
secpod
Q3 Vulnerability Report 2025
www.secpod.com

Executive Summary

Unified Security Intelligence as a Strategic Enabler of Continuous Vulnerability and Exposure Management.

The Q3 threat landscape underscores a continued escalation in enterprise risk, marked by an 11% increase in total vulnerabilities from the previous quarter and a mid-quarter surge in critical exposures. August alone saw 540 critical vulnerabilities, reflecting attackers' growing sophistication and agility in weaponizing new flaws.

In this context, Unified Security Intelligence (USI) continues to emerge as a strategic enabler of proactive cyber defense. USI consolidates vulnerability intelligence, exploit data, misconfiguration findings, and patch analytics into a single, unified operational layer, delivering end-to-end visibility and actionable context across endpoints, servers, network infrastructures and cloud infrastructures.

This quarter, USI expanded coverage to 5,962 CVEs, including 34 zero-days and 115 CISA Known Exploited Vulnerabilities (KEVs), reflecting enhanced responsiveness to real-world attack data. The platform's deep visibility into 751 misconfigurations, 970 CRE-mapped remediations, and 851 patch controls demonstrates its ability to translate security findings into measurable risk reduction.

Where traditional tools remain fragmented, USI provides a single source of truth that correlates exploitability, exposure, and business impact, enabling security leaders to:

- **Quantify and communicate exposure:** From critical zero-days in Cisco, Ivanti, and NetScaler products to mid-tier CVEs driving lateral movement across cloud and infrastructure software.
- **Enforce consistent controls:** Through CRE (Common Remediation Enumeration)- and CCE (Common Configuration Enumeration)-aligned remediation standards spanning Windows, macOS, and Linux environments.

- **Prioritize with intelligence:** By mapping exploit data, CVSSv4 metrics, and business context for faster, risk-based remediation.

The Q3 data also highlights USI's expanding multi-cloud intelligence, monitoring 164 AWS and 80 Azure resource types, along with 379 AWS CSPM (Cloud Security Posture Management), 188 Azure CSPM rules, 152 AWS CSPA (Cloud Security Posture Anomaly) rules, 54 Azure CSPA rules, 28 AWS CIEM (Cloud Infrastructure Entitlement Management) rules & 24 Azure CIEM rules. These advances reinforce unified risk visibility and governance across hybrid and multi-cloud infrastructures.

Importantly, USI continues to drive the industry shift from reactive patching to continuous vulnerability and exposure management (CVEM), where detection, prioritization, and remediation operate in near real time to keep pace with evolving threats and business-critical risks.

Table of Contents

Q3 Key Highlights & Trends

Vulnerability trends continued to intensify in Q3, highlighting the growing complexity of enterprise security risks.

11% — **increase in total vulnerabilities compared to Q2, reflecting sustained exposure across expanding digital infrastructures.**

540 — **Critical vulnerabilities surged mid-quarter, peaking in August with 540 instances, indicating a period of heightened exploit activity.**

34 — **zero-day vulnerabilities detected, more than doubling from Q2, emphasizing the urgency for proactive detection and faster patch cycles.**

115 — **CISA Known Exploited Vulnerabilities covered, reinforcing the need for ongoing alignment with global advisories and federal directives.**

40+ — **widely exploited and high-fidelity vulnerabilities were tracked, showing that attackers continue to weaponize fresh flaws despite improved remediation.**

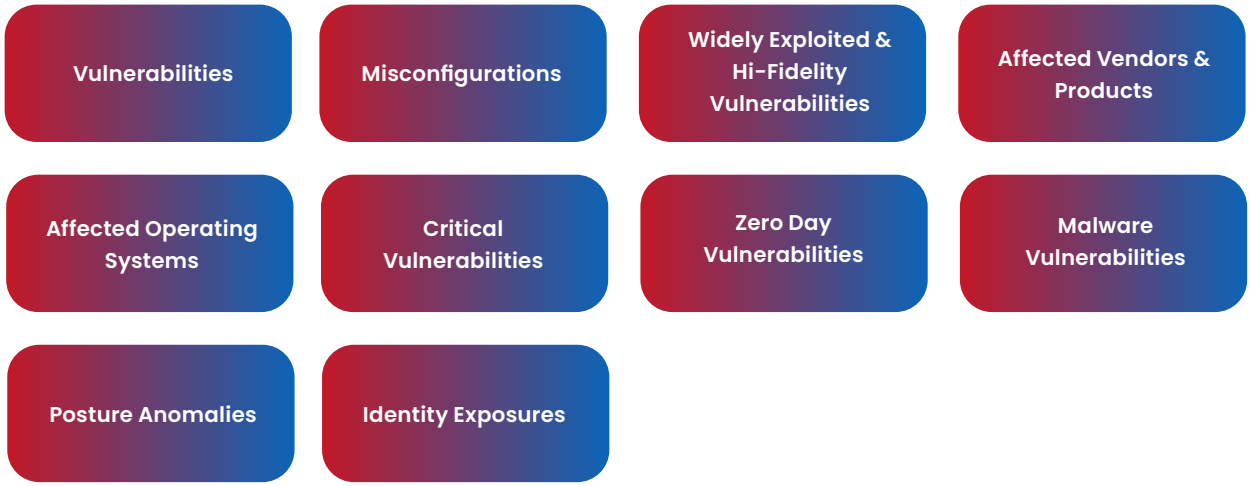
94 — **malware-linked vulnerabilities highlight growing intersections between ransomware, backdoor, and persistent threat groups.**

48% — **AWS and Azure coverage expanded dramatically, with a 48% rise in AWS resource monitoring and a 22% increase in Azure CSRM rules, strengthening unified cloud visibility and compliance.**

These findings reaffirm the value of Unified Security Intelligence (USI) in consolidating detection, prioritization, and remediation, turning fragmented data into actionable insights that help organizations stay ahead of evolving threats.

Report Coverage Areas

This quarter's report provides a comprehensive analysis of the global vulnerability landscape, covering critical areas that define enterprise risk posture.



Q3 Report Coverage

For Endpoints, Network Infrastructure and Servers

The data for Q3 continues to highlight how Unified Security Intelligence (USI) consolidates multiple security checks into a unified source of truth, empowering security teams to see, prioritize, and remediate risk in one place. The growing dataset reflects stronger coverage across vulnerabilities, configurations, and critical security intelligence.

CVEs Covered: 5,962

SecPod's USI continuously ingests and correlates new vulnerability data, ensuring no critical CVE is left untracked. This quarter's expanded coverage demonstrates its capability to adapt dynamically to the evolving threat landscape.

Misconfigurations & CCEs: 751

The consistent mapping between CCEs and misconfiguration findings reinforces USI's commitment to standardized and actionable security controls.

Local Checks 5,848 vs. Remote Checks 828

Q3 shows a continued emphasis on deep host-level visibility, covering patch levels, configurations, registry settings, and file integrity, while also improving external exposure scans. The higher number of local checks underscores strong endpoint assurance, while the increased remote checks highlight progress in perimeter and risk mapping.

Zero-Days Covered: 34

USI's real-time ingestion and tagging of zero-day data more than doubled this quarter, reflecting faster detection of critical exposures before exploit kits go public, helping security teams move from reaction to prevention.

CISA Vulnerability Coverage: 115

By automatically mapping to CISA's Known Exploited Vulnerabilities (KEV) list, USI helps organizations maintain compliance with U.S. federal directives while proving due diligence during internal and external audits.

Network Device Vulnerabilities: 828

USI continues to track vulnerabilities across routers, switches, and firewalls, enabling unified visibility across both device and network security layers.

The patching and remediation metrics reflect how USI drives end-to-end risk reduction, from discovery to remediation:

- **Comprehensive CRE Mapping: 970**

  USI aligns each remediation to the Common Remediation Enumeration standard, ensuring traceability across Windows, macOS, and Linux.

- **Third-Party Application Coverage: 571**

  By integrating vendor advisories and community feeds, USI brings third-party patches into the same view as OS updates.

- **Configuration Remediation: 540**

  Misconfigurations are treated with the same urgency as vulnerabilities, integrated into compliance and automation workflows.

- **Patch Coverage: 851**

  With continuous orchestration across environments, USI ensures timely, automated patch deployment and verification.

Q3 Coverage

Endpoints, Network Infrastructure and Servers

Total Number of CVEs Covered

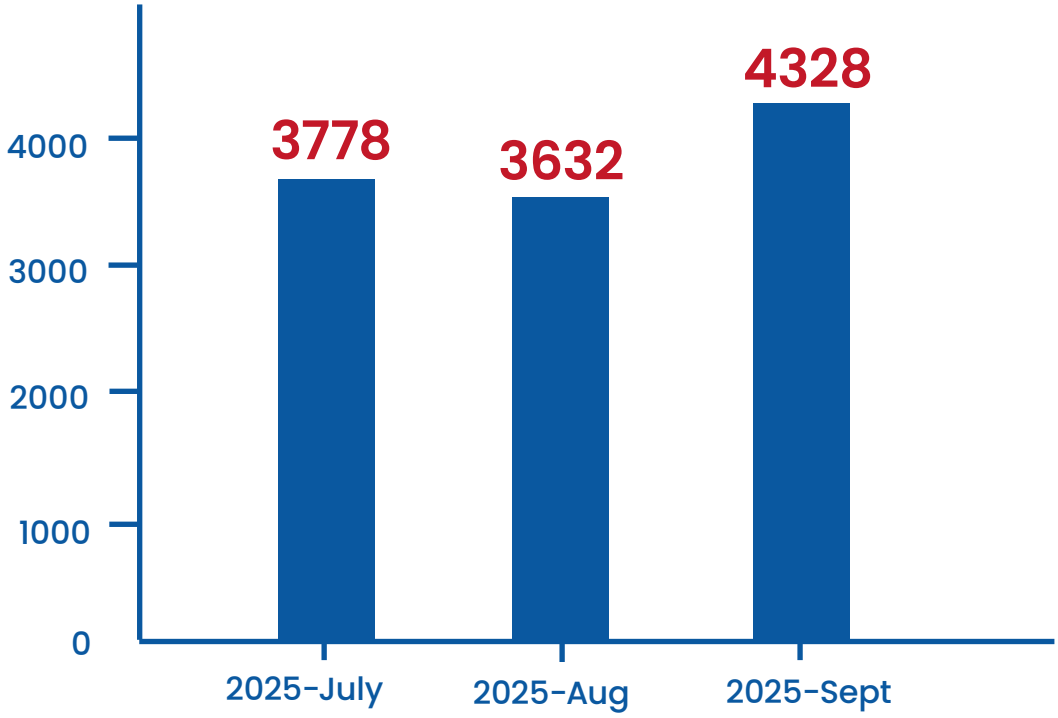


Figure 1: Shows the Number of vulnerabilities published from July to September 2025

In Q2, 5,711 CVEs were identified, but a closer look The vulnerability trend across reveals dynamic shifts in the global threat landscape. SecPod's unified security intelligence detected a consistent volume of vulnerability disclosures, underscoring the growing complexity of modern IT ecosystems.

- **July 2025: 3,778 vulnerabilities** were reported, marking the start of a sustained period of high exposure.
- **August 2025: The numbers slightly dipped to 3,632,** reflecting temporary stabilization, possibly due to delayed vendor patch releases.
- **September 2025: Vulnerabilities surged to 4,328,** indicating renewed threat activity, particularly across cloud and infrastructure software categories.

These fluctuations highlight the need for continuous visibility, contextual prioritization, and automated remediation powered by unified security intelligence. The correlation of vulnerability growth with evolving attack surfaces emphasizes that reactive patching alone is insufficient; proactive cyber hygiene is critical.

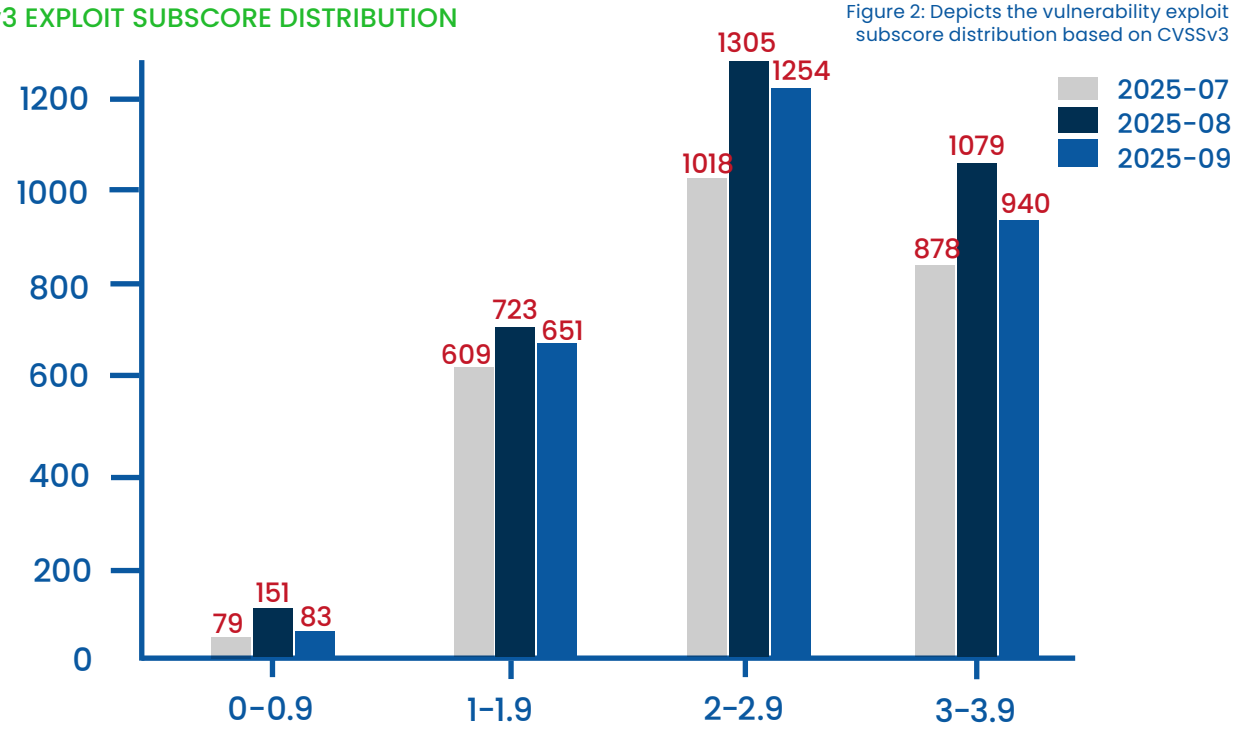
RISK INSIGHT

The risk in vulnerabilities shows a high-risk posture for organizations with unpatched or poorly managed assets. The concentration of vulnerabilities in September suggests heightened attacker focus on unmonitored systems. Continuous vulnerability and exposure management is essential to minimize remediation time and strengthen enterprise resilience.

