challenges. This section examines the top five industries investing in security audits—what they prioritize, why it may not be enough, and how their current focus could leave them vulnerable in the shifting threat landscape of 2025 and beyond.

1 Information technology and services: Web and API Security as a primary concern

The IT & Services sector accounts for the largest audit requests, strongly focusing on securing digital applications.

- Web applications comprise over **40% of all audits,** reflecting the industry's reliance on online platforms.
- API security assessments represent **around 25%,** highlighting growing concerns around API-driven architectures.
- **Cloud and network penetration testing audits** indicate a shift toward more comprehensive security strategies.



2 Computer software: strengthening application and cloud security

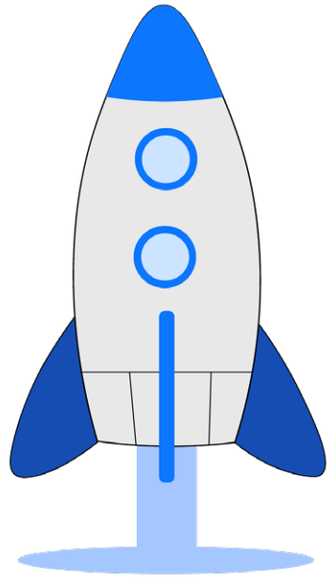
Software companies prioritize protecting customer-facing applications and cloud infrastructure.

- Web applications constitute nearly **30% of** all security assessments, reinforcing their critical role in security strategies.
- API security audits make up over **20%,** reflecting the sector's transition to API-driven architectures.
- Cloud and multi-layer security assessments represent around **50%,** signaling a growing focus on securing SaaS platforms.

3 Financial services: securing transactions and digital interfaces

The financial services sector places significant emphasis on securing financial transactions and customer data.

- Web applications and APIs each account for over **35%** of audits, ensuring transaction integrity.
- Mobile banking security assessments represent **close to 30%,** highlighting the increasing reliance on mobile platforms for financial services.
- Comprehensive audits covering cloud and network security make up **the remainder**, demonstrating a risk-based approach to cybersecurity.



4 Marketing and advertising: protecting cloud-based infrastructure

The marketing and advertising industry prioritizes securing customer data and digital platform.

- Cloud security assessments make up over **50% of all audits,** reflecting the industry's heavy reliance on cloud-based systems.
- Web application security accounts for around **35%,** ensuring the protection of digital campaigns and platforms.

5 Healthcare & hospitals: strengthening multi-layered security

The healthcare sector focuses on data security and regulatory compliance.

- Web applications account for nearly **50%** of security assessments, protecting patient data.
- Mobile, cloud, and network security audits collectively make up around **50%,** underscoring the need for multi-layered security strategies in digital healthcare.

Reading between the numbers

A company's biggest security investment isn't driven by risk alone—it's dictated by what failure would cost them the most. Tech firms move fast but can't afford fragile foundations, financial services chase speed while guarding every transaction, and healthcare prioritizes trust over efficiency.

Security isn't just about threats; it reflects what each industry values and what it can't afford to lose.

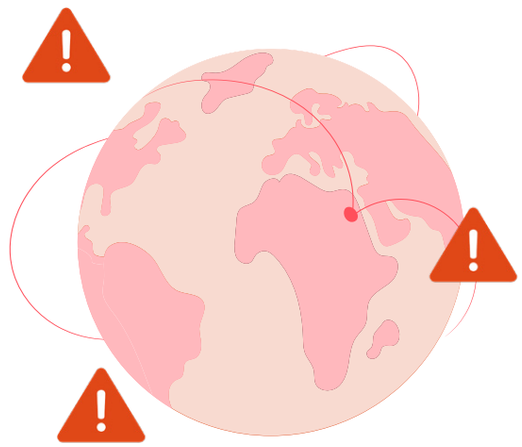
- **Technology and software companies** prioritize **web and API security,** aligning with their reliance on digital platforms.
- **Financial services firms** focus on **transaction security, mobile banking, and API protection** to safeguard customer assets.
- Due to their dependence on **data-driven campaigns, marketing, and advertising companies** emphasize **cloud security.**
- **Healthcare organizations** require **comprehensive security measures** to protect sensitive patient information.

