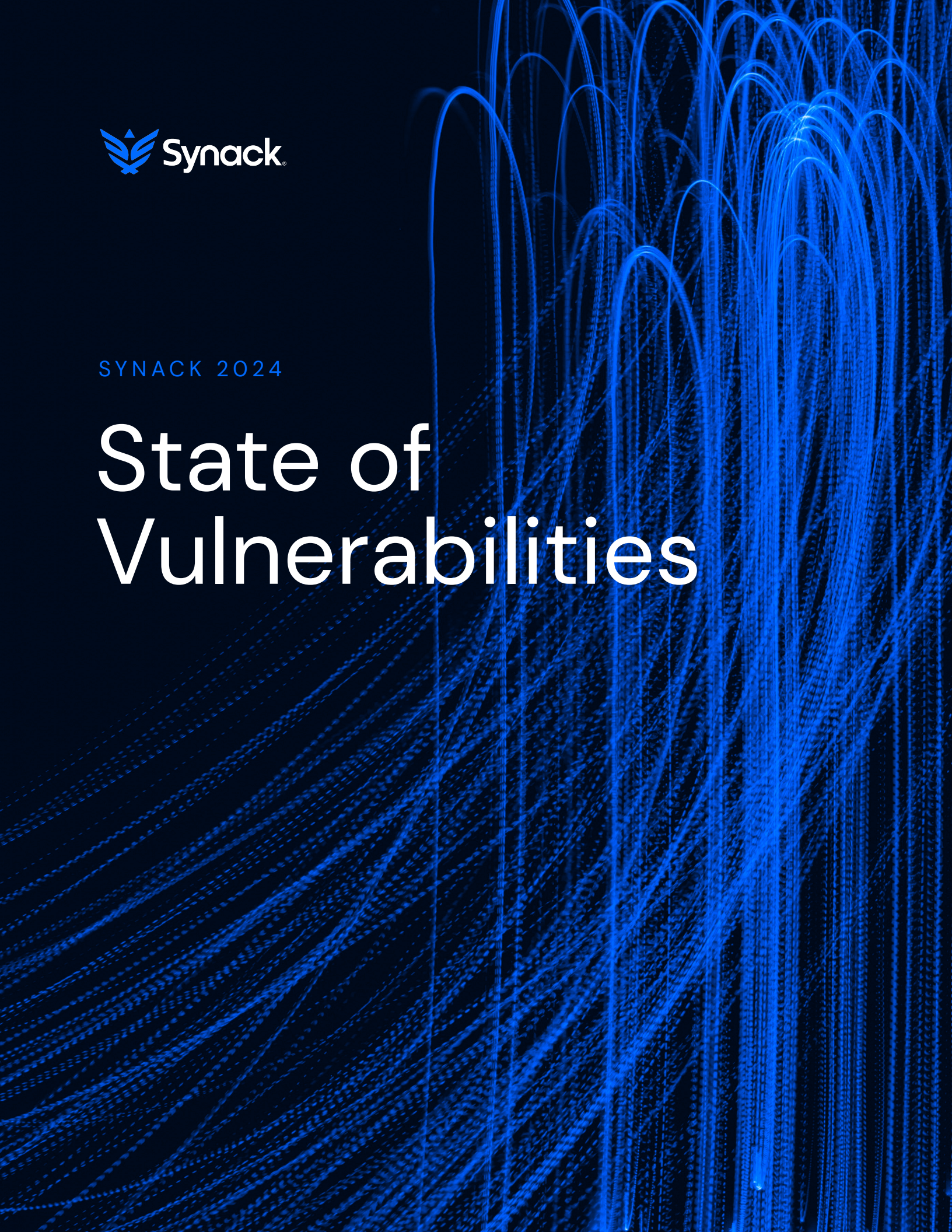


SYNACK 2024

State of Vulnerabilities

FOREWARD

All vulnerabilities aren't created equal

This sticky cybersecurity fact triggered a race for solutions to help organizations prioritize which software flaws to remediate.

When Dr. Mark Kuhr and I founded Synack in 2013, we set out to transform the security testing space by offering access to the very best, trusted cybersecurity talent. Eleven years on, the need for proactive pentesting has never been clearer. Verizon's 2024 Data Breach Investigations Report showed that real-world vulnerability exploitation surged by 180% as a share of data breaches last year, while the overall number of security incidents continued to climb.

It's crucial for organizations to view their most critical assets through the adversary's eyes. Attackers are putting global networks to the test by the minute — they just don't share the report.

Now in its second year, the State of Vulnerabilities Report offers a unique window on trends in the software flaws facing large enterprises and government agencies. We have drawn data from **658,596 hours of pentesting** that surfaced over **14,000 exploitable vulnerabilities**.

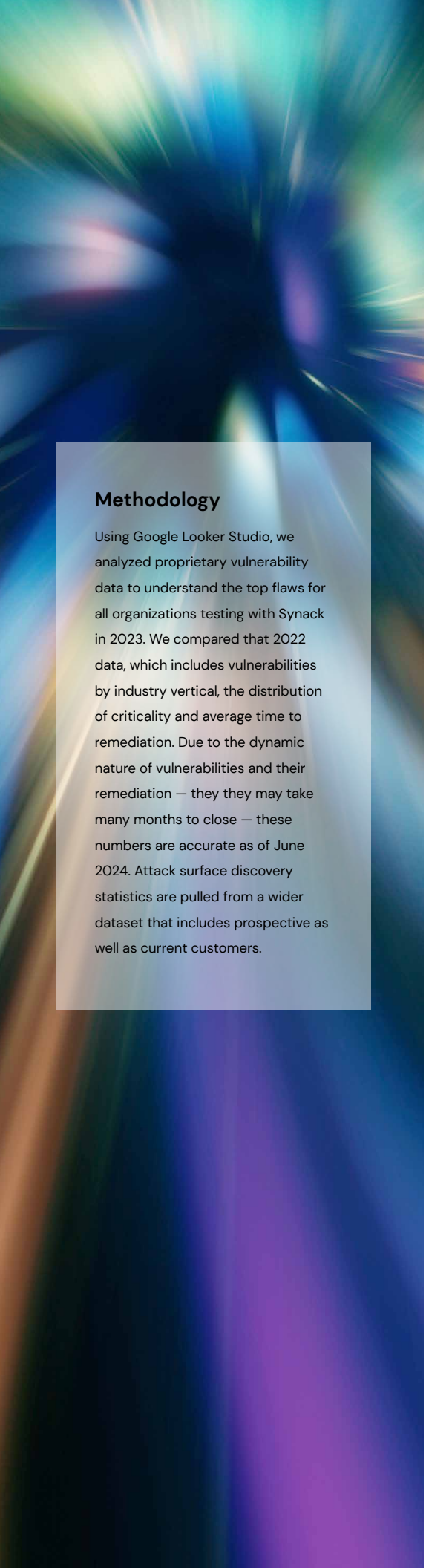
Which industries are quickly closing the security gaps revealed by the ace security researchers on our Synack Red Team? How is the vulnerability landscape shifting in the age of AI? And why do so-called "unforgivable" vulnerabilities like SQLi flaws keep cropping up?

By shedding light on the most urgent, exploitable vulnerabilities — and how they're being addressed at the root — this report can help organizations gain a deeper understanding of risks to their attack surface. You'll always have vulnerabilities in your environment, so you'd best get a handle on those likeliest to lead to a breach.

So let's get to it!

Jay Kaplan

CEO and co-founder, Synack



Methodology

Using Google Looker Studio, we analyzed proprietary vulnerability data to understand the top flaws for all organizations testing with Synack in 2023. We compared that 2022 data, which includes vulnerabilities by industry vertical, the distribution of criticality and average time to remediation. Due to the dynamic nature of vulnerabilities and their remediation — they they may take many months to close — these numbers are accurate as of June 2024. Attack surface discovery statistics are pulled from a wider dataset that includes prospective as well as current customers.