Vulnerability exploit and impact distribution based on CVSS v3

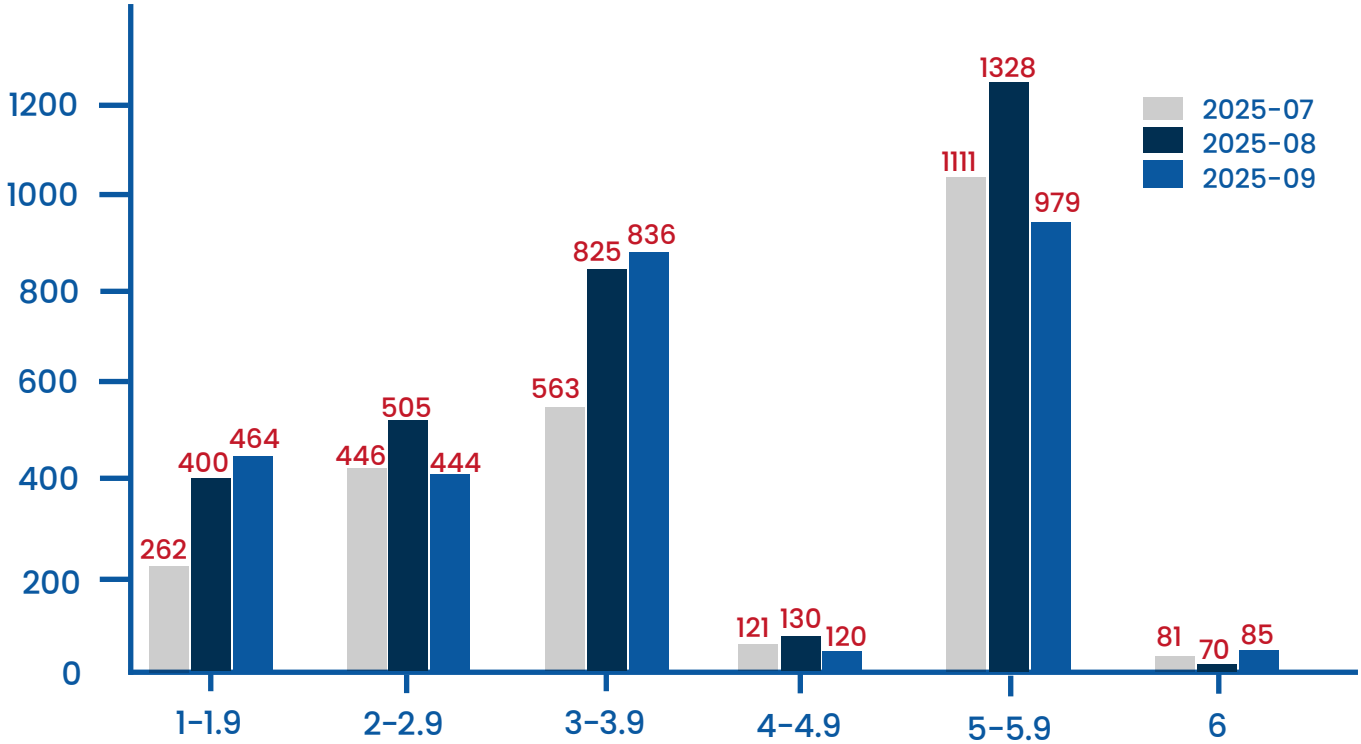
CVSSv3 EXPLOIT SUBSCORE DISTRIBUTION

Figure 2: Depicts the vulnerability exploit subscore distribution based on CVSSv3



CVSSv3 IMPACT SUBSCORE DISTRIBUTION

Figure 3: Depicts the vulnerability impact subscore distribution based on CVSSv3



Even as overall vulnerability volumes fluctuated through the quarter, the underlying exploit and impact risk remained consistently high. Here are some key observations.

Exploitability stayed persistently moderate-to-high
Across July to September, most vulnerabilities clustered in the 2.0–3.9 exploitability range, indicating that many flaws remained readily exploitable with limited attacker effort. August saw the highest surge, with over 1,300 CVEs scoring above 2.0.

Impact potential remained significant
Most vulnerabilities carried moderate-to-high business impact, concentrated in the 3.0–5.9 range. August again peaked, with over 1,300 vulnerabilities capable of causing operational disruption or data loss if exploited.

Mid-range CVEs continue to pose real risk
While few vulnerabilities reached the maximum scores, the broad middle layer remains widely weaponizable, often leveraged in chained attacks for lateral movement.

RISK INSIGHT

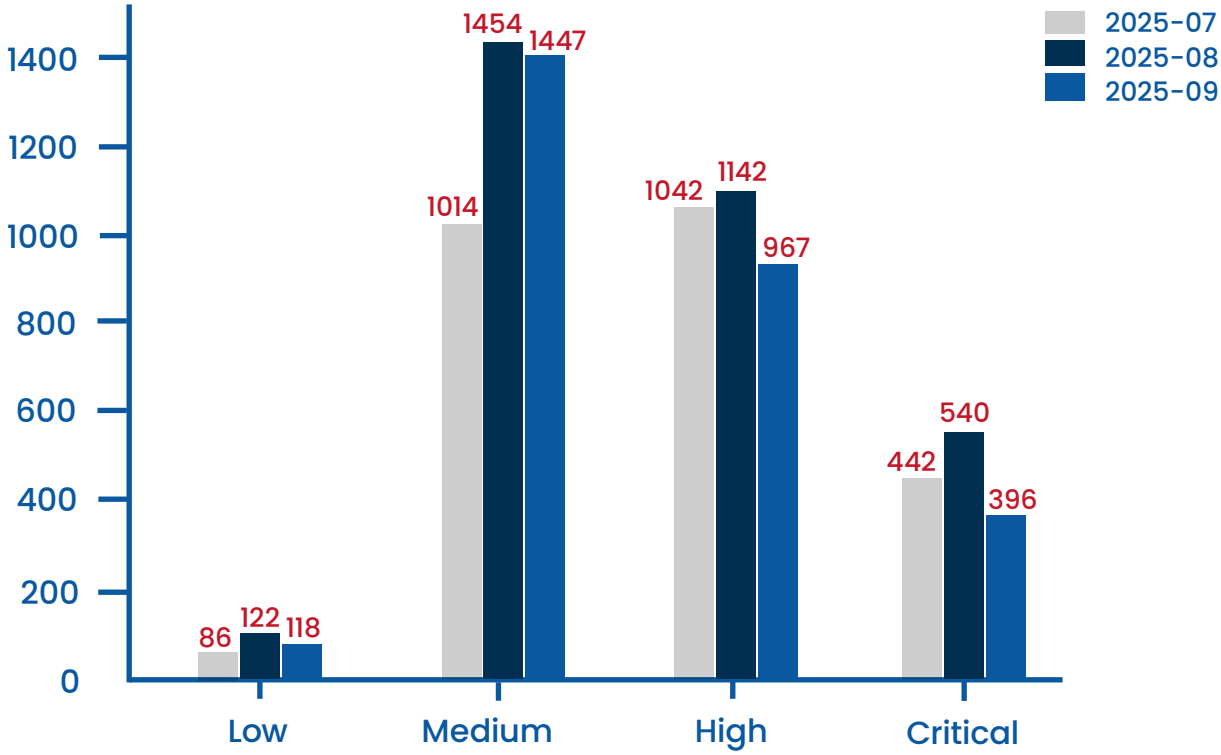
There is an immediate need for smarter risk prioritization with unified security intelligence, as most vulnerabilities fell in the moderate exploitability and impact range. These mid-range CVEs, though not critical, are highly weaponizable and often exploited first in real-world attacks. Relying solely on CVSS scores can lead to underestimating cumulative risk exposure.

Know more about risk prioritization.

Monthly CVSS V3 Distribution

MONTHLY CVSSv3 DISTRIBUTION

Figure 4: Depicts the vulnerability distribution monthly CVSS V3



Unified Security Intelligence doesn't just count vulnerabilities; it analyzes how their severity patterns shift over time to reveal evolving risk trends. The chart illustrates the distribution of low, medium, high, and critical vulnerabilities across the quarter:

- Critical vulnerabilities **peaked in August with 540**, surpassing both July (442) and September (396). This indicates a mid-quarter surge in high-impact, exploit-ready risks, demanding rapid response and tighter patch cycles.
- High and medium severity vulnerabilities remained consistently dominant, with each month logging **more than 900–1,400 CVEs.** This highlights that while critical spikes draw attention, persistent mid-tier risks continue to drive most enterprise exposure.
- **Low-severity vulnerabilities held steady** at comparatively low levels.

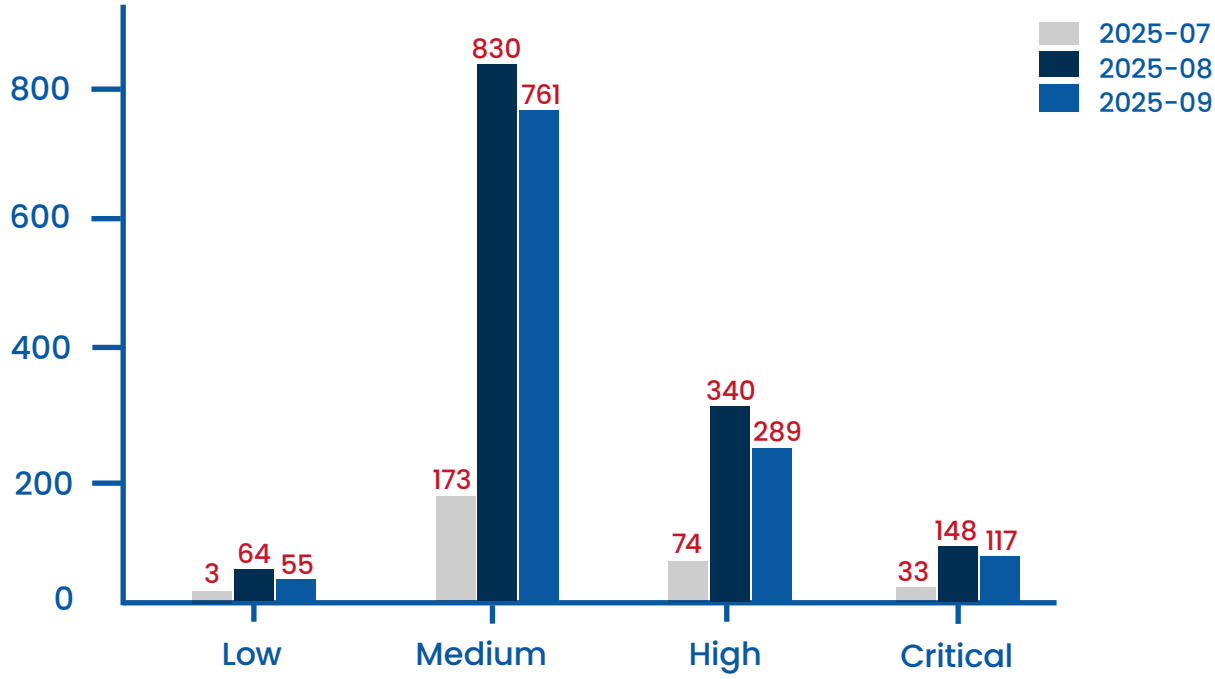
RISK INSIGHT

The August spike in critical vulnerabilities and persistent high-severity volumes show that exploit-ready risks remain elevated, demanding continuous, intelligence-driven prioritization to prevent surge in exposure.

Monthly CVSS V4 Distribution

MONTHLY CVSSv4 DISTRIBUTION

Figure 5: Depicts the vulnerability distribution monthly CVSS V4



As Unified Security Intelligence evolves, so does the way we evaluate vulnerability risk.

CVSSv4 introduces greater precision by factoring in exploit likelihood, environmental exposure, and business impact moving beyond static severity scores. This chart reveals a clear trend:

- **Medium-severity vulnerabilities** consistently dominate across the quarter reflecting the largest share of detected CVEs that demand sustained remediation focus.
- **High and critical vulnerabilities** form a smaller portion by count, yet carry elevated operational risk due to their exploit potential and urgency for patching.
- August shows a **sharp surge in overall vulnerability volume**, followed by a moderate decline in September signaling either improved remediation velocity or reduced new disclosures in the subsequent month.

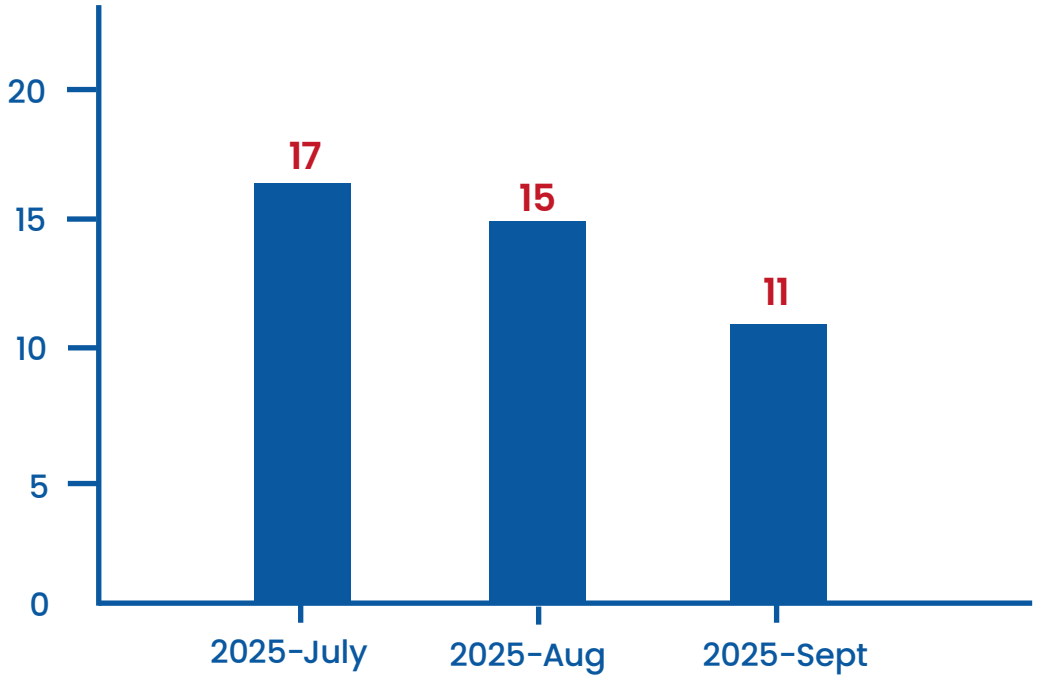
RISK INSIGHT

USI maps CVSSv4 insights to exploit likelihood and business impact, driving smarter, risk-based remediation.