> *Different industries have unique security priorities—tech companies focus on APIs, financial firms safeguard transactions, and healthcare organizations prioritize patient data and system integrity. But at the core, they all share the same challenge: building resilience against threats that could undermine trust and disrupt operations.*

Jinson Varghese, Information Security Lead, Astra

8 Forecast 2025—The road ahead

Emerging threats

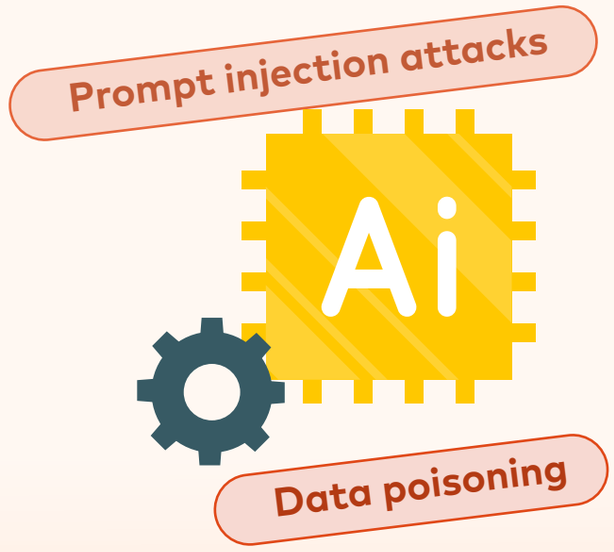


Looking ahead to 2025, the security landscape is marked by a growing intersection of AI, cloud infrastructure, and interconnected systems. As AI becomes more integrated into business-critical applications—**from personalized healthcare assistants to financial services**—it's also introducing new points of vulnerability.

The nature of attacks is shifting from exploiting traditional vulnerabilities to exploiting the complexities of machine learning models. Thus, it is no longer about exploiting known weaknesses but finding the vulnerabilities in **AI's ability to process, interpret, and act on data in real time.**

This section outlines the emerging risks that are beginning to reshape how security professionals **protect AI, data, and digital infrastructure.**

Exploiting large language models (LLMs)



Large language models (LLMs) are quickly becoming one of the most attractive targets for attackers. **OWASP's Top 10 for Large Language Models (LLMs)** outlines critical flaws, such as data poisoning, prompt injection attacks, and adversarial inputs, that exploit weaknesses in AI decision-making alongside research to demonstrate how to exploit them.

For instance, **OpenAI** recently showcased how adversarial inputs could manipulate AI systems into generating harmful outputs, indicating that the risks of AI misuse are real and escalating.

A new era of data exposure

Privacy risks are escalating as AI plays a larger role in handling sensitive personal data. Health companion bots, for example, collect and process personal health information, offering tailored advice on diet, exercise, and mental well-being. If AI models are not properly secured, this data is a prime target for misuse.

A **2023 report** from Harmonic Security highlighted how AI systems, particularly those in fintech and healthcare, have been tricked into revealing confidential information. The data leaks include payroll information and private health details.

Social engineering at scale

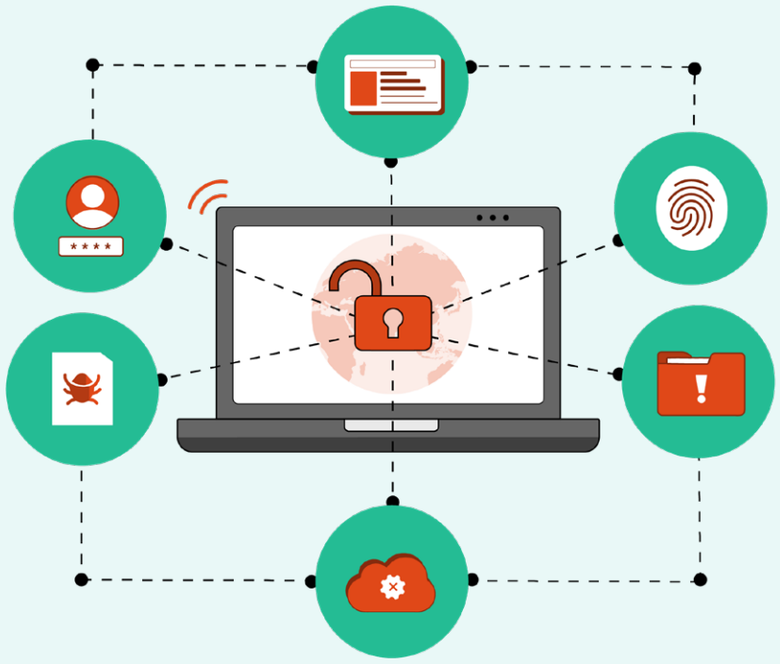
Phishing attacks have always been a problem, but AI is turning them into an industrialized operation. What once required manual effort is now automated by generative AI tools, enabling attackers to create hyper-realistic phishing campaigns that are nearly impossible to distinguish from legitimate communications.