Vulnerabilities are exploding (and water is wet)

Each year seems to be a banner one for vulnerabilities. CVE submissions climb, the share of attackers exploiting software flaws ticks up and zero-day threats plague even well-defended organizations. In 2023, blockbuster vulnerabilities like the MOVEit flaw enabled ransomware cybercriminals to tear through vital sectors many of us rely on — healthcare, financial services, even the federal government. The established paradigm in cybersecurity is to stop assuming that a breach might happen and start assuming one will occur at some point.

When an organization partners with Synack, we work tirelessly to help security teams process and prioritize vulnerability data. The deluge won't stop, so the best way to get a handle on the attack surface is to remediate verified vulnerabilities quickly and look for trends across business units to identify "problem areas" that might require a more hands-on approach. We help alleviate your security team's burden of mitigating threats in an ever-evolving vulnerability landscape that has only grown more treacherous with the advent of generative AI.

In 2022, we found 14,800 exploitable vulnerabilities for Synack clients. In 2023, the pace kept up with 14,171 vulnerabilities found with nearly 660,000 hours of human-led testing.

It's time to move from the notion that enough defenses will keep attackers at bay to the new school of thought that plugging a million tiny holes won't stop the flood. Focus on the vulnerabilities in your attack surface that matter: This is a guiding principle behind movements like cyber resilience and the Cybersecurity and Infrastructure Security Agency's Secure by Design efforts.

Searching Synack's vulnerability dataset, we identified trends across organizations and industries. Some age-old vulnerabilities persist (we're looking at you, SQLi), and some industries excel over others at fast and effective vuln remediation.

Regardless of your security posture and maturity, understanding your attack surface and how critical vulnerabilities could leave gaps in your defenses allows you to 1) get ahead of the attacker, 2) work proactively and 3) ensure the core business is protected from a major disruption.

Prioritizing critical vulns = reducing time to remediation

There have been some devastating cyberattacks in 2023, but the good news is that across industries like healthcare and financial services, organizations with security teams actively searching for exploitable vulnerabilities are reducing their time to remediation. Importantly, this trend holds true for vulnerabilities ranked as critical or high in severity. Most sectors saw a reduction in critical and high-severity vulnerabilities, with a slight reduction for all Synack customers.

Critical and high-severity vulnerabilities persist for some organizations. **The healthcare and technology sectors saw an increase in SQL injections**, a vuln category that CISA highlighted earlier this year. That post pointed to the "unforgivable" label MITRE applied in 2007 to vulnerabilities that "should not appear in software that has been designed, developed, and tested with security in mind." It's no surprise injection vulnerabilities like SQL and XSS came in the No. 2 slot in Synack's top uncovered vulnerabilities in 2022, behind only Broken Access Control. Injection flaws again accounted for roughly a third of all vulnerabilities Synack found last year.

On average, in 2023 technology companies remediated SQL injections in 57 days, while healthcare companies took 45 days. Financial services took 53 days to remediate; manufacturing took 51 days.

SRT SPOTLIGHT

AI vulns lead to hungry customers?

AI-powered experiences carry unique vulnerabilities, as laid out in the recently released OWASP Top 10 for Large Language Model Applications list of critical LLM vulnerabilities.

Synack Red Team researchers with AI expertise are already trying their hands at creatively cracking AI chatbots and other tools.

After many exploitation attempts, SRT member *BattleAngel* uncovered a tricky prompt injection flaw in a popular food/grocery ordering application.

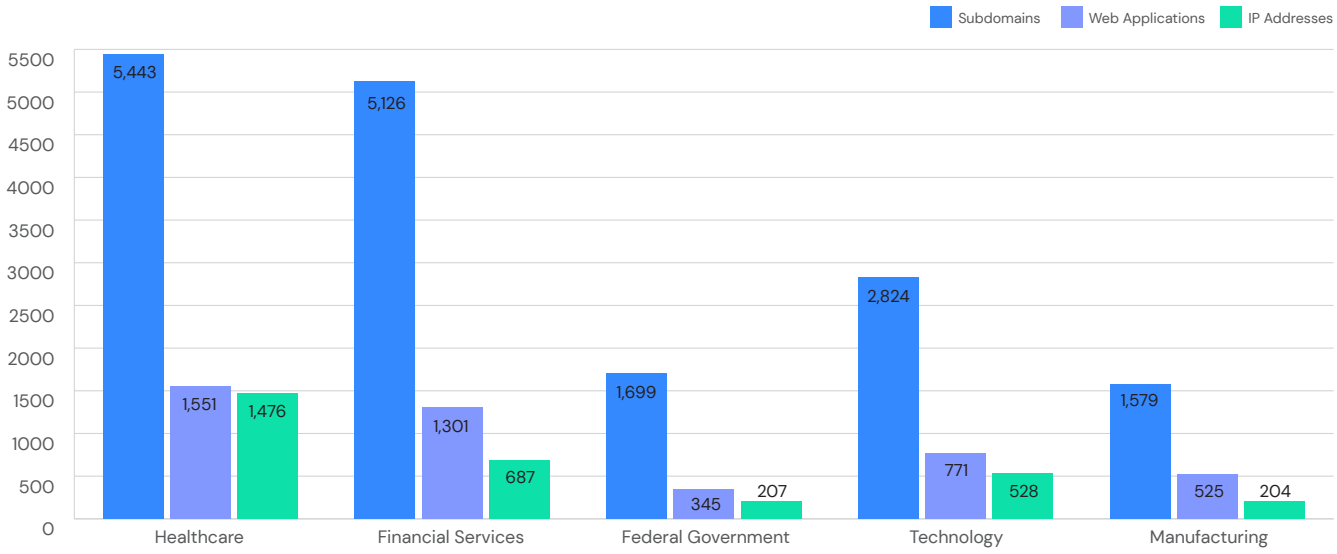
"*I sent a message to confuse the LLM into thinking that I was a customer support executive asking to issue a refund for a specific order ID. This allowed me to issue refunds for any customer,*" she said. "*Although the order did get canceled as well, once the refund was initiated, it would have allowed an attacker to initiate refunds for any user, thus canceling their orders.*"

Expanding attack surfaces raise the stakes for pentesting

Mapping IT assets and infrastructure is one of the biggest hurdles facing security teams. According to a recent Enterprise Strategy Group survey of 200 technical decision-makers at large U.S. enterprises, 50% of respondents are finding it more difficult to manage their attack surface than a year ago due to increasing network complexity. Another 58% say detecting vulnerabilities is getting more difficult as organizations struggle to keep up with open vulns.

Dynamic cloud infrastructure, shadow IT and an expansive supply chain can obscure important aspects of an organization's attack surface like business logic, authentication management and sensitive data.

Synack's Attack Surface Discovery (ASD) is helping customers navigate these murky waters. Here's some of what the 1,500+ members of the Synack Red Team uncovered when combing through organizations' externally facing assets:



Attack surface varies by sector. Average number of exposed assets by industry, based on ASD data.

The healthcare sector had the most expansive attack surface of industries reviewed, with a digital footprint of nearly 5,500 subdomains and over 3,000 combined web apps and IP addresses per organization. This tracks with the industry's need to balance various public-facing assets, whether assisting patients with scheduling or supporting collaboration on medical research.

Financial services came in a close second as banking institutions shifted more activities and transactions online.

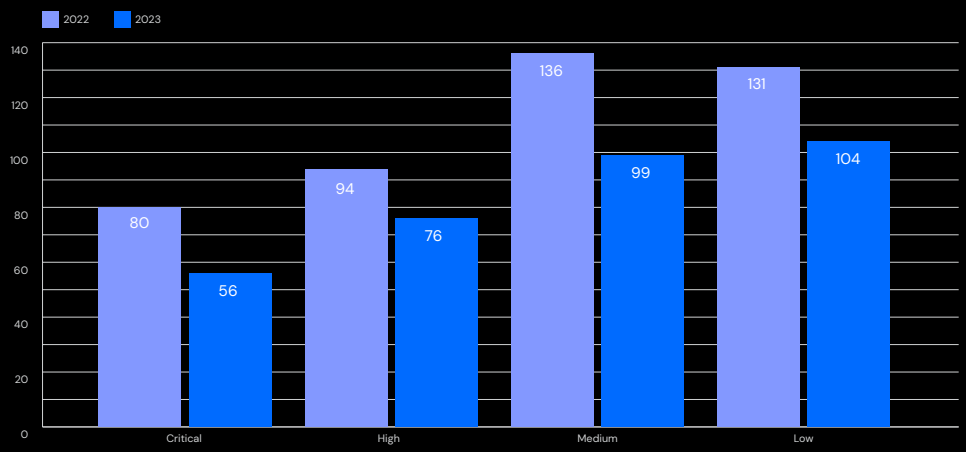
The U.S. federal government, meanwhile, has had to balance the need to enable public access to critical services like health insurance while minimizing the number of external IP addresses that could become targets for attackers. And the technology and manufacturing sectors each have their own deep tech stacks to manage.