Total Number of widely exploited & high fidelity vulnerabilities

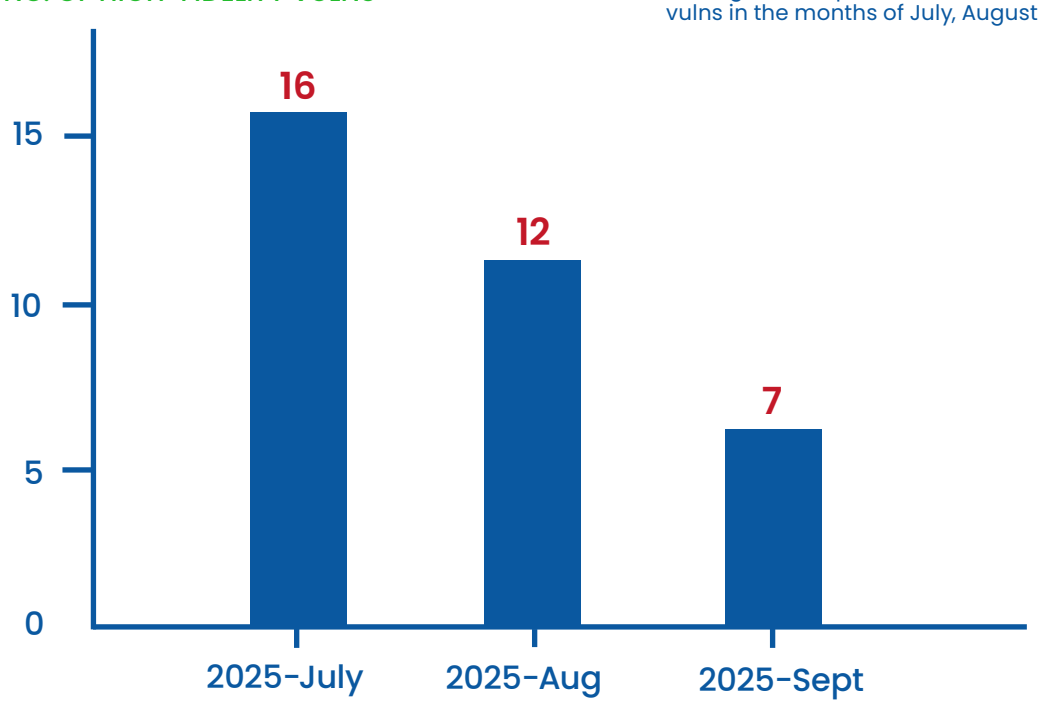
MONTHLY NO. OF WIDELY EXPLOITED VULNS

Figure 6: Depicts the total no. of widely exploited vulns in the months of July, August & September



MONTHLY NO. OF HIGH-FIDELITY VULNS

Figure 7: Depicts the total no. of high-fidelity vulns in the months of July, August & September



Along with detecting vulnerabilities, knowing which ones are actively exploited or carry high-fidelity risk is what makes Unified Security Intelligence (USI) indispensable.

By continuously ingesting exploit intelligence and prioritizing vulnerabilities that pose the greatest threat, USI ensures IT security teams focus on what truly matters:

- Widely exploited vulnerabilities remained high through July (17) and August (15) before dropping to 11 in September, reflecting a temporary slowdown in attacker activity.
- High-fidelity vulnerabilities followed a similar pattern, falling from 16 in July to 12 in August, and further to 7 in September indicating improved remediation and reduced exploit traction.

Despite the dip, double-digit counts of exploited vulnerabilities underscore that attackers continue to weaponize fresh exposures every month, demanding constant vigilance and prevention-first vulnerability management.

RISK INSIGHT

Although exploited and high-fidelity vulnerabilities declined through Q3, attackers continue to weaponize new flaws rapidly. Unified Security Intelligence (USI) bridges this gap by correlating global exploit data with organizational exposure, helping IT security teams spot and act on the most dangerous vulnerabilities first. Without such continuous, intelligence-driven prioritization, even short remediation delays can reopen critical risk windows.

Top 10 Affected Vendors/ Products

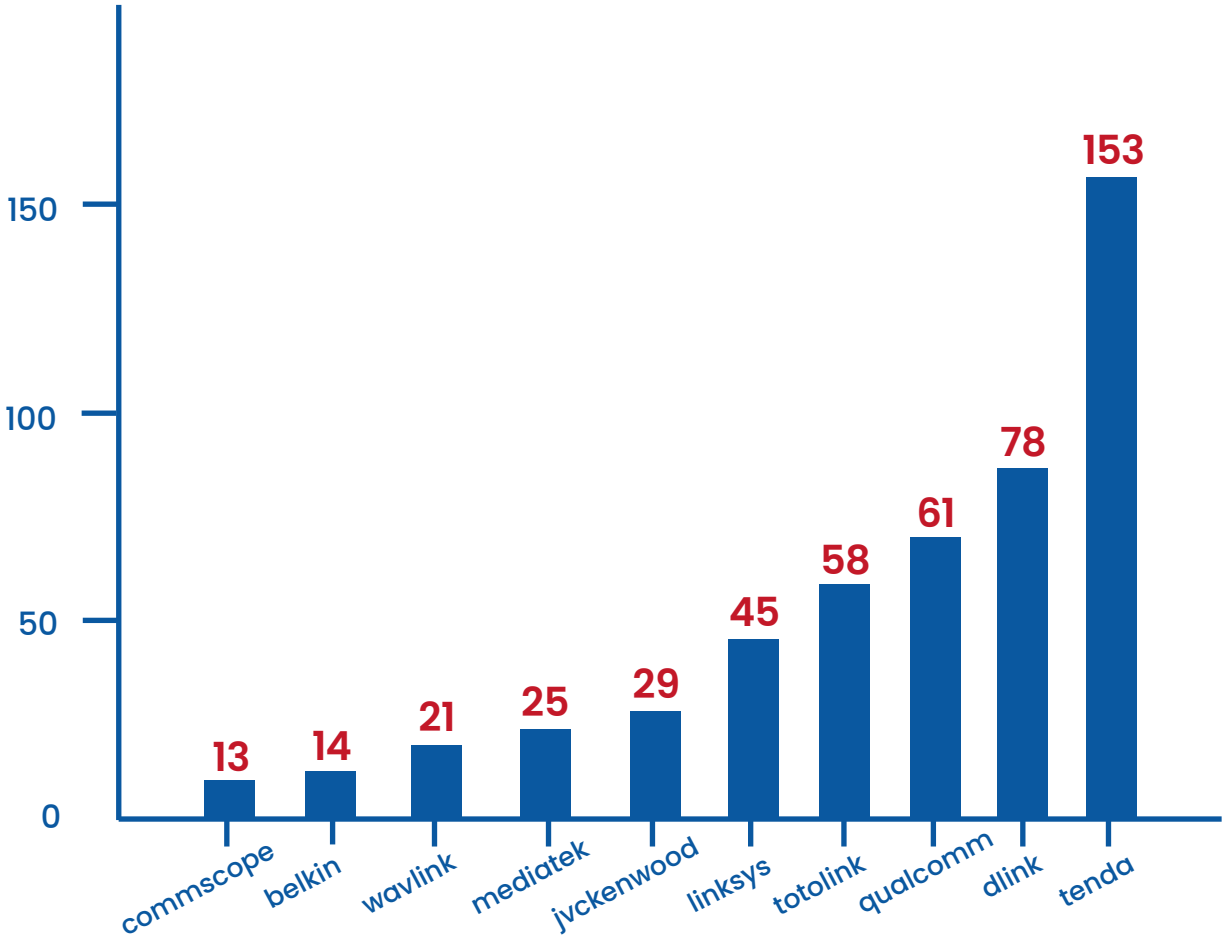


Figure 8: Shows the top affected Hardwares

As Unified Security Intelligence (USI) extends its visibility into hardware ecosystems, it highlights vendors with recurring vulnerability exposure. This chart reveals network and connectivity OEMs, notably Tenda, D-Link, and Qualcomm, as the most affected, reflecting persistent weaknesses in firmware and device security.

While brands like CommScope and Belkin show minimal counts, the 153 cases linked to Tenda indicate concentrated exposure that may warrant targeted mitigation and firmware compliance audits. USI's correlation of these hardware trends enables proactive patching, vendor accountability, and reduced attack surface across devices.

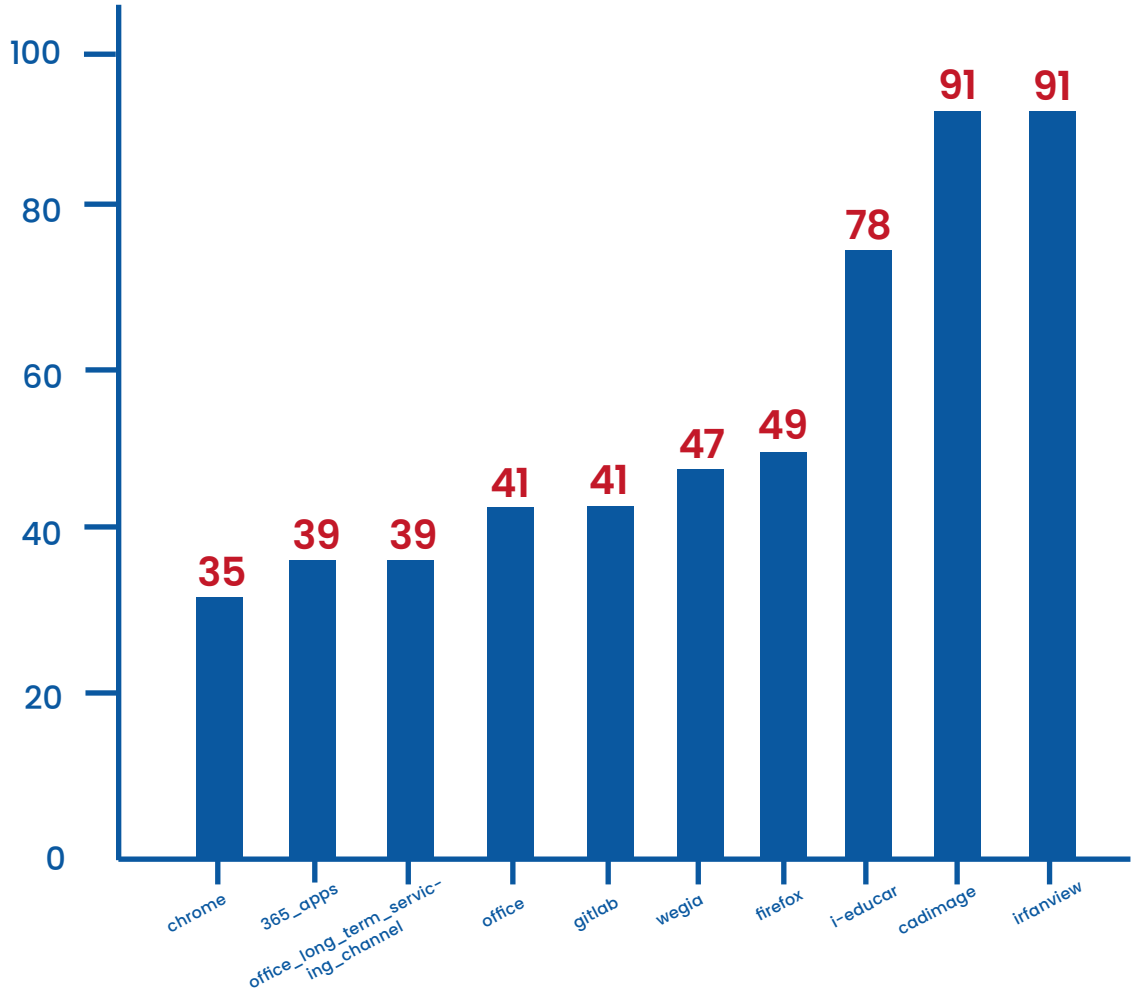


Figure 9: Shows the top affected Apps

As Unified Security Intelligence (USI) expands visibility across enterprise applications, it uncovers recurring vulnerability concentrations in both productivity and niche platforms. This chart shows IrfanView and Cadimage leading with the highest vulnerability counts (91 each), followed by i-Educar with 78, signaling exposure in less frequently patched or third-party integrated tools.

Mainstream applications like Firefox, GitLab, and Office 365 also feature consistently, emphasizing that even widely managed platforms demand continuous patch vigilance. USI's correlation of app-level trends enables prioritized remediation, ensuring both core and peripheral software stay aligned with organizational security posture.