These **AI-driven schemes** can mimic a user's writing style, generate personalized messages, and even automate social engineering tactics. This results in an exponential increase in the scale and effectiveness of phishing attacks, which seriously threaten businesses and individuals.

API and Cloud vulnerabilities: the AI dependency

APIs have long been the backbone of SaaS and cloud services, enabling seamless data exchange across platforms. However, as AI systems become deeply integrated into these services, vulnerabilities in API security are becoming a significant concern, especially in cloud-based environments.

Thus, API vulnerabilities, particularly those used in cloud environments, will be a **focal point** for attackers in 2025. These APIs are crucial for AI's ability to function at scale. In 2024, multiple high-profile breaches involved attacks that targeted such CVEs to inject malicious code into AI-driven systems.



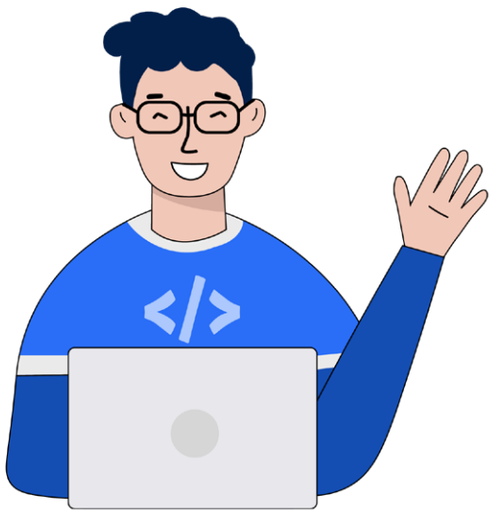
Proactive measures for a stronger security future

Cybersecurity isn't a rat race to catch up with new techniques and attacks but a constant struggle to stay ahead. Simply put, with rising costs - direct and implied - irrespective of your industry, size, audience, etc, no company can afford an attack and stay in the black. It is the survival of the fittest.

According to IBM, the average cost of a data breach reached $4.88 million in 2024, a 15% increase over three years. The primary culprit? Delayed remediation due to disjointed security tools and processes.

Thus, the landscape now demands that organizations shift from reactive security to proactive, unified, and continuous security strategies to combat increasing attack complexity, regulatory scrutiny, and security tool sprawl.
In the coming year, forward-thinking security teams will prioritize unified security platforms, privacy-first engineering, and continuous security monitoring to bridge these gaps.

> *When you first start thinking about security, you make it complex - more tools, more alerts, more noise. But if you keep going, if you really think deeply about it with an AI first mindset, you get to something beautiful: security that's so neatly integrated, it just works seamlessly. That's what 2025 is about - not adding complexity, but eliminating it. We're going to see security tools which 'actually' help fix or even fix the security gaps for engineers & security teams with less to no noise.*
>
> 
>
> Shikhil Sharma, CEO and Co-Founder, Astra



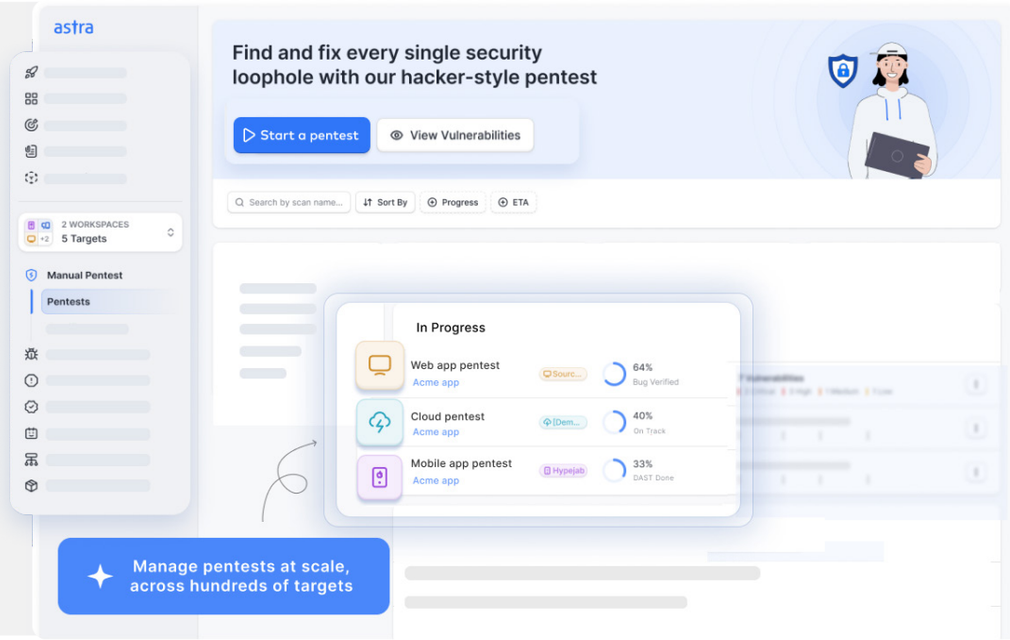
1 The rise of unified security platforms