Synack customers reduced time to remediation

Average time to remediation, measured in days

Despite mounting pressure on security teams, Synack clients reduced their mean time to remediation for critical severity vulnerabilities by **24 days**, while high severity vulns were remediated in **18 fewer days**.

Comparison of remediation days for 2022 and 2023



SRT SPOTLIGHT

New tech, old techniques

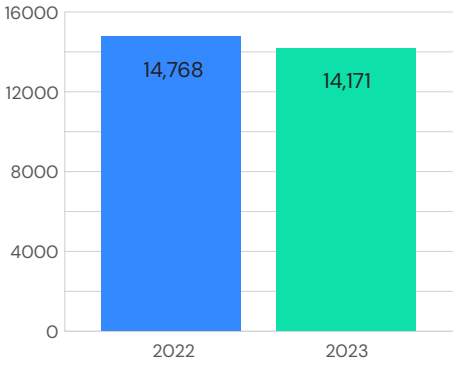
The advent of generative AI has introduced entirely new categories of vulnerabilities particular to large language models and other machine learning systems. But as AI chatbots and tools spread, traditional security risks haven't gone away, as Synack Red Team member *nullgOre* has discovered firsthand in his testing.

"Standard attacks against AI/ML infrastructure are just as viable as the latest 'hotness' of performing prompt injection attacks or any of the interesting new attack classes that have been created since the explosion of AI/ML in the daily lives of people around the world," nullgOre said.

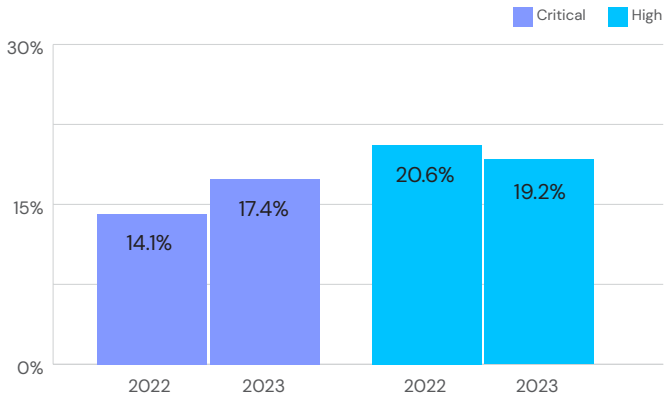
Critical & high-severity vulns are on the rise across industries

While we saw a slight drop in total vulnerabilities, customers experienced more critical-severity vulnerabilities and about the same number of high-severity flaws. This makes the reduced time to remediation that much more impressive.

Comparison of total vulns for 2022 and 2023



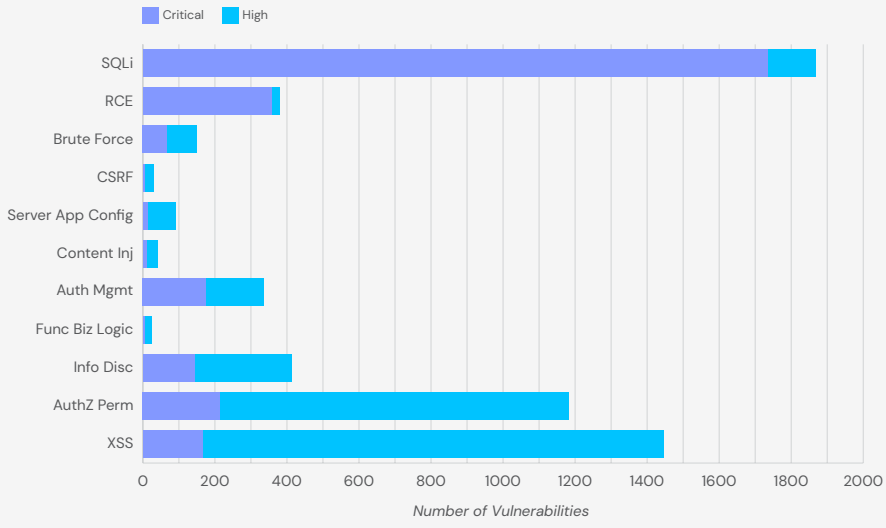
Comparison of share of critical and high vulnerabilities in 2022 and 2023 for all Synack customers



Severity Breakdown by Vulnerability Category

The same categories of vulnerabilities persist year after year, exposing security gaps as critical as they are predictable. SQL injections crop up for customers as steadily as a metronome, and remote code execution flaws are a consistent headache for security teams. While securing tech development is a systemic problem, organizations can at least identify vulnerability trends on their attack surface to source a root cause. Does a team of developers need additional code review or more security education? Are systems and networks segmented appropriately?

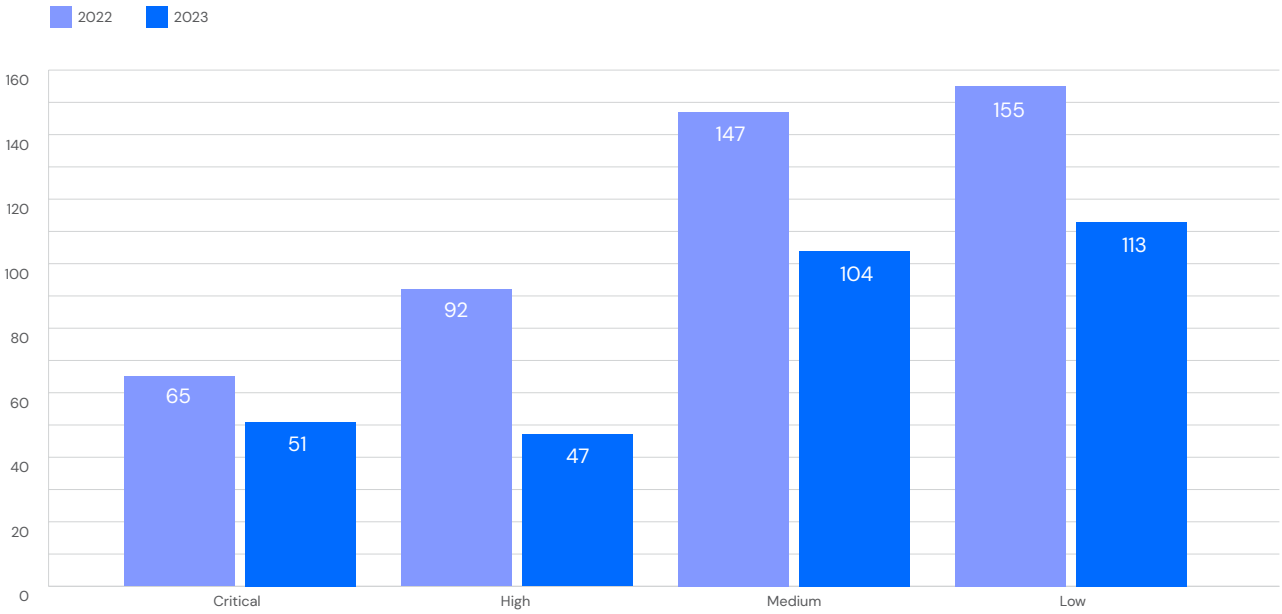
Distribution of vulnerabilities by type and segmented by critical and high severity



Healthcare

Hats off to our healthcare clients, who reduced time to remediation of critical vulnerabilities by an average of **14 days**. Even more impressive is the remediation time on high-severity vulns—a **45-day** reduction.