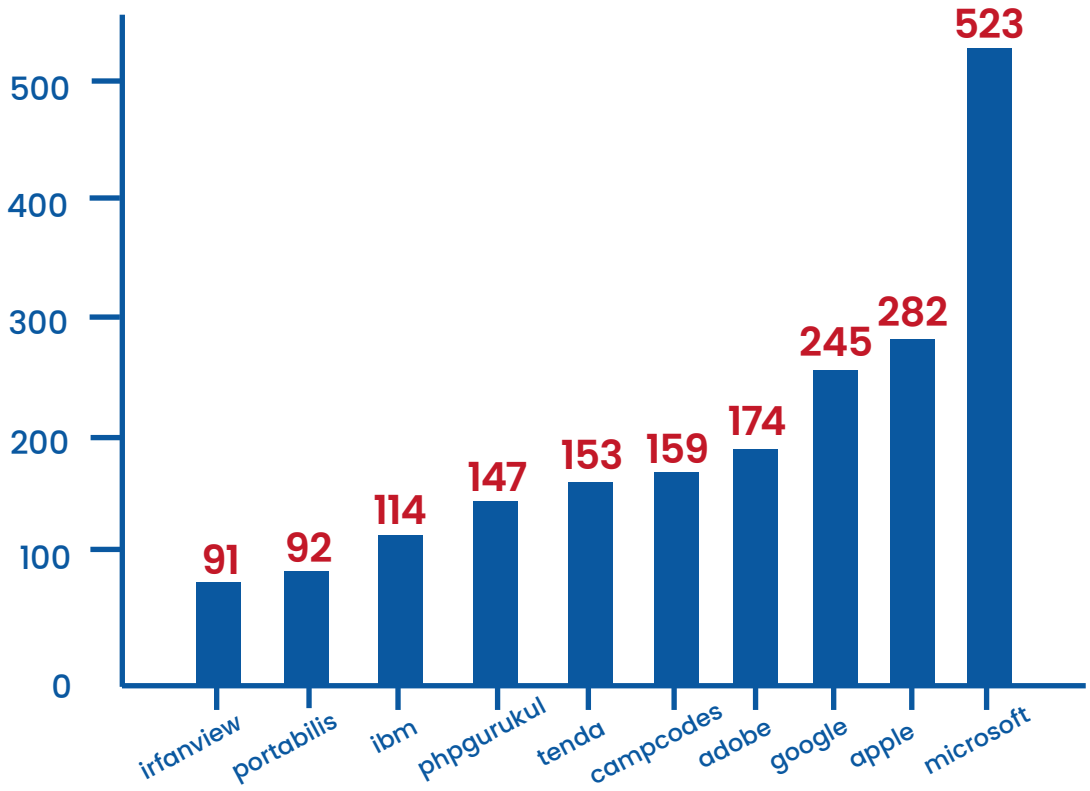


Figure 10: Shows the top affected vendors

The chart illustrates the software and hardware vendors with the highest number of reported vulnerabilities, highlighting exposure concentration among major technology providers.

- Microsoft leads with 523 vulnerabilities, reflecting the scale and complexity of its product ecosystem, spanning Windows, Office, and Azure services.
- Apple (282) and Google (245) follow, showing continued exposure across operating systems, browsers, and mobile platforms.
- Adobe (174) remains a recurring target, largely due to vulnerabilities in creative and document management applications.
- Campcodes (159), Tenda (153), and PHPGurukul (147) represent mid-tier vendors with significant exposures—primarily in web frameworks and IoT firmware.
- IBM (114), Portabilis (92), and IrfanView (91) record moderate vulnerability counts, emphasizing that even enterprise-grade and niche software solutions are not immune.

Large ecosystems like Microsoft, Apple, and Google continue to attract exploit development due to their ubiquity, while smaller vendors face challenges in maintaining secure code and timely patch releases. Continuous vulnerability tracking and unified exposure management are essential to mitigate risk across these diverse ecosystems.

RISK INSIGHT

The highest vulnerability concentration in Microsoft, Apple, and Google highlights attackers' focus on widely deployed ecosystems. Organizations relying on these vendors face amplified exploitation risks and must prioritize timely patching and exposure control.

Top 10 affected Operating Systems

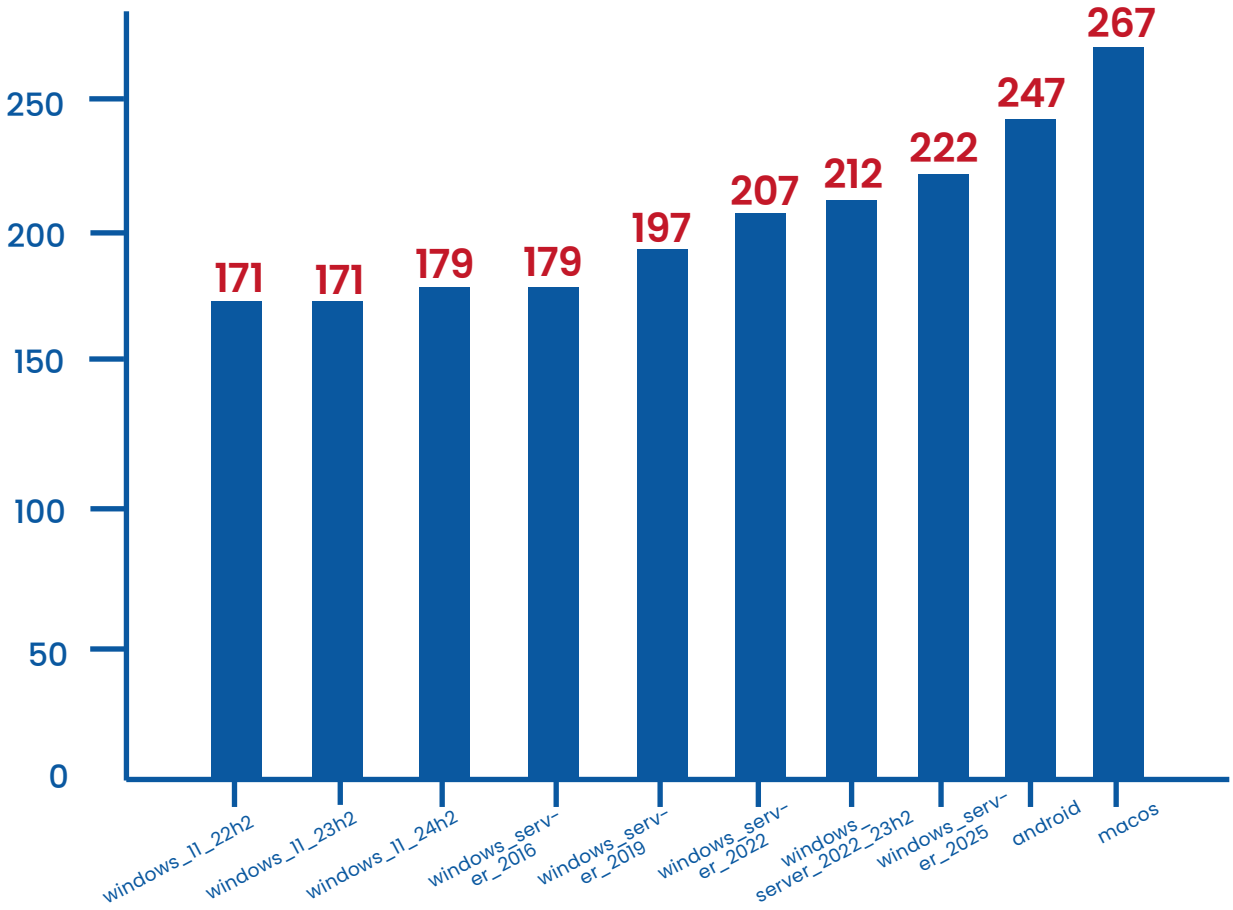


Figure 11: Shows the top affected operating systems

The chart shows macOS (267 vulnerabilities) and Android (247 vulnerabilities) as the most affected operating systems, followed closely by Windows Server 2025 (222) and other recent Windows builds. This indicates that attackers are increasingly exploiting both modern desktop and mobile platforms, underscoring the need for cross-platform vulnerability management and timely patch deployment across heterogeneous IT environments.

RISK INSIGHT

With macOS and Android emerging as the most affected operating systems, organizations face an expanded attack surface beyond traditional Windows environments. This shift underscores the need for consistent, cross-platform vulnerability monitoring and remediation to prevent exploitation across diverse IT ecosystems.

Top 10 Critical Vulnerability List

Sl. No.	CVE-ID	CVSS Score	Product	Description	Impact
1	CVE-2025-6617	8.8 (High)	D-Link DIR-619L (Firmware 2.06B01)	Stack-based Buffer Overflow	Full System Compromise
2	CVE-2025-2938	8.8 (High)	GitLab CE/EE (versions 17.3 to 18.1.1)	Elevation of Privilege	Privilege Escalation
3	CVE-2025-5459	8.6 (High)	Puppet Enterprise (2018.1.8 through 2023.8.3 and 2025.3)	Root Command Execution	Complete Primary Host Control
4	CVE-2025-27152	7.7 (High)	Axios (versions up to 1.7.9)	Server-Side Request Forgery (SSRF) and Credential Leakage	Information Disclosure/SSRF
5	CVE-2024-35164	7.5 (High)	Apache Guacamole (versions 1.5.5 and older)	Improper validation of console codes	Arbitrary Code Execution
6	CVE-2025-45729	6.3 (Medium)	D-Link DIR-823-Pro (Firmware 1.02)	Improper Permission Control	Partial System Compromise
7	CVE-2025-7259	6.5 (Medium)	MongoDB Server (v8.1.0)	Denial of Service (DoS)	Service Downtime (High Availability Impact)
8	CVE-2025-5450	6.3 (Medium)	Ivanti Connect Secure / Policy Secure (22.7R2.7 and older)	Improper Access Control	Integrity Loss and Privilege Escalation
9	CVE-2025-53021	4.2 (Medium)	Moodle (3.x through 3.11.18, unsupported)	Session Fixation via the sesskey parameter in the OAuth2 login flow	Account Takeover
10	CVE-2023-47310	N/A (Older/Unscored)	Apache Software Foundation (Product not specified in snippet)	Could not find sufficient details to score and classify this vulnerability within the search results.	Full System Compromise

RISK INSIGHT

Internet-facing infrastructure and endpoint/application RCEs/privilege-escalation flaws can be chained quickly from initial access to full system compromise. From a USI view, prioritize by exposure, exploitability, business-impact to immediately isolate exposed endpoints/apps with RCE/privilege bugs and run focused efforts for anomalous app behavior and lateral movement.

Zero Day Vulnerability List

Sl. No.	CVE-ID	CVSS Score	Severity	Product	Description
1	CVE-2025-4428	7.2	High	Ivanti Endpoint Manager Mobile (EPMM)	Code Injection The vulnerability allows a remote user to execute arbitrary code on the target system.
2	CVE-2025-20352	7.7	High	Cisco IOS and IOS XE SNMP implementation	Stack-based buffer overflow The vulnerability allows a remote user to compromise the affected system.
3	CVE-2025-6543	9.8	Critical	NetScaler Gateway and NetScaler ADC	Buffer overflow The vulnerability allows a remote attacker to perform a denial of service (DoS) attack.
4	CVE-2023-47565	8	High	QNAP QVR Firmware	OS Command Injection The vulnerability allows a remote attacker to execute arbitrary shell commands on the target system.
5	CVE-2025-7775	9.8	Critical	Citrix NetScaler ADC and NetScaler Gateway	Buffer overflow The vulnerability allows a remote attacker to execute arbitrary code on the target system.
6	CVE-2025-20362	6.5	Medium	Cisco ASA and FTD	Missing authorization The vulnerability allows a remote attacker to bypass authorization checks.
7	CVE-2024-8963	9.4	Critical	Ivanti Cloud Service Appliance	Path traversal The vulnerability allows a remote attacker to perform directory traversal attacks.
8	CVE-2024-39717	7.2	High	Versa Networks Director	Arbitrary file upload The vulnerability allows a remote user to compromise vulnerable system.
9	CVE-2017-7269	9.8	Critical	Microsoft IIS 6.0	Buffer overflow The vulnerability allows a remote attacker to execute arbitrary code on the target system.
10	CVE-2025-4428	8.6	High	Cisco IOS XR Software	Code Injection The vulnerability allows a remote user to execute arbitrary code on the target system.

RISK INSIGHT

Unified Security Intelligence reveals a surge in high-severity zero-day flaws across Cisco, Ivanti, and NetScaler products, exposing broad attack surfaces. Critical buffer overflow and code injection vulnerabilities pose imminent risks of remote exploitation. Continuous vulnerability and exposure management is essential to prevent cascading attacks across systems.

Top 10 Misconfigurations

CCE-ID	Description	CCSS
CCE-80903-8	This policy setting controls whether Microsoft Defender Antivirus network protection will display a warning, or block network traffic. The recommended state for this setting is: `Enabled`.	9.8
CCE-80902-0	This policy setting sets the Attack Surface Reduction rules.\n\nAttack surface reduction helps prevent actions and apps that are typically used by exploit-\nseeking malware to infect machines	9.8
CCE-71567-2	A default deny all policy on connections ensures that any unconfigured network usage will be rejected	9.8
CCE-71586-2	The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files.	8.6
CCE-71578-9	The 'pam_faillock.so' module maintains a list of failed authentication attempts per user during a specified interval and locks the account in case there were more than the configured number of consecutive failed authentications	8.4
CCE-76111-4	There are a number of methods to access the root account directly. Without a password set any user would be able to gain access and thus control over the entire system	8.1
CCE-80916-0	This policy setting manages whether or not Microsoft Defender Antivirus scans excluded files and directories when running a Quick Scan.	7.8
CCE-80905-3	This policy setting controls whether Microsoft Defender Antivirus Endpoint Detection and Response (EDR) is enabled in block mode (passive remediation)	7.8
CCE-71584-7	The 'rsync' service can be used to synchronize files between systems over network links.	7.3
CCE-76108-0	When a system-wide policy is set up, the default behavior of applications will be to follow the policy. Applications will be unable to use algorithms and\nprotocols that do not meet the policy, unless you explicitly request the application to do so.	7.3

RISK INSIGHT

Unified Security Intelligence highlights that recurring Defender and authentication misconfigurations expose endpoints to privilege escalation and undetected lateral movement. Correlating these weaknesses across assets enables prioritized remediation, ensuring endpoint defense and access controls remain continuously enforced.

Top 10 Malware Vulnerability Enumeration

MVE ID	Threat Name	Type
MVE-000859	Qilin Ransomware Group	Threat Group
MVE-001002	UNC6148 Group	Threat Group
MVE-000878	Overstep Malware	backdoor
MVE-001013	Linuxsys Cryptominer	Malware
MVE-000627	UNC3886	Threat Group
MVE-000876	Storm 2603	Threat Group
MVE-001007	Warlock Ransomware	Ransomware
MVE-000879	Fire Ant Campaign	Campaign
MVE-000880	Auto Color Backdoor	Backdoor
MVE-001005	CL-STA-0969 Group	Threat Group

RISK INSIGHT

Malware Vulnerability Enumerations reveal a growing overlap between ransomware, backdoor, and threat group activities, indicating a surge in multi-vector, persistent attacks. Enterprises must strengthen vulnerability management with unified security intelligence and continuous vulnerability and exposure management to neutralize these evolving campaigns.