According to **Anomali**, security teams today manage 15 to 25 different security tools on average, leading to overwhelming alerts, false positives exceeding **40 %**, and remediation delays of over **97 days for critical vulnerabilities.** This fragmented approach creates alert fatigue and security blind spots.
According to a Gartner report, 75% of organizations seek to consolidate the number of cybersecurity vendors they use. Driving factors include heightened concerns about operational complexity and a need to improve risk mitigation.

Astra's OrbitX platform introduces a new era of unified security. Scattered data and fragmented tools no longer hinder your ability to stay ahead of threats. A single, integrated dashboard consolidates all security insights across targets, vulnerabilities, and pentests, providing a seamless, holistic view of your entire ecosystem.
This unified approach simplifies security management and empowers teams to make swift, informed decisions. It enhances efficiency and ensures consistent protection across all assets.

Key Insights:

- A centralized hub for all security data, enabling effortless tracking and analysis.
- Real-time, continuous penetration testing, delivering ongoing visibility without silos.
- Simplified workflows with intuitive, cross-functional navigation for teams.
- Seamless integration management across CI/CD pipelines, ensuring cohesive protection.



2 Privacy-first engineering will become the standard

With data privacy regulations tightening worldwide, security is no longer just about stopping breaches—it is about ensuring compliance from day one. In 2025, privacy-first engineering is set to become a foundational practice as companies work to:

Key insights:

- Mitigate compliance risks from regulations like **SOC 2, PCI DSS, GDPR, NIST, GLBA, and ISO 27001**, which mandate strict security controls and regular audits. Non-compliance can lead to severe consequences—GDPR fines alone have exceeded **€4.48 billion** since its enforcement.
- There is a growing recognition among C-level executives about the importance of API security, with **46%** reporting it as a topic of executive discussion. However, **55%** of respondents have faced delays in application rollouts due to API security issues, highlighting the real-world impact of inadequate security measures.
- Embed privacy controls at the code level to build trust with customers. According to a **Cisco benchmarking study**, 75% of consumers say they won't buy from companies that don't protect their data.

Maintaining compliance is not a one-time effort—it requires continuous monitoring to ensure security controls remain effective against evolving threats. Astra helps businesses stay audit-ready and compliant by providing:

- Automated security scanning to detect vulnerabilities that could violate **SOC 2, PCI DSS, GDPR, ISO 27001**, and other regulatory standards.
- Real-time compliance tracking to monitor security postures against frameworks, ensuring organizations stay ahead of compliance gaps.
- Instant remediation insights with prioritized fixes so teams can resolve compliance risks before they escalate into security incidents.

Integrating compliance into everyday security practices, Astra ensures businesses remain secure and audit-ready without slowing down innovation.