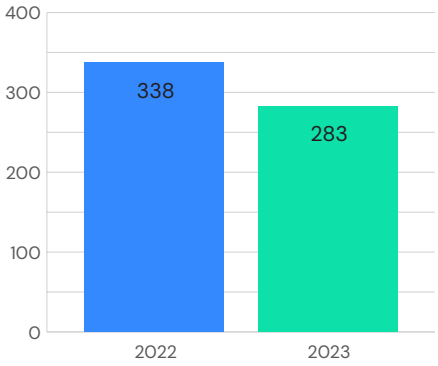
Comparison of time to remediation, measured in days, in 2022 and 2023 for healthcare clients



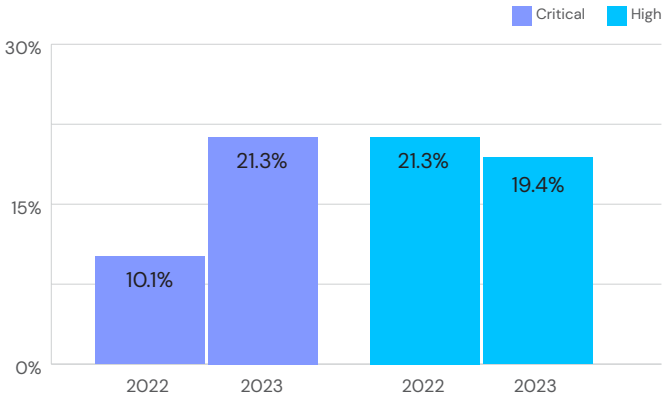
Healthcare systems have been under siege in recent months, and some threat groups have demanded (and received) top dollar ransoms in the fallout of successful breaches. There's no shortage of attack vectors that healthcare security teams have to contend with—HVAC systems, medical devices, even Xboxes provided for pediatric patients.

In 2022, critical vulnerabilities made up 10.1% of healthcare vulnerabilities found and 21.3% were high severity. In 2023, the critical vuln distribution jumped to 21.3% and the high-severity vulns stayed steady at 19.4%.

Comparison of total vulns for 2022 and 2023



Comparison of share of critical and high vulnerabilities in 2022 and 2023 for healthcare clients

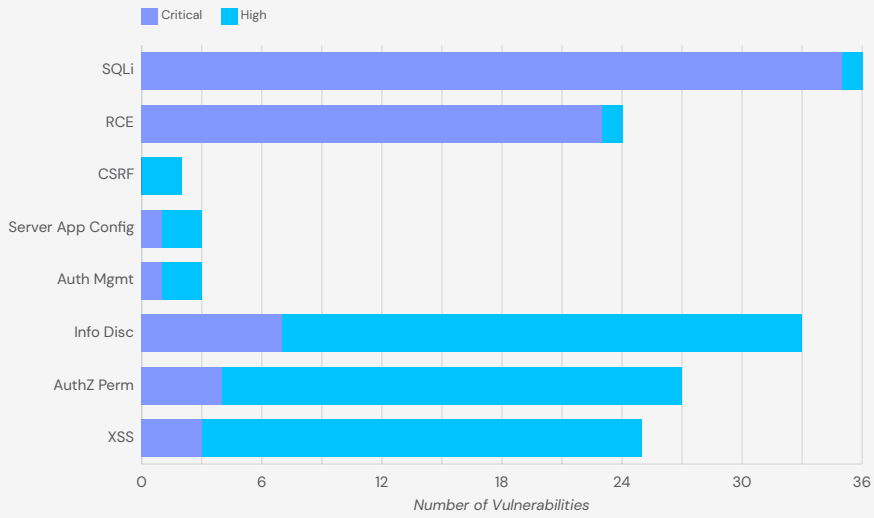


Severity Breakdown by Vulnerability Category

The shifting distribution of vulnerability categories shows remote code executions and SQL injections trending up amid an overall rise in vulnerability severity. Vulnerabilities tied to authorization permissions and cross-site scripting have dropped, but rank higher in severity when found.

As increasingly complex systems, hospitals and healthcare settings have an uphill battle for vulnerability management and remediation. But it doesn't mean that there isn't a way to improve—faster and more effective remediation helps to keep attackers from being able to find critical footholds into the system.

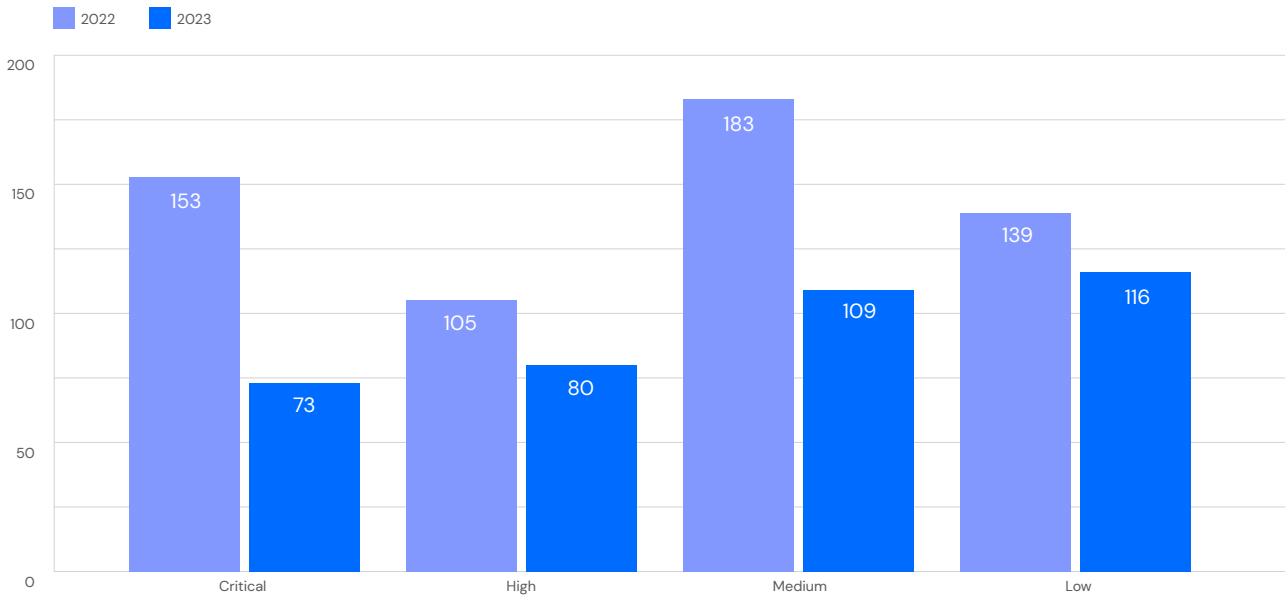
Distribution of vulnerabilities by type and segmented by critical and high severity



Financial Services

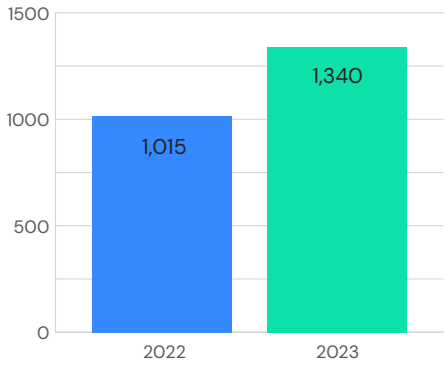
Financial service customers saw a reduction in time to remediation for both critical and high vulnerabilities (there was a reduction across all severity types). They reduced remediation time of critical vulnerabilities by **80 days** and high-severity vulns by **15 days.**

Comparison of time to remediation, measured in days, in 2022 and 2023 for financial service clients

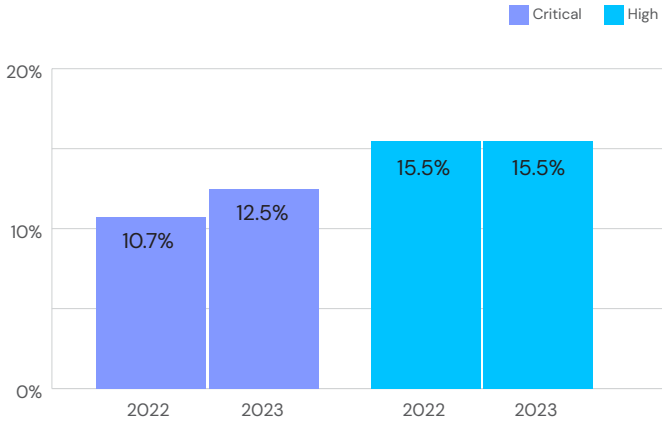


In 2022, critical vulns made up 10.7% of financial services vulnerabilities found, and 15.5% were high severity. In 2023, critical vulnerabilities increased slightly to 12.5%, while high-severity ones remained the same at 15.5%.