Top 10 Posture Anomalies

Anomaly Name	Anomaly ID	Category	Description
Vulnerable process making outbound network connection	PA-2022-1001	Risk	Identifies vulnerable processes making external network connections—flagged as anomalous port-specific behavior.
Unusual tasks are scheduled in Task Scheduler	PA-2022-1011	System	Detects unusual scheduled tasks in Windows Task Scheduler, indicating possible malicious or unauthorized automation.
Firewall disabled	PA-2022-1033	System Security	Detects systems where the firewall is disabled, exposing devices to unfiltered network traffic.
UAC policy not configured properly	PA-2022-1034	System Security	Flags systems where User Account Control (UAC) is misconfigured, reducing resistance to unauthorized privilege escalation.
ASLR is disabled	PA-2022-1036	System Security	Identifies devices where Address Space Layout Randomization (ASLR) is turned off, increasing the risk of memory-based attacks.
Anomaly found in users with elevated privilege	PA-2022-1021	System Security	Detects unexpected or anomalous elevated/sudo user privileges that can lead to unauthorized access or data compromise.
Irregular Host IP to MAC address maps	PA-2022-1003	Network	Flags anomalies in ARP tables where Host IP-to-MAC mappings are inconsistent—may indicate spoofing or misconfigurations.
Increasing Critical Vulnerability Count	PA-2022-1017	Risk	Monitors and alerts on devices showing a rising trend in critical vulnerabilities, using anomaly detection techniques.
Unique software applications on few systems	PA-2022-1002	Software Assets	Identifies rare software installed only on a few systems within a cluster, indicating potential shadow IT or risk.
Anomalous events in Windows Event log	PA-2022-1004	Events	Detects blacklisted or suspicious events (e.g., failed logins, multiple login attempts, account updates) using event log analysis.

RISK INSIGHT

These posture anomalies reveal deep-rooted weaknesses across system configurations, user privileges, software assets, and network behavior which can get exploited.
USI enables continuous visibility and contextual correlation of such anomalies, transforming isolated signals into actionable risk intelligence. By normalizing and prioritizing these anomalies, USI shifts organizations to more proactive risk remediation.
Know more about posture anomaly management.

Q3 Report

Cloud Coverage

For AWS and Azure Cloud Security

The data for Q3 continues to demonstrate how comprehensive unified security intelligence consolidates multiple compliance frameworks and security controls into a unified monitoring system, empowering security teams to identify, assess, and remediate risks across multi-cloud environments. The expanding dataset reflects significant growth in coverage across CSPM rules, CSPA assessments, and CIEM capabilities for AWS and Azure platforms.

AWS CLOUD SECURITY COVERAGE

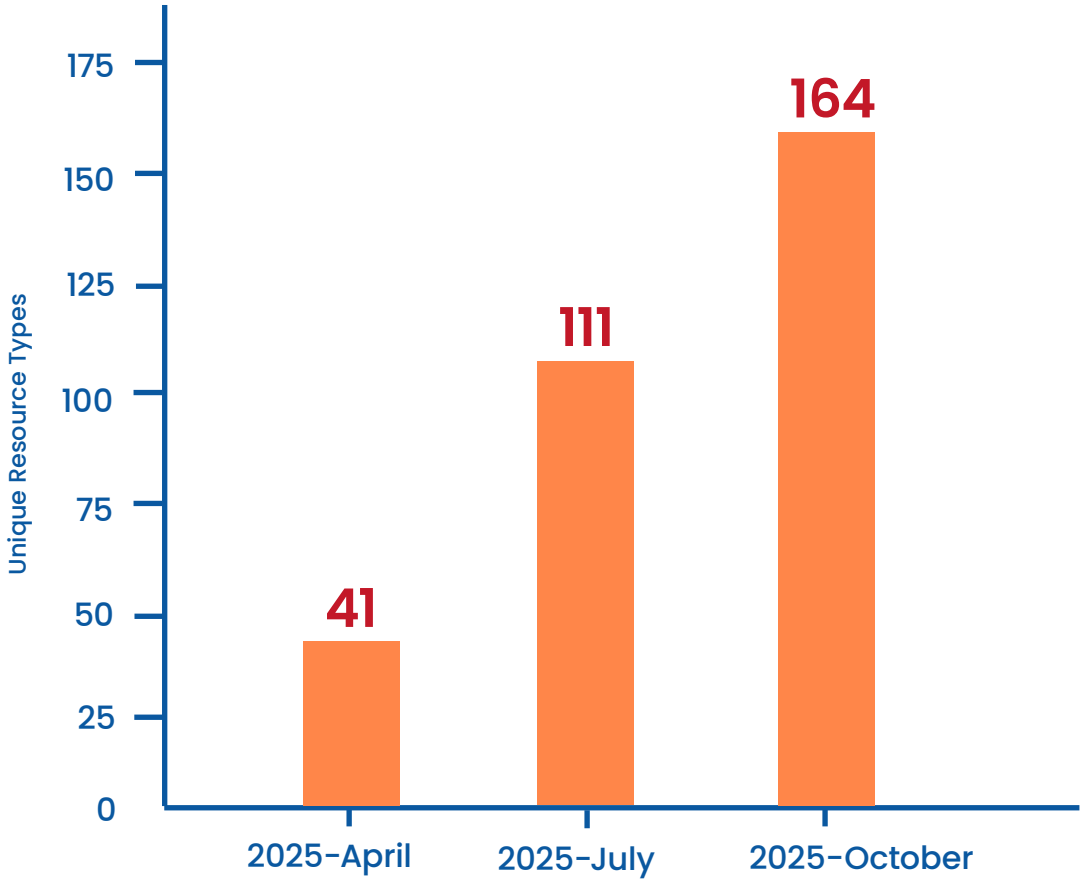


Figure 12: Shows the AWS combined resource types (CSPM Rules + CSPA + CIEM)

Combined Resource Types Covered: 164

Unified Security Intelligence (USI) now monitors 164 unique AWS resource types across CSPM Rules, CSPA, and CIEM frameworks, a 300% expansion from April's baseline of 41 resources. From July to October, coverage increased by 48%, adding 53 new resource types. This sustained growth trajectory demonstrates the USI's agility in adapting to AWS's expanding service catalog while maintaining comprehensive security visibility across compute, storage, networking, and identity infrastructure.

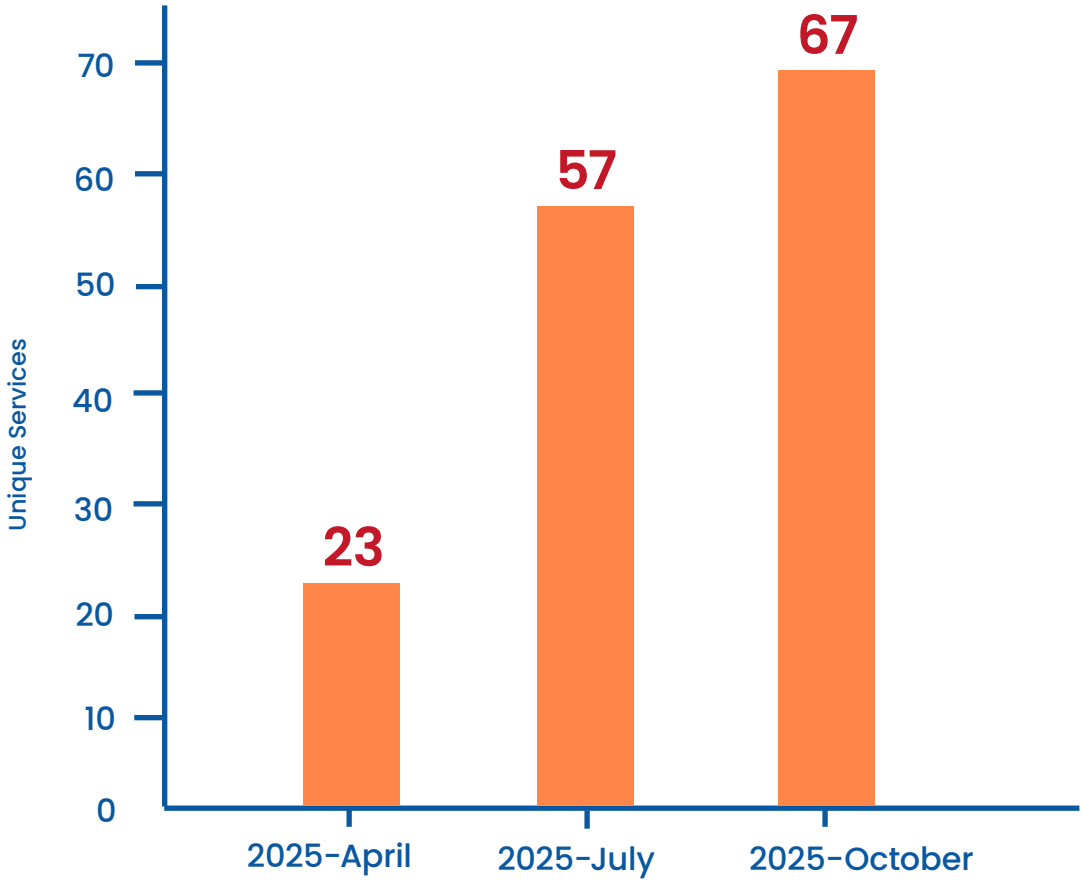


Figure 13: Shows the AWS combined services (CSPM Rules + CSPA + CIEM)

Combined Services Monitored: 67

Q3 coverage now encompasses 67 distinct AWS services, representing a 191% increase from April's 23 services. USI added 10 additional services between July and October, building on the 34 services added in the previous quarter. This expansive breadth ensures security teams maintain unified oversight across the entire AWS ecosystem, from foundational services like EC2 and S3 to specialized offerings including SageMaker, IoT Core, and emerging AWS capabilities.

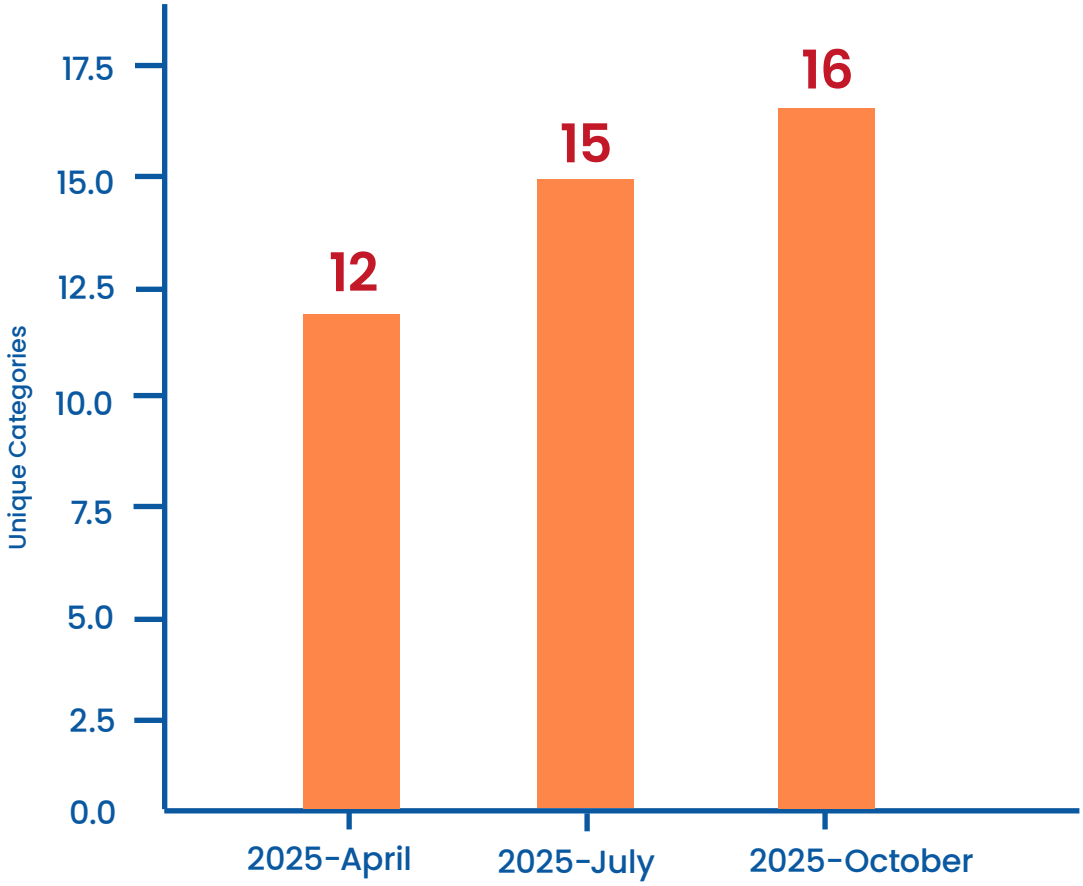


Figure 14: Shows the AWS combined categories (CSPM Rules + CSPA + CIEM)

Combined Categories Covered: 16

Unified Security intelligence coverage now spans 16 unique security categories, up 33% from April's 12 categories and reflecting a 7% increase from July's 15 categories. This categorical expansion ensures comprehensive protection across all AWS security domains, from identity and access management to data protection, compliance, and threat detection.