3 Continuous security will replace point-in-time testing

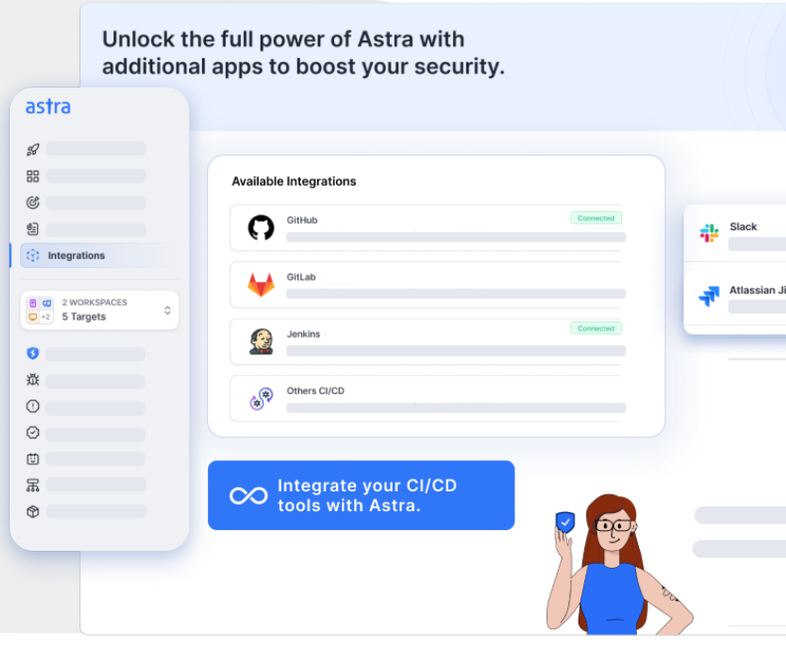
Cyberattacks do not wait for quarterly or annual security assessments, so security teams can no longer afford to rely on outdated security models. As businesses recognize the risks of periodic testing, the shift from point-in-time testing to continuous security is accelerating.

Industry data highlights the urgency of this transition:

- **According to a study**, 60% of breaches in the last year were due to known, unpatched vulnerabilities
- **65 %** of breaches exploited vulnerabilities disclosed more than a year ago.

Astra helps security teams stay ahead of attackers with the following:

- Always-on vulnerability scanning: **Unlimited DAST scans for Web app, API, and cloud security** scans to detect real-time risks.
- **Vetted scans:** Security engineers actively validate vulnerabilities instead of generating scan reports.
- **Seamless CI/CD integration:** Security scans running with every release to ensure vulnerabilities do not reach production.



The road ahead with Astra Security

- **13,000+ security tests** conducted in **2024**, helping businesses identify and address vulnerabilities.
- **Millions** are saved by preventing security flaws from being exploited.
- Trusted by companies across **SaaS, fintech, healthcare, and e-commerce** for their security needs.

In 2025, security teams will seek solutions that simplify workflows, reduce noise, and provide **actionable remediation guidance**—not just vulnerability reports.

Astra is evolving to meet these needs. By shifting from **reactive to proactive security,** businesses using Astra are improving **breach prevention, accelerating remediation, and ensuring compliance**—all while streamlining security operations.

The future of security isn't just about finding vulnerabilities—i**t's about fixing them efficiently**. Astra is focused on enabling that shift.

Final thoughts

Organizations invest more in security tools, frameworks, and policies every year. Yet breaches continue to rise, attackers evolve faster than defenses, and security teams remain caught in reaction cycles. If effort alone could solve the problem, we wouldn't be here.

The truth is that security isn't failing because companies aren't trying hard enough. It's failing because the very foundations of our approach are flawed. The idea that we can defend our way to safety assumes a static battlefield. But attackers don't play by these rules. They move unpredictably, exploit what's overlooked, and innovate faster than defenses can adapt.

The organizations that will survive the next decade won't be the ones with the biggest security budgets—they'll be the ones willing to challenge the security mindset itself. This means:

- **Think like an attacker, not an auditor**

  Compliance-driven security doesn't prevent breaches. You're already behind if you're securing only what regulations tell you.

- **Bet on offensive security, not just defenses.**

  The companies that prioritize aggressive, proactive testing—leveraging BAS, real-world adversarial testing, and automated red teaming with CTEM—will genuinely reduce risk.

- **See security as a business enabler, not an expense**

  The companies that embed security into product development, customer experience, and operational agility will outpace those that treat it as a cost center.

- **Personalize cloud security**

  As cloud environments become more complex, companies must adopt hyper-customized security strategies that adapt to their unique cloud stacks, architectures, and evolving attack surfaces.

The cybersecurity industry doesn't need another wake-up call but a complete redefinition of security success. It's no longer about catching up but rather breaking free from a system never designed for modern digital businesses' speed, scale, and complexity.

astra

Meet the Team

Editorial

Shikhil Sharma
Ananda Krishna
Ujwal Ratra
Shelton Jacob

Content

Sanskriti Jain
Rithika Sarmah

Data Curation

Saurabh Miglani
Jinson Varghese
Aaditya Anmol
Prateek Kuber

Design

Ananya Nair

Special thanks to

Peter Merkert, Naman Vyas, Jayesh Singh Chauhan, Lalit Indoria, Aditya Anand, Suhel Khan, Bhavesh Kumar