Comparison of total vulns for 2022 and 2023



Comparison of share of critical and high vulnerabilities in 2022 and 2023 for financial services clients

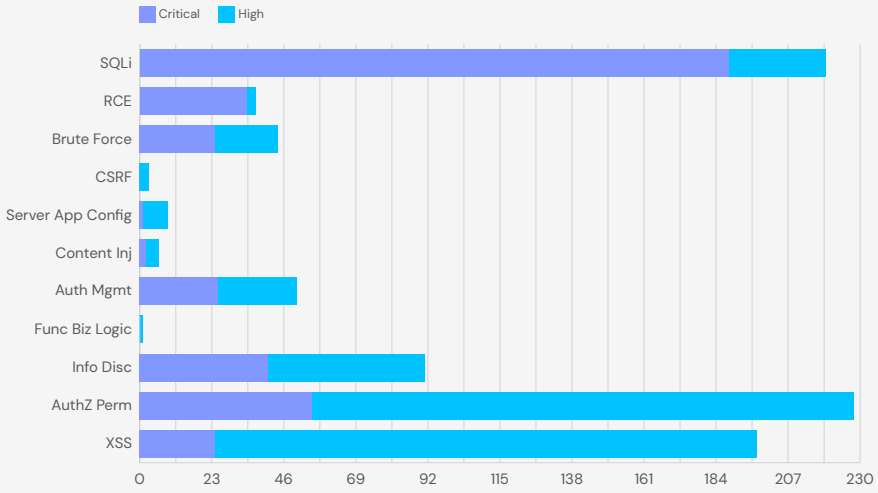


Severity Breakdown by Vulnerability Category

Last year saw more critical or high vulnerabilities from categories like cross-site scripting, insecure authorization permissions and a huge jump in SQL injections.

As business operations rely more heavily on APIs, allowing applications, systems, and databases to communicate data efficiently, these additional attack vectors invite new threats.

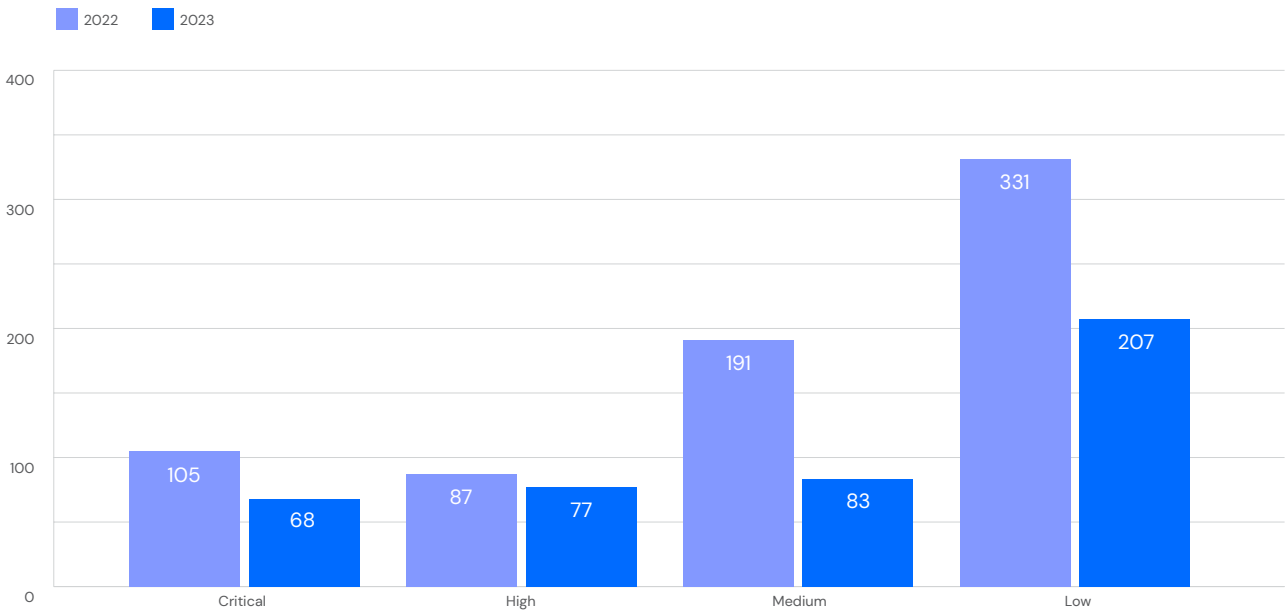
Distribution of vulnerabilities by type and segmented by critical and high severity for financial services clients in 2023



Federal Government

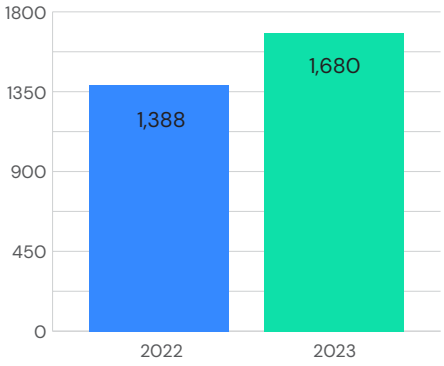
Departments and agencies of the U.S. federal government reduced their remediation time for critical vulnerabilities by **37 days** and high-severity vulnerabilities by **10 days**.

Comparison of time to remediation, measured in days, in 2022 and 2023 for federal government clients

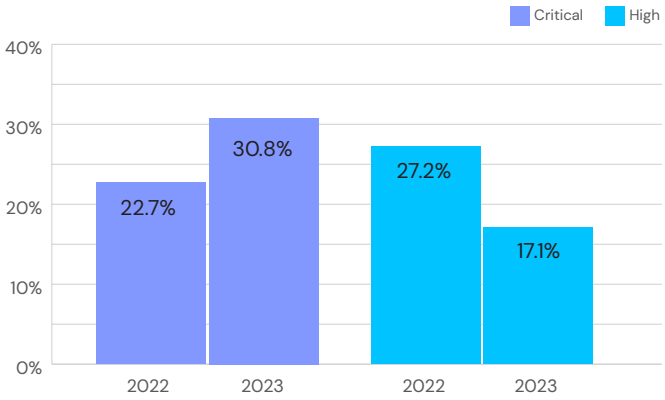


Critical vulnerabilities increased for federal government clients, from 22.7% in 2022 to 30.8% in 2023. High-severity vulnerabilities fell from 27.2% of all vulnerabilities to 17.1%.