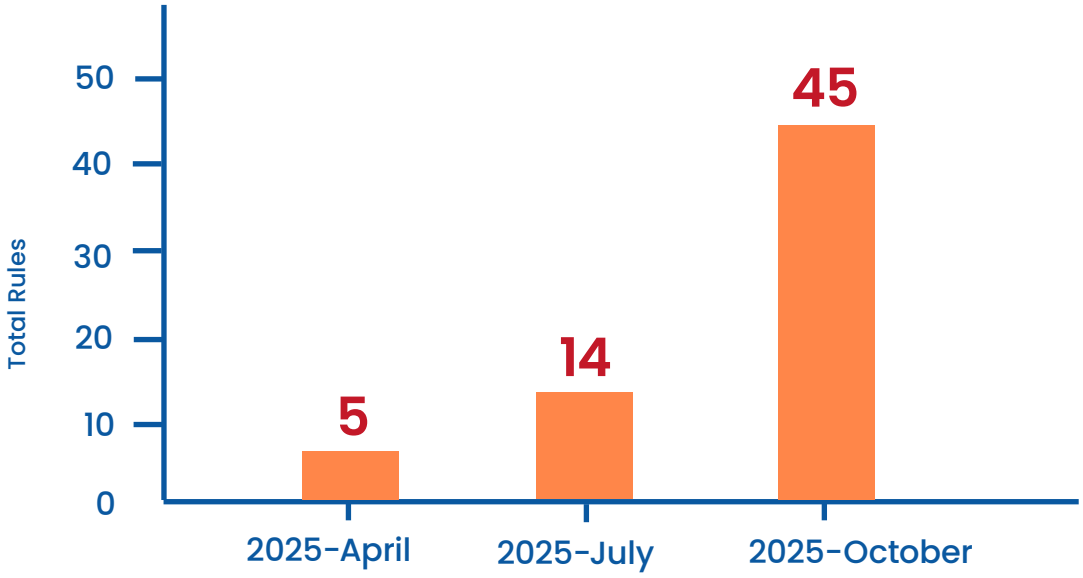


Figure 15: Shows the AWS CSPA Rule-based

AWS CSPA Total Rules: 110

The number of AWS-specific compliance and security configuration rules grew from 5 in April to 14 in July, and further to 45 by October, marking an overall 221% increase within six months. This accelerated growth reflects the platform's enhanced commitment to keeping pace with evolving AWS security best practices and emerging compliance requirements.

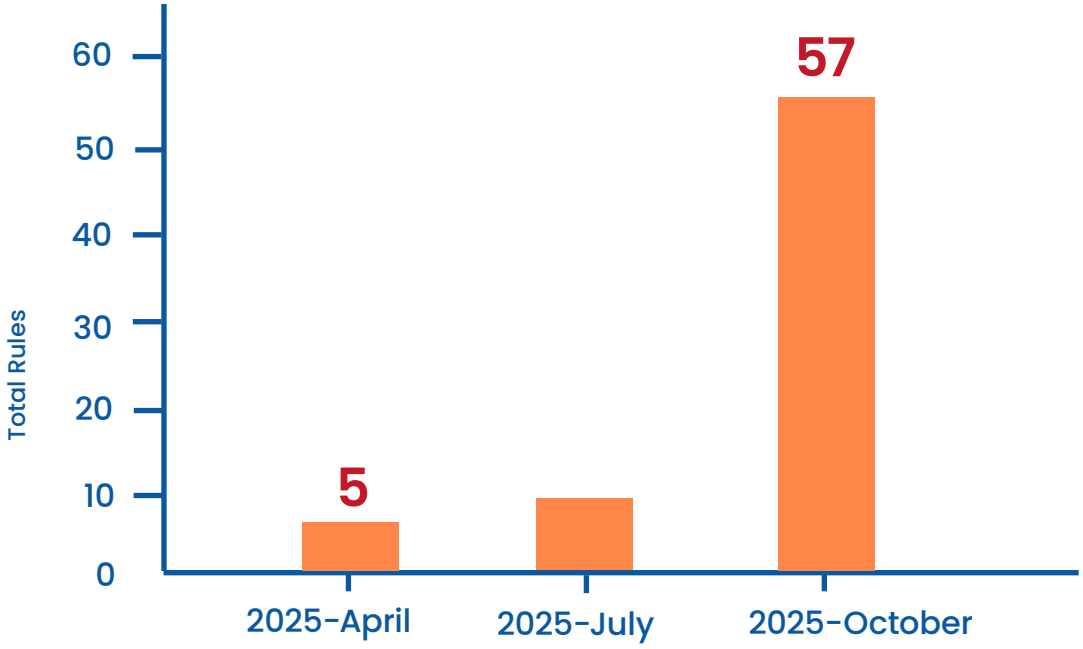


Figure 16: Shows the AWS CSPA Outlier-based

AWS CSPA Outlier-Based Detection: 57

Outlier-based detection capabilities have reached 57 rules, representing a 533% expansion from April's 5 rules. The third quarter saw particularly strong growth, with 48 new outlier rules added, a 533% increase from July alone. These advanced behavioral analytics identify anomalous configurations and deviations from established security baselines, enabling proactive threat detection.

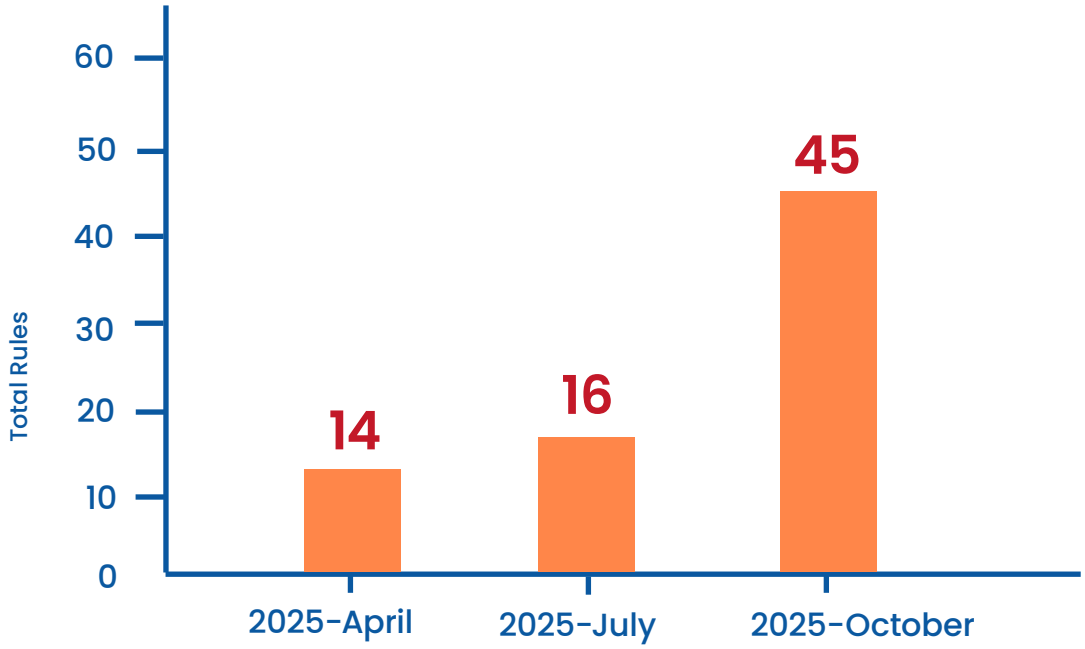


Figure 17: Shows the AWS CSPA rule-based

AWS CSPA Rule-Based Controls: 45

Rule-based assessments now cover 45 controls, demonstrating a 221% increase from April's 14 rules and a 180% surge from July's 16 rules. These validation checks ensure configurations comply with established security standards, providing consistent policy enforcement and governance across all AWS environments.

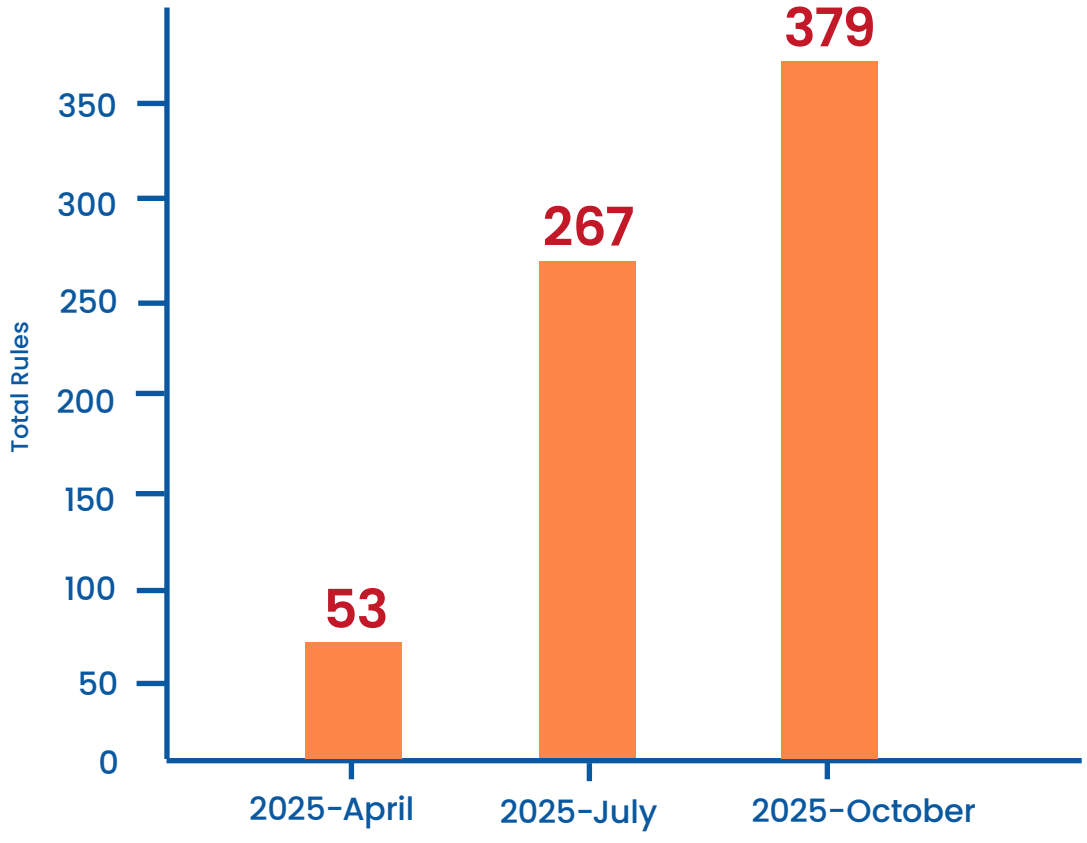


Figure 18: Shows the AWS CSPM Rules

AWS CSPM Rules: 379

The Cloud Security Posture Management framework has expanded to 379 rules, a 615% increase from April's initial 53 rules and a 42% growth from July's 267 rules. This quarter added 112 new rules, reinforcing deep coverage across critical AWS security domains, including IAM, network security, encryption at rest and in transit, audit logging, and data protection controls.

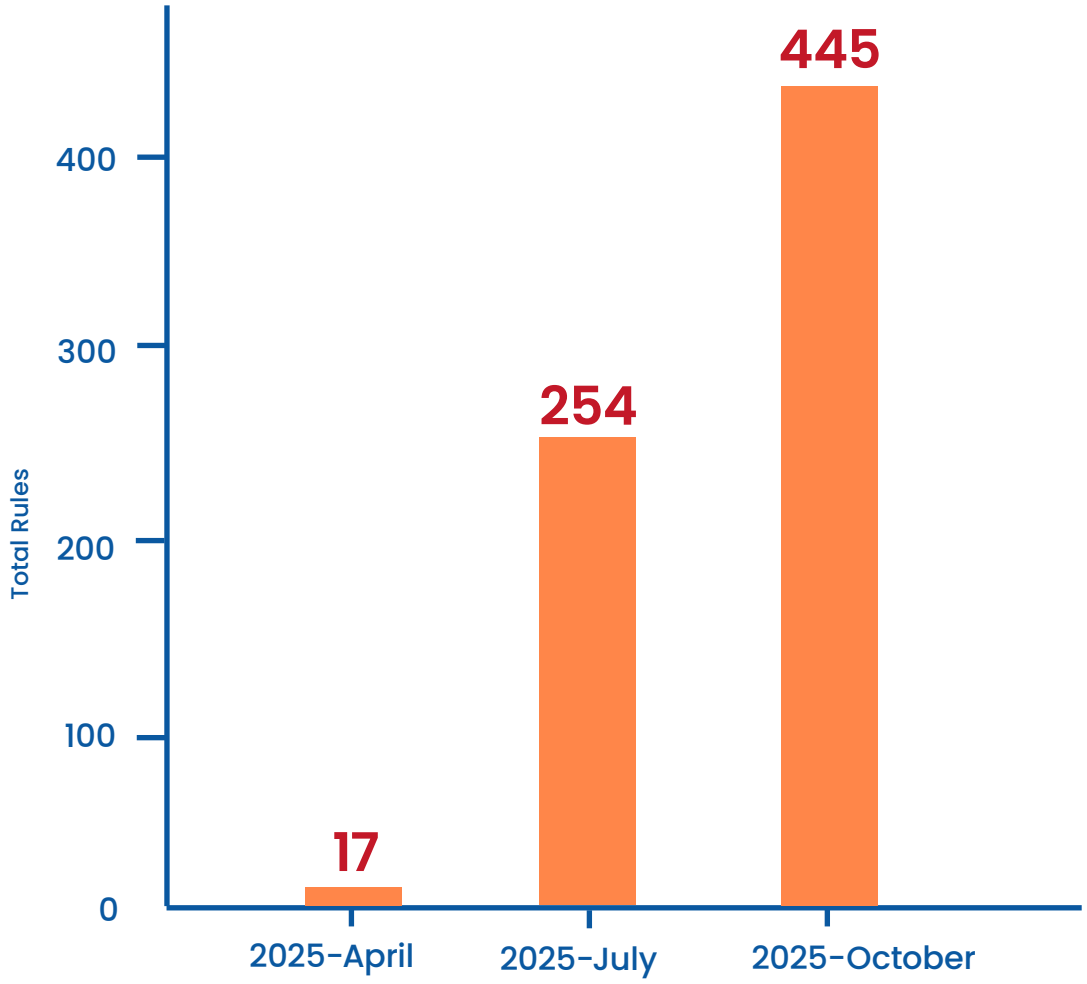


Figure 19: Shows the AWS CSRM Rules

AWS CSRM Rules: 445

Cloud Security and Risk Management rules now total 445, representing an extraordinary 2,518% expansion from April's baseline of 17 rules. Between July and October, CSRM coverage grew by 75%, adding 191 contextual risk rules. They prioritize and contextualize security findings based on exploitability, business impact, and threat landscape, helping teams focus remediation resources on the most critical exposures first.