Comparison of total vulns for 2022 and 2023



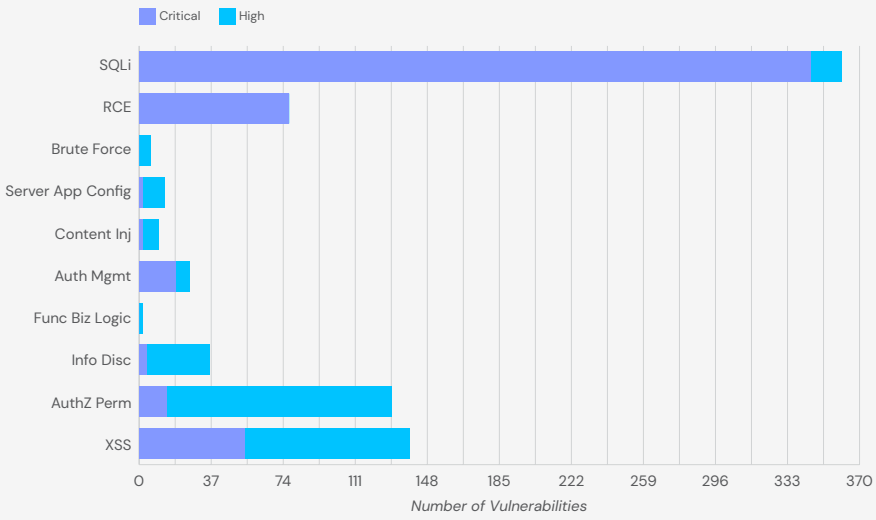
Comparison of share of critical and high vulnerabilities in 2022 and 2023 for federal government clients

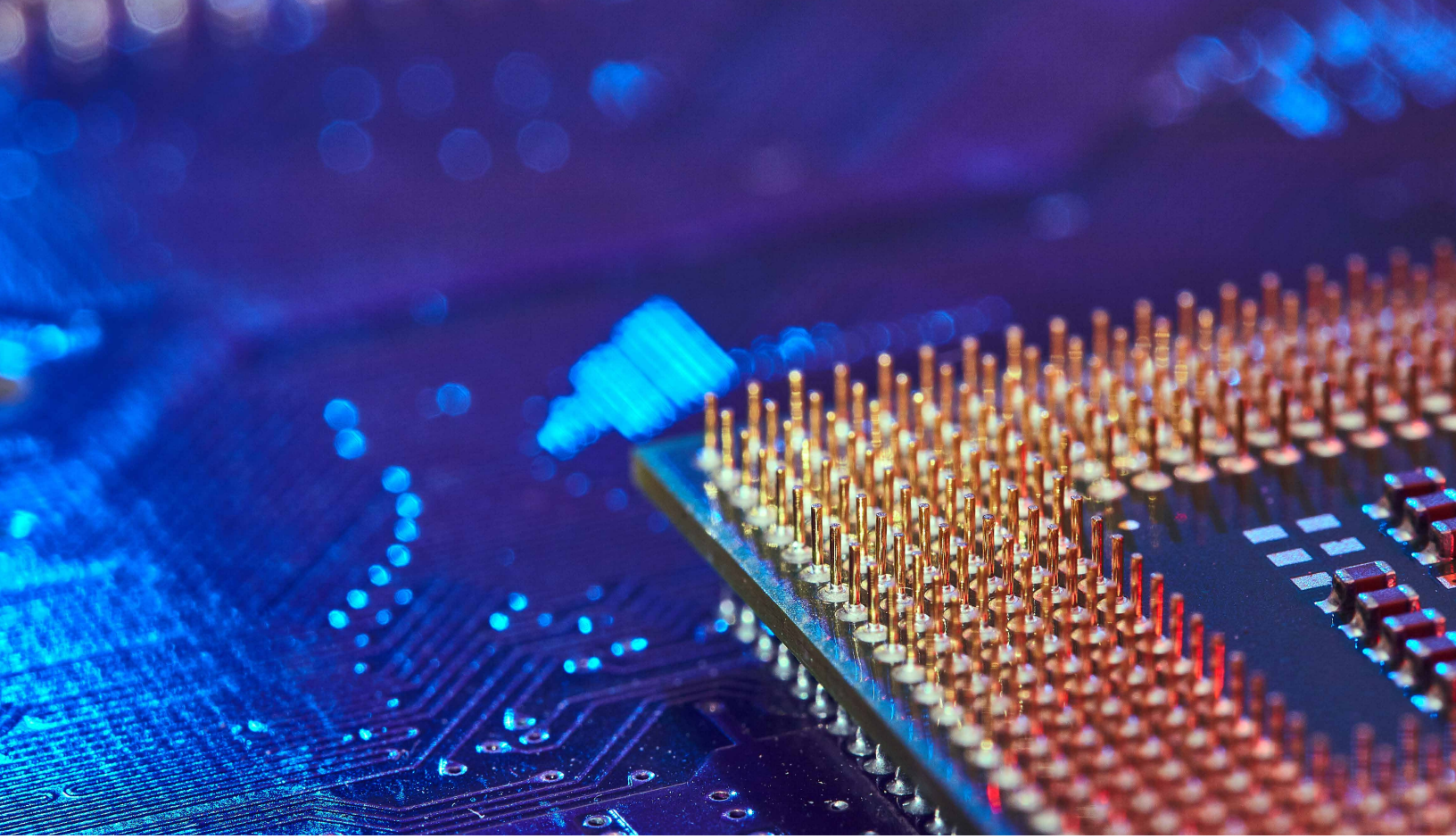


Severity Breakdown by Vulnerability Category

Finding fewer remote code execution vulns and brute force attacks is good news for the federal government, but a spike in SQL injections and other content injections — along with cross-site scripting — tells a story of insecure databases.

Distribution of vulnerabilities by type and segmented by critical and high severity for federal government clients in 2023

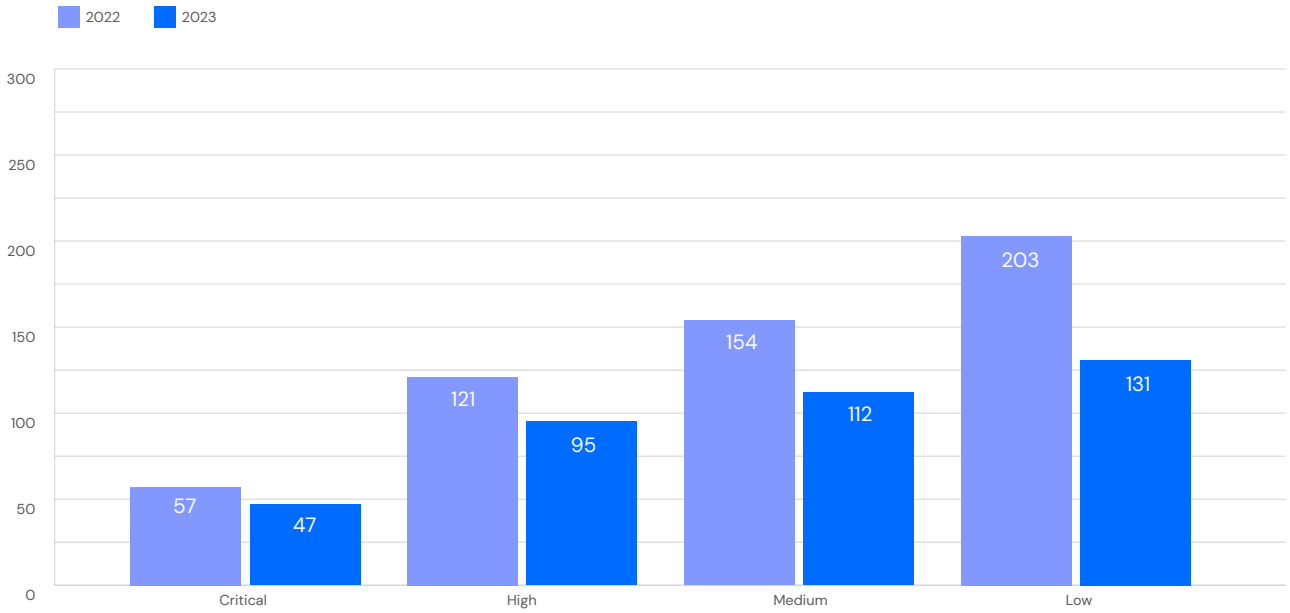




Technology

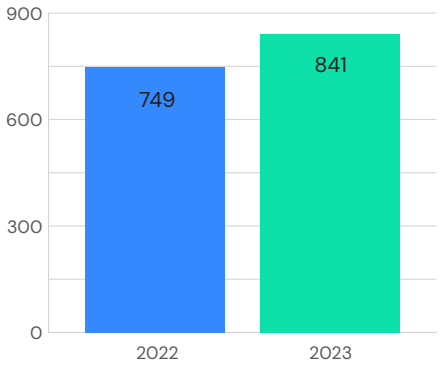
Technology sector customers saw a dramatic reduction in remediation time for high-severity vulnerabilities, solving for them in **26 fewer days**. Meanwhile, it took them **10 fewer days** to resolve critical vulnerabilities.