AZURE CLOUD SECURITY COVERAGE

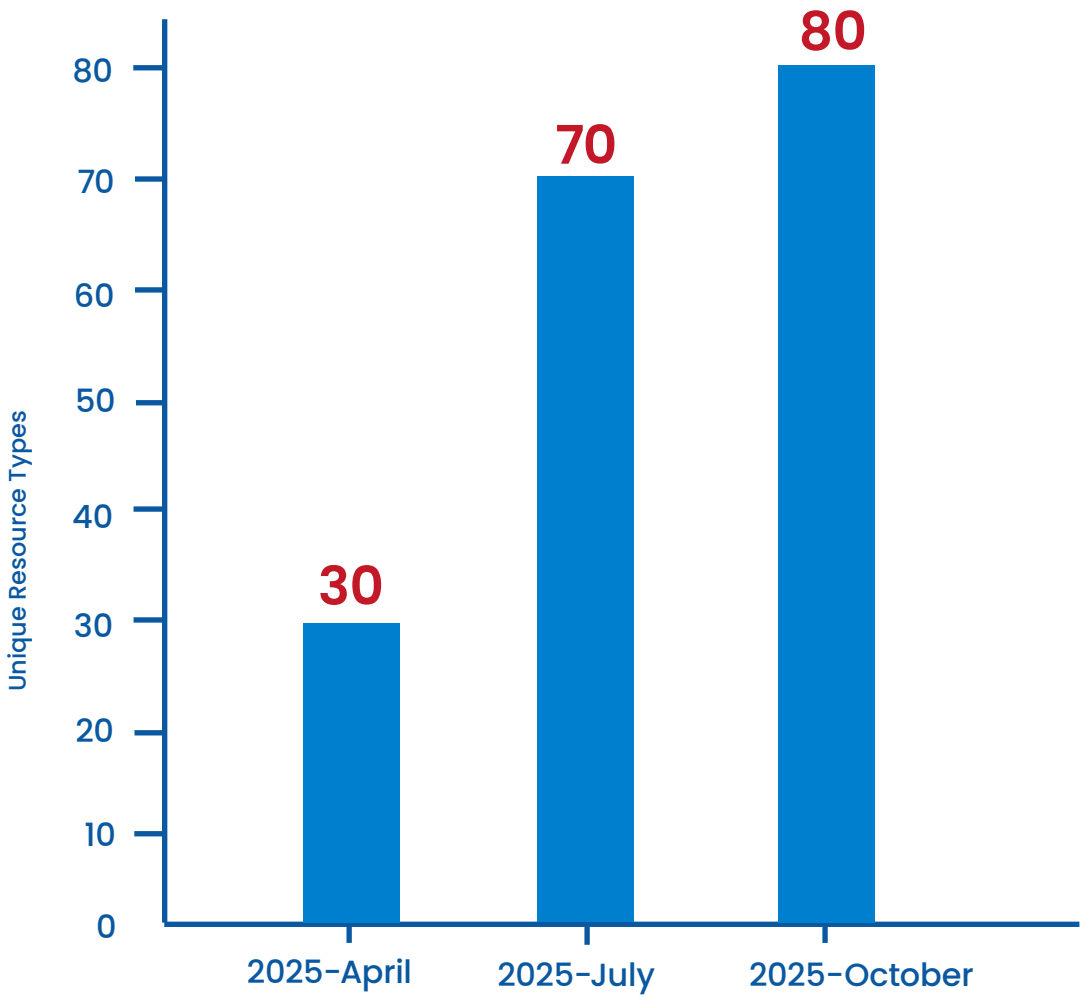


Figure 20: Shows the Azure combined resource types (CSPM Rules + CSPA + CIEM)

Combined Resource Types Covered: 80

The platform now monitors 80 unique Azure resource types across CSPM Rules, CSPA, and CIEM frameworks, a 167% expansion from April's baseline of 30 resources. Between July and October, coverage increased by 14%, adding 10 new resource types to the existing 70. This sustained growth trajectory demonstrates the platform's responsiveness to Azure's expanding service ecosystem while maintaining comprehensive security visibility across computing, storage, networking, identity, and data services.

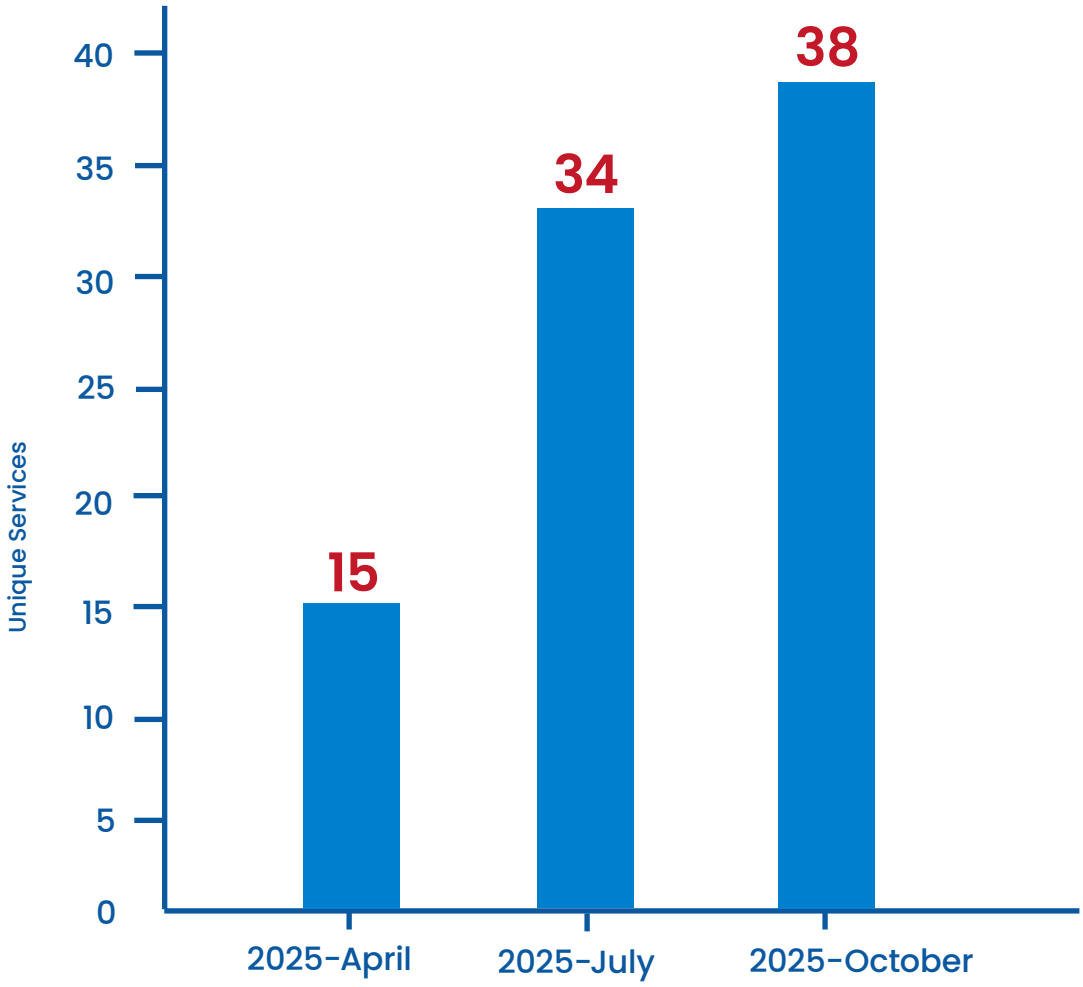


Figure 21: Shows the Azure combined services (CSPM Rules + CSPA + CIEM)

Combined Services Monitored: 38

Q3 coverage now encompasses 38 distinct Azure services, representing a 153% increase from April's 15 services. The platform added 4 additional services between July and October, building on the substantial 19 services added in the previous quarter. This expanding breadth ensures security teams maintain unified oversight across Microsoft's cloud ecosystem, from foundational services like Virtual Machines and Storage Accounts to specialized offerings including Azure Synapse Analytics, Azure Kubernetes Service, and emerging AI/ML services.

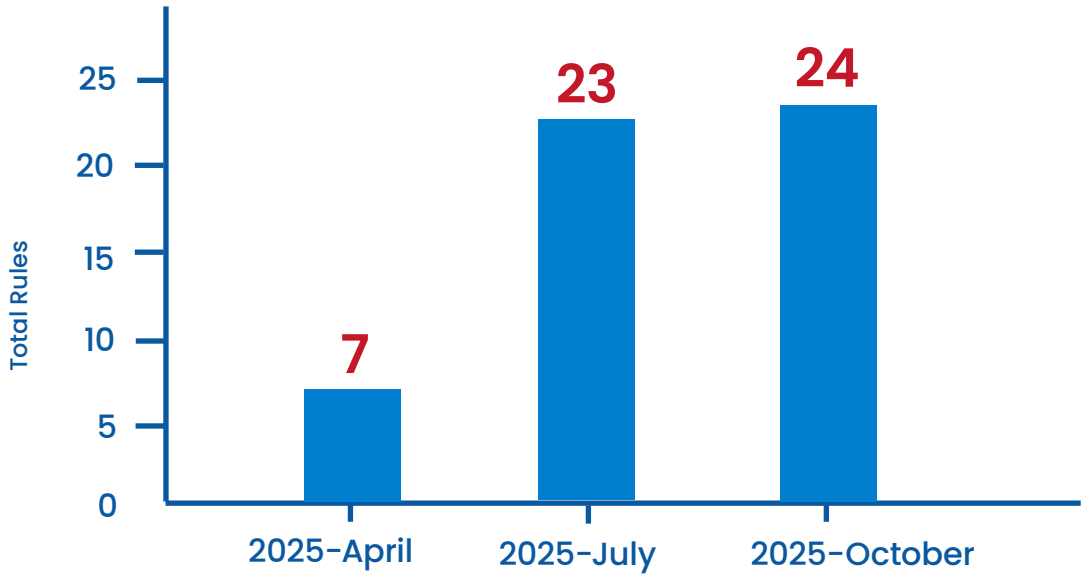


Figure 22: Shows the Azure CSPA

Azure CSPA Total Rules: 24

The Cloud Security Posture Assessment framework has grown to 24 total rules, a 243% increase from April's baseline of 7 rules. Between July and October, the framework expanded by 4%, adding 1 new rule to the 23 rules established in July. This growth reflects the platform's commitment to aligning with Microsoft's evolving security best practices and Azure-specific compliance requirements.

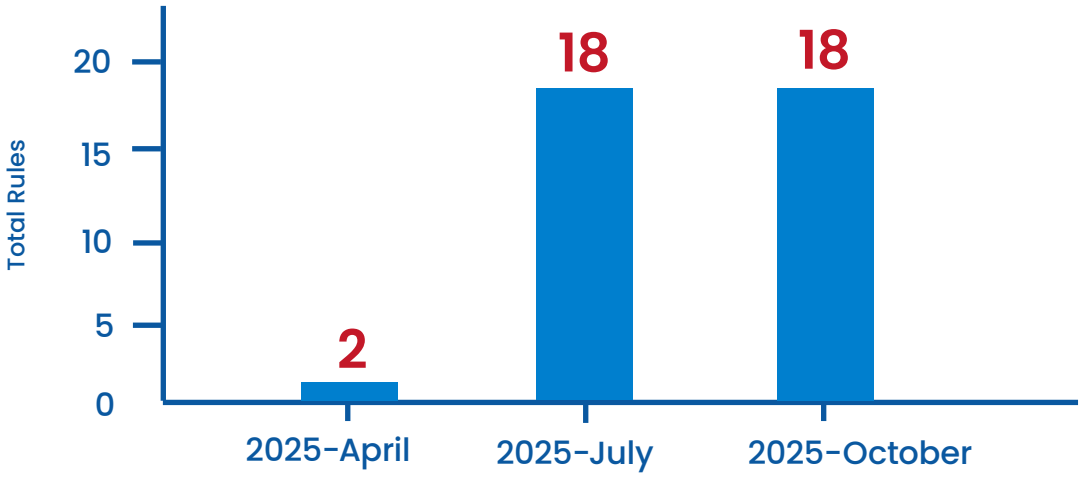


Figure 23: Shows the Azure CSPA Rule-based

Azure CSPA Rule-Based Controls: 18

Traditional rule-based assessments now cover 18 controls, demonstrating a 700% expansion from April's 2 rules. The framework maintained stable coverage from July (18 rules) through October, having achieved comprehensive baseline coverage of Azure's core security configurations. These validation checks ensure configurations comply with Microsoft Cloud Security Benchmark and industry standards, providing consistent policy enforcement and governance across all Azure environments.

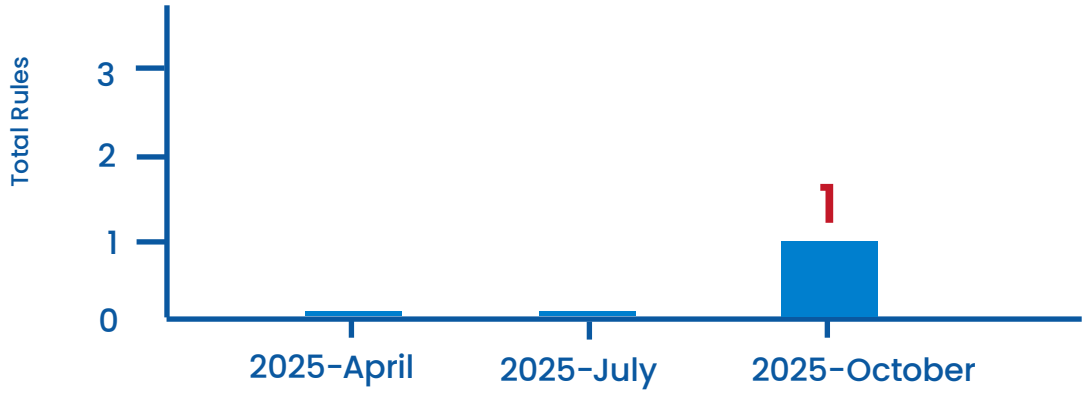


Figure 24: Shows the Azure CSPA outlier-based

Azure CSPA Outlier-Based Detection: 1

Outlier-based detection capabilities were introduced in Q3 with the deployment of 1 behavioral analytics rule in October. This represents a new capability for Azure environments, enabling the identification of anomalous configurations and deviations from established security baselines. This foundation positions the platform for expanded behavioral analytics in future releases, supporting proactive threat detection before misconfigurations escalate into security incidents.

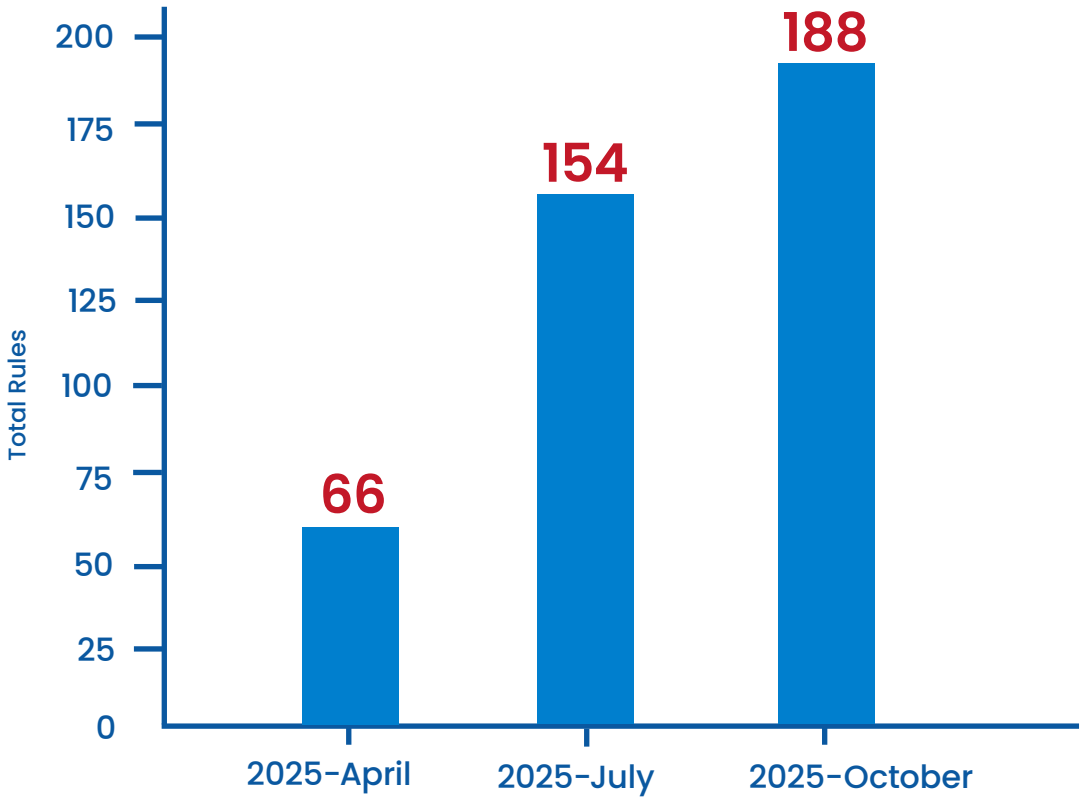


Figure 25: Shows the Azure CSPM Rules

Azure CSPM Rules: 188

The Cloud Security Posture Management framework has expanded to 188 rules, a 185% increase from April's initial 66 rules and a 22% growth from July's 154 rules. This quarter added 34 new rules, reinforcing comprehensive coverage across critical Azure security domains, including Azure Active Directory, network security groups, encryption at rest and in transit, activity logging, Key Vault management, and data protection controls.

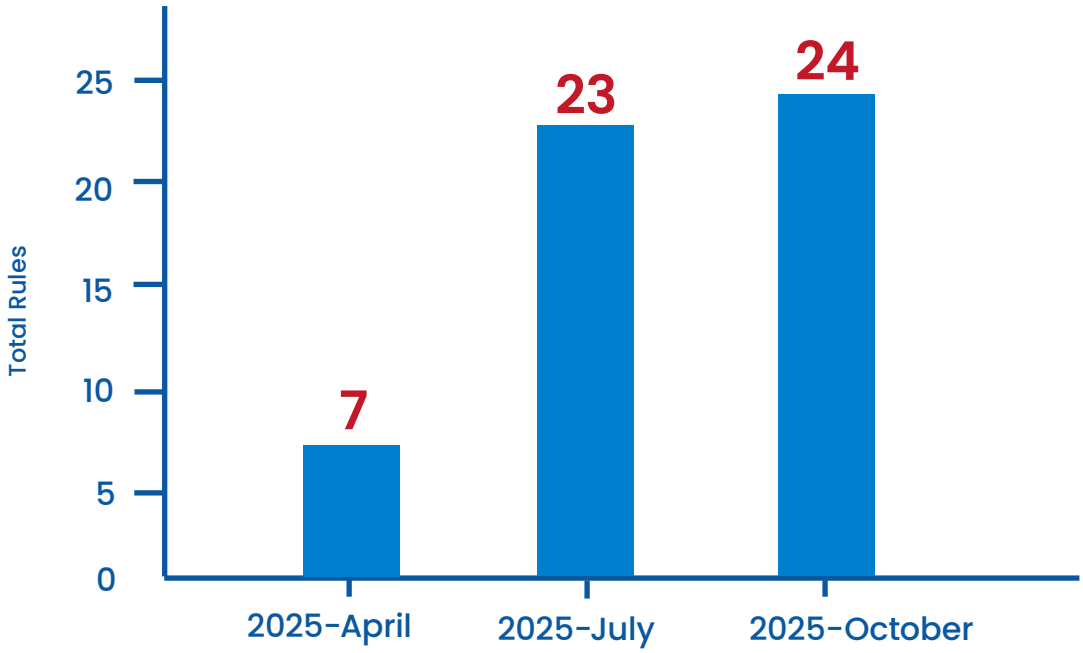


Figure 26: Shows the Azure CSPA

Azure CSPA Total Rules: 24

Cloud Security Posture Assessment coverage reached 24 rules, demonstrating a 243% expansion from April's baseline of 7 rules. While coverage remained stable from July (23 rules) through October, with the addition of 1 rule, this reflects maturity in Azure assessment capabilities. The platform has established comprehensive coverage of Azure's core security assessment requirements, with incremental enhancements focused on emerging Azure services and evolving threat patterns.

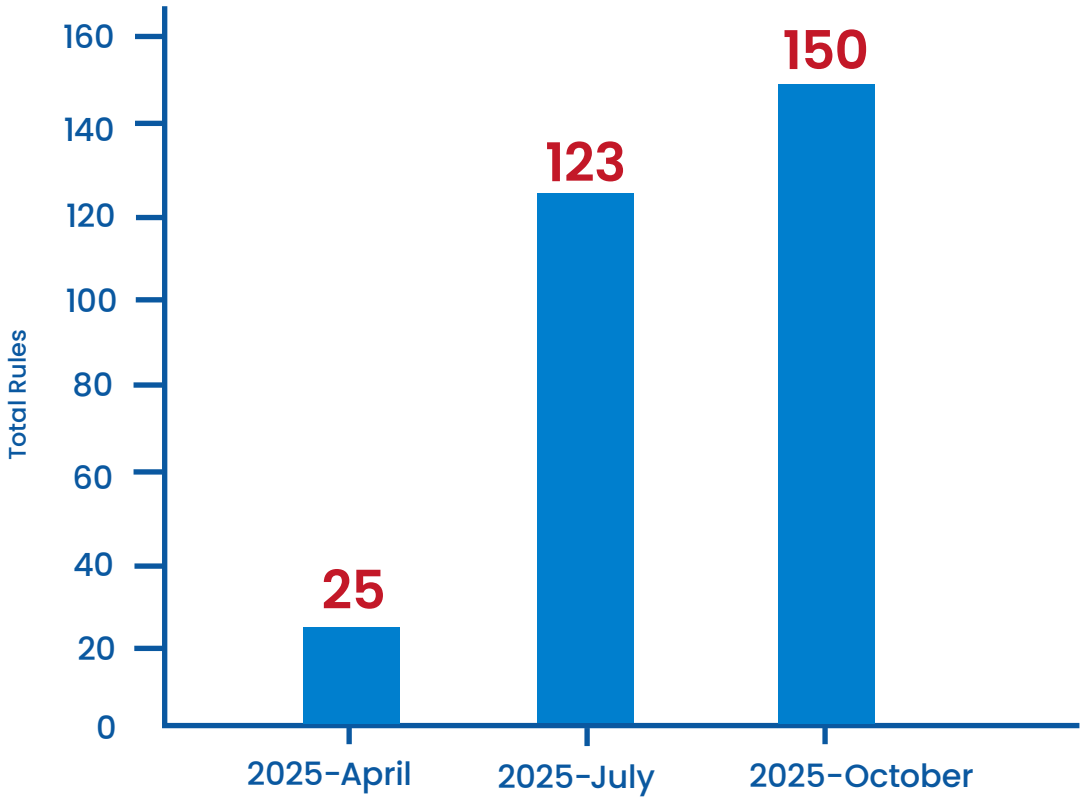


Figure 27: Shows the Azure CSRM Rules

Azure CSRM Rules: 150

Cloud Security and Risk Management rules now total 150, representing an extraordinary 500% expansion from April's baseline of 25 rules. Between July and October, CSRM coverage grew by 22%, adding 27 contextual risk rules to the existing 123. These intelligence-driven rules prioritize and contextualize security findings based on Azure-specific attack vectors, business impact, and threat landscape dynamics, helping teams focus remediation resources on the most critical exposures in their Microsoft cloud environments.

RISK INSIGHT

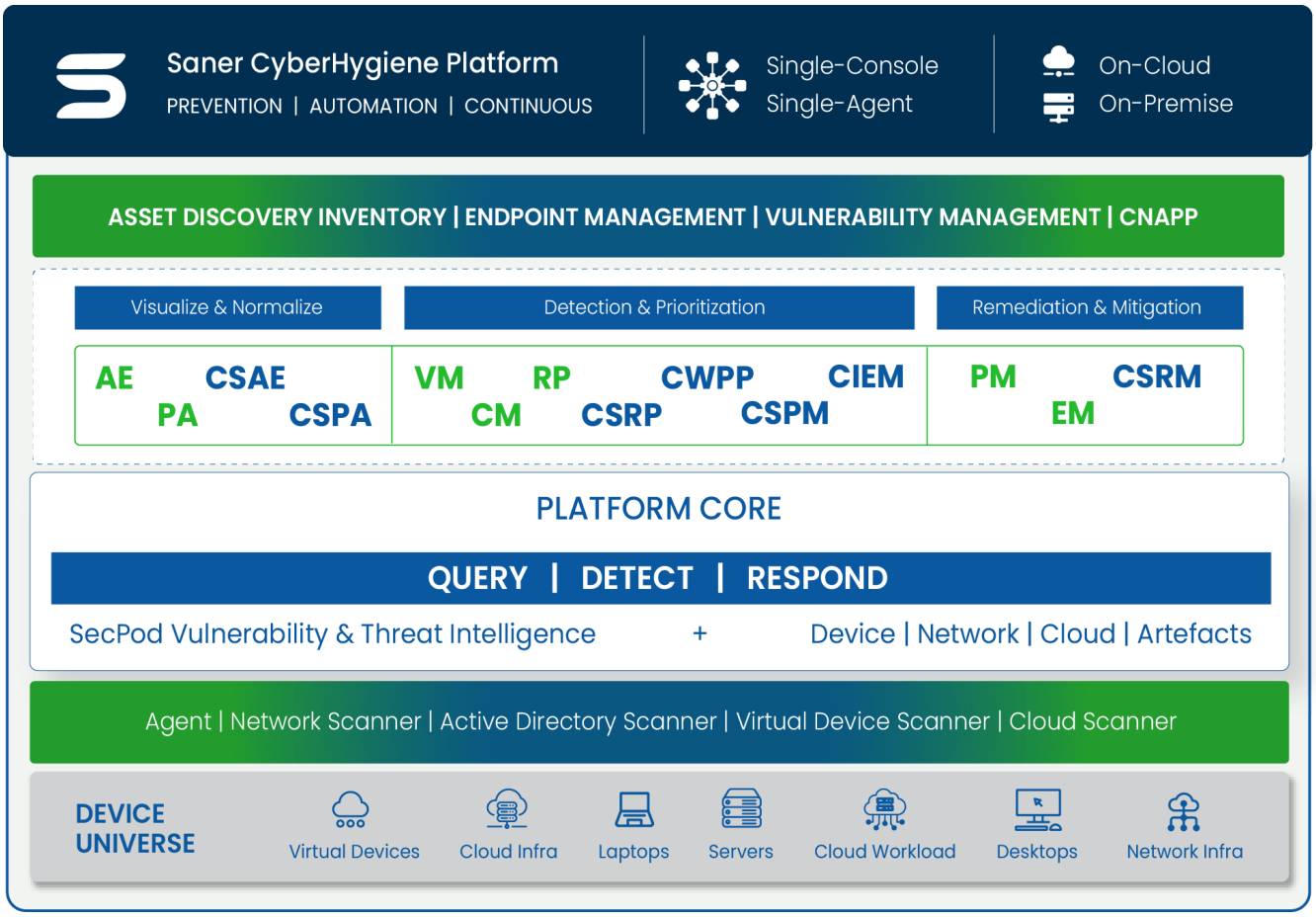
The rapid expansion of AWS and Azure coverage reveals growing risks from misconfigurations, excessive permissions, and inconsistent controls across multi-cloud environments. A 75% rise in AWS CSRM rules and 22% growth in Azure coverage highlight increasing exposure complexity. Unmonitored cloud assets and identity misalignments remain prime vectors for data leakage and privilege abuse. Unified Security Intelligence (USI) correlates these risks with exploit data for precise, real-time prioritization. Continuous cloud posture monitoring is critical to maintaining governance, compliance, and resilience at scale.

Scan, Normalize, Detect, Prioritize & Remediate Endpoint & Cloud Security Risks with Saner

Saner Platform is a suite of solutions that help organizations establish a strong security posture to proactively prevent attacks in endpoints and the cloud.

SANER CLOUD – An AI-fortified Cloud-Native Application Protection Platform (CNAPP) that delivers continuous visibility, security compliance, and risk mitigation for cloud environments.

SANER CVEM – A Continuous Vulnerability and Exposure Management (CVEM) solution that delivers continuous visibility, identifies, assesses, and remediates vulnerabilities across enterprise devices and network infrastructure.



SecPod is a leading cybersecurity technology company committed to preventing cyberattacks through proactive security. Its mission is to secure computing infrastructure by enabling preventive security posture.

At the core of SecPod's offerings is the Saner Platform - a suite of solutions that help organizations establish a strong security posture to preempt cyber threats against endpoints, servers, network and cloud infrastructure, as well as cloud workloads. With its cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

info@secpod.com

secpod