Comparison of time to remediation, measured in days, in 2022 and 2023 for technology clients

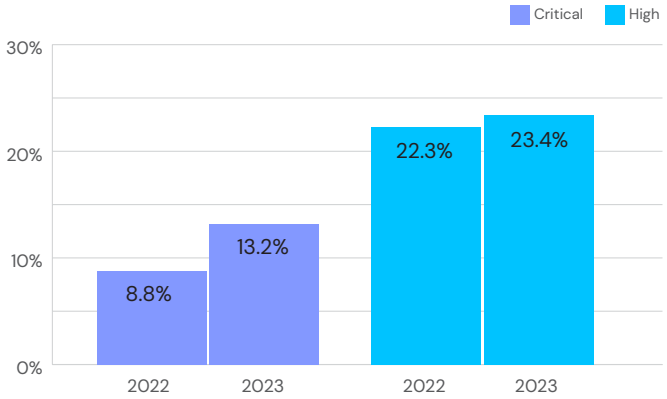


Technology's share of critical and high vulnerabilities shot up, however. In 2022, only 8.8% of software flaws were critical and 22.3% were high severity, while last year those figures were 13.2% and 23.4%.

Comparison of total vulns for 2022 and 2023



Comparison of share of critical and high vulnerabilities in 2022 and 2023 for technology clients

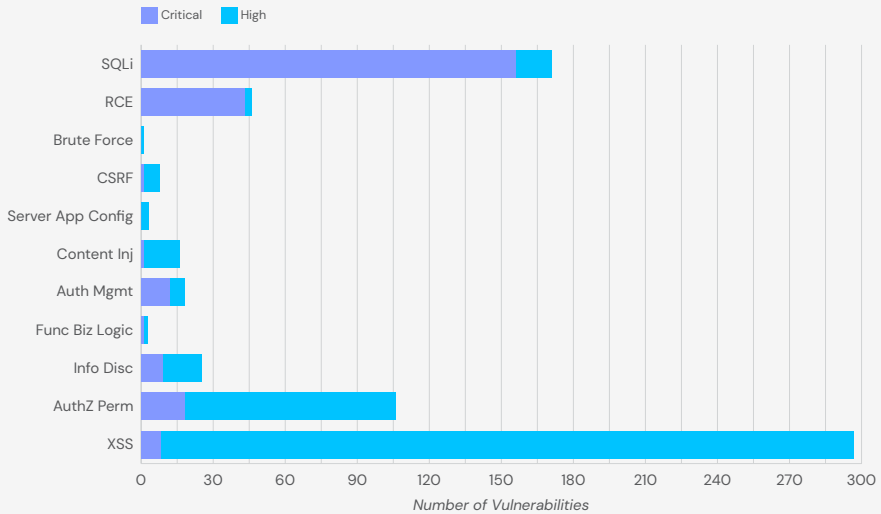


Severity Breakdown by Vulnerability Category

With continuous testing and vulnerability reporting, tech organizations still reduced their mean time to remediate these high and critical vulns. Enterprises with mature testing programs could leverage analysis in the Synack Platform to see which business units needed to level up their secure coding skills.

Again, SQL injections and remote code executions increased in 2023, as did the severity of cross-site scripting vulnerabilities.

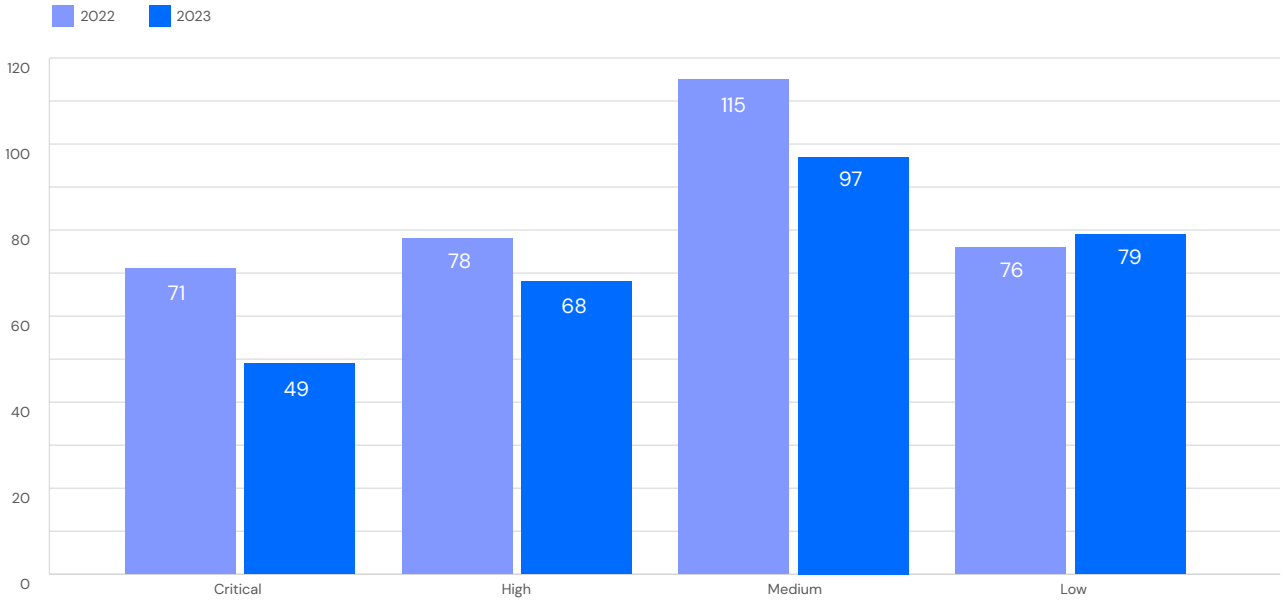
Distribution of vulnerabilities by type and segmented by critical and high severity for technology clients in 2023



Manufacturing

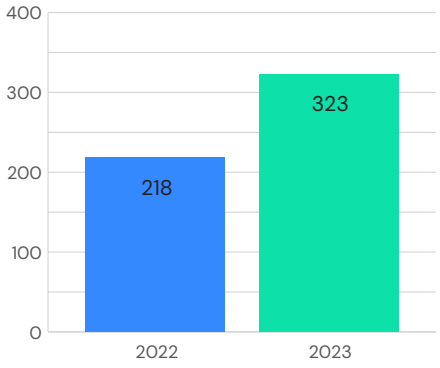
The manufacturing sector reduced critical vulnerability remediation by **22 days** and high-severity vuln remediation by **10 days.**

Comparison of time to remediation, measured in days, in 2022 and 2023 for manufacturing clients

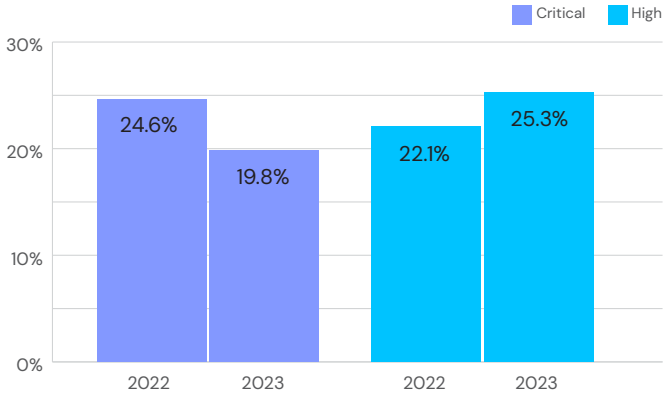


Synack Red Team members found fewer critical and high-severity vulnerabilities for this sector last year. In 2022, critical vulnerabilities accounted for 24.6% of all vulns, while 22.1% were considered high severity. In 2023, critical vulnerabilities dipped to 19.8%, but high-severity went up to 25.3%.

Comparison of total vulns for 2022 and 2023



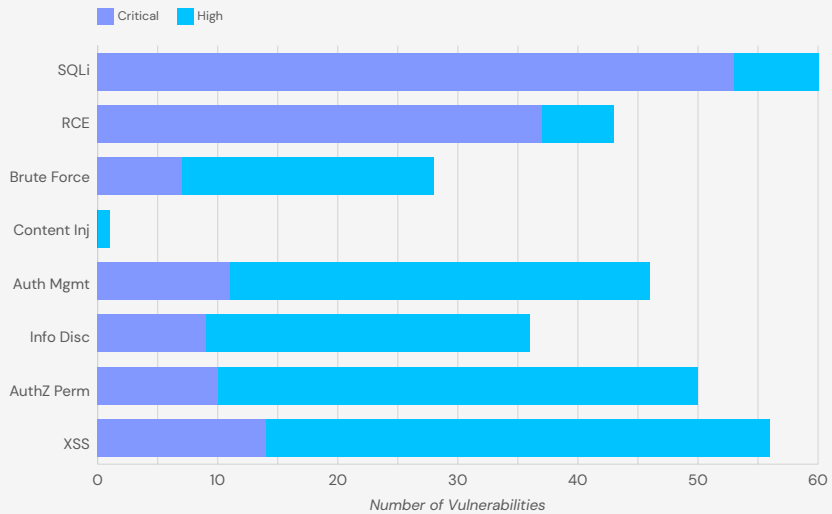
Comparison of share of critical and high vulnerabilities in 2022 and 2023 for manufacturing clients



Severity Breakdown by Vulnerability Category

Many sectors, including manufacturing, are at a crossroads of digital transformation. Connect too much of the manufacturing process to digital tools and you risk a breach or attack taking down your core business, but these industries need to integrate to stay competitive.

Distribution of vulnerabilities by type and segmented by critical and high severity for manufacturing clients in 2023

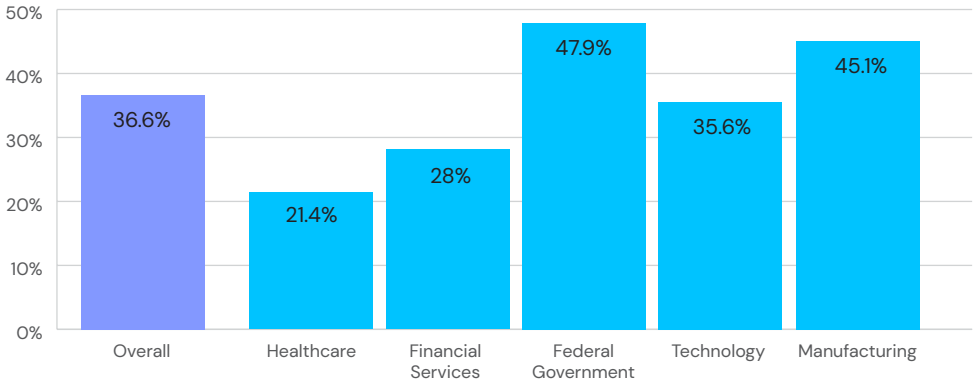


Industry Comparisons

Industries face different levels of security risks. Factors that differentiate an industry's security posture include: size of tech stack, complexity of tech stack, nature of business, company size, remote workers, supply chain and more.

In 2023, almost 37% of all vulnerabilities found by Synack were critical or high-severity. Using that statistic as a baseline, we compared the industries highlighted in this report. Manufacturing and the federal government had the largest share of critical and high-severity with 45.1% and 47.9% respectively. On trend was technology with 35.6%. Finally, financial services and healthcare fell below with 28% and 21.4% respectively.

Share of critical and high-severity vulnerabilities by industry



SRT SPOTLIGHT

AI shakes up security testing

Cutting-edge GenAI tools are already accelerating the security researchers' ability to uncover vulnerabilities.

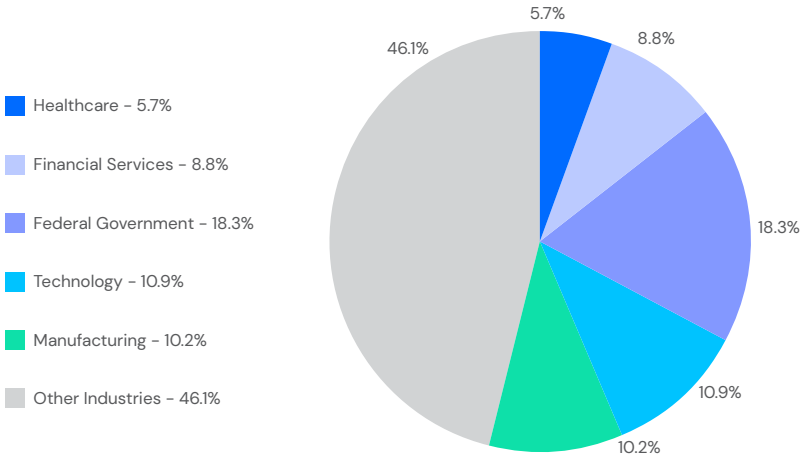
Synack Red Team member *Nicolas Krassas* recently used ChatGPT when conducting a security test on a target with an exposed Redis server. (Redis is a popular in-memory database that many organizations use to handle data they want to be able to access quickly.)

"The problem was that the specific system had a very large number of data entries, and using Metasploit was not possible because the Redis Extractor module was crashing," Krassas said. So he used ChatGPT to help him write a Python script that could iterate through different Redis keys and obtain just the first 20 entries associated with them. *"This allowed me to demonstrate to the team in a better way the results obtained from the server without stressing the client infrastructure."*

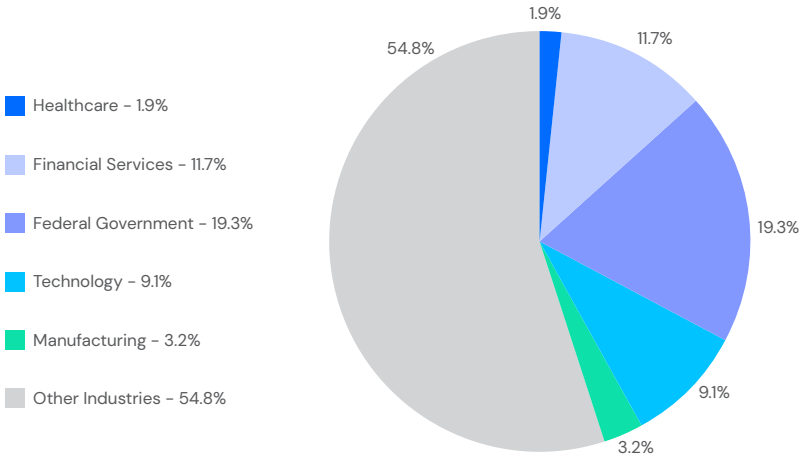
Makeup of SQLi and RCE vulnerabilities by industry

In 2023, SQL injections and remote code executions are typically vulnerabilities that could have the biggest impact on an organization if exploited by a bad actor. Of all critical and high-severity SQLi and RCE vulnerabilities found for Synack clients, we mapped how much each highlighted industry is contributing to those pernicious vuln categories.

SQLi vulnerabilities by industry



RCE vulnerabilities by industry



CONCLUSION

Vulnerabilities persist across various assets, whether cloud, API, host, infrastructure, web apps or even AI/LLMs. As the software development life cycle has sped up for many Synack clients, they've cut the time to remediate critical software flaws, a trend we hope holds in 2024.

But 56 days — the average time it took Synack customers to remediate a critical vulnerability last year — still offers too large a window for attackers to break through, especially with the specter of using AI to automate the exploitation of simpler vulnerability categories like SQLi. This is a metric we should look to reduce to hours, not days or weeks, a goal that necessitates a different approach to pentesting.

In a sea of CVEs, simply managing vulnerabilities, let alone addressing their root causes, is a daunting task for even mature security teams. By combining continuous, human-led pentesting with quality data analysis, Synack's Penetration Testing as a Service (PTaaS) platform clears the way for customers to focus on flaws that can actually be exploited. To learn more about PTaaS and vulnerability trends, please visit www.synack.com.

What sets Synack apart?

Learn more →