CHECK POINT™

2025

CLOUD SECURITY REPORT

CISO Priorities for Securing the Modern Cloud

Research by

Cybersecurity
INSIDERS

A Message from the Global CISO at Check Point

In today's interconnected world, network security is essential for every aspect of our digital lives. Organizations face a significant challenge in securing branch offices, data centers, cloud deployments, SaaS applications, mobile users, and email communications more effectively in the AI age.

At Check Point, we provide a unique hybrid mesh architecture with over 250 third-party integrations which boosts flexibility by allowing direct connections between cloud services and data centers, resulting in enhanced security, reduced latency, and improved performance. Below follows some guidance on how organizations can protect their cloud infrastructure, and reduce cloud expenses, which continue to soar year-after-year.

- **Consolidate Fragmented Tools into Unified Security Platforms:**
  Consider solutions with a unified console that simplifies feature discovery and dashboard navigation, supported by a cloud-based platform for agility, scalability, and uninterrupted operations

- **Gain Visibility Across Cloud Environments:**
  Focus on tools that enhances visibility via consolidated logging, monitoring, event management, and forensics, aiding compliance and bridging security gaps

- **Leverage AI Defensively to Counter AI-Driven Threats:**
  By integrating automation, AI, and ML, hybrid mesh enhances security teams' scalability, enabling faster and more effective responses to potential threats while optimizing resource utilization

CISOs today are no longer just defenders—they are strategic enablers of cloud innovation. To protect what's next, they must move beyond patchwork security toward unified, intelligent, and automated defenses. In the race between speed and safety, real-time readiness is the only path forward.

Deryck Mitchelson,
Global CISO at Check Point Software Technologies

Overview

Cloud architectures are evolving faster than most security teams can adapt. As hybrid, multi cloud, edge, and SaaS adoption accelerates, organizations are contending with fragmented environments, inconsistent controls, and expanding attack surfaces. Detection is delayed, tooling is overloaded, and many defenses remain outdated— all while adversaries automate, adapt, and scale their own capabilities. The result is a growing mismatch between how the cloud is being used and how it's being secured.

To better understand how security leaders are responding to these pressures, Cybersecurity Insiders set out to examine the real-world strategies, priorities, and constraints shaping cloud defense today. Through a comprehensive survey of over 900 CISOs, cybersecurity professionals, and IT decision-makers conducted in early 2025, this report captures the current state of cloud security from the CISO's perspective — including what's working, what's breaking down, and where organizations are investing next.

Key Findings Include:

- **Cloud adoption is accelerating across every architectural layer— especially hybrid, multi-cloud, and edge — but security strategies have not kept pace.** 62% of organizations expanded cloud-edge technologies (like SASE), 57% expanded hybrid cloud, and 51% adopted multi cloud, fragmenting environments and overwhelming traditional perimeter-based defenses.

- **Cloud-related breaches are rising fast, and many still go undetected for hours or even days.** 65% of organizations experienced a cloud-related incident in the past year; only 9% detected it within the first hour, and 62% took more than 24 hours to remediate it.

- **Detection tools fail to surface threats — users, audits, or third parties discover most incidents.** Only 35% of organizations detected incidents via security monitoring tools; most incidents are discovered by end users, third parties, or during audits, exposing critical gaps in real-time threat visibility.

- **Security operations are under strain from tool sprawl and alert overload.** 71% of organizations use over 10 cloud security tools, and 45% receive over 500 daily alerts, eroding response speed, analyst capacity, and risk prioritization.

- **AI is rising as a top security priority, but most teams still feel unprepared to defend against AI-powered threats.** 68% of organizations say AI adoption is a priority, yet only 25% are confident in their ability to defend against machine-driven attacks like automated evasion and malware.

- **Application-layer security remains dangerously outdated, leaving APIs and business-critical web assets exposed.** 61% still rely on signature-based WAF detection as their primary defense, despite the rise of evasive app-layer threats, and only partial adoption of behavioral and AI/ML-based techniques.

These findings reveal a cloud security landscape under pressure — and a clear mandate for change. The following pages unpack the key trends, challenges, and strategic responses shaping how security leaders are adapting to a faster, more fragmented, and more hostile cloud environment.

01

Cloud Complexity Outpaces Security

Cloud infrastructure is becoming more distributed, dynamic, and difficult to defend. As hybrid and multi-cloud adoption grows, traditional security models built for centralized environments are breaking down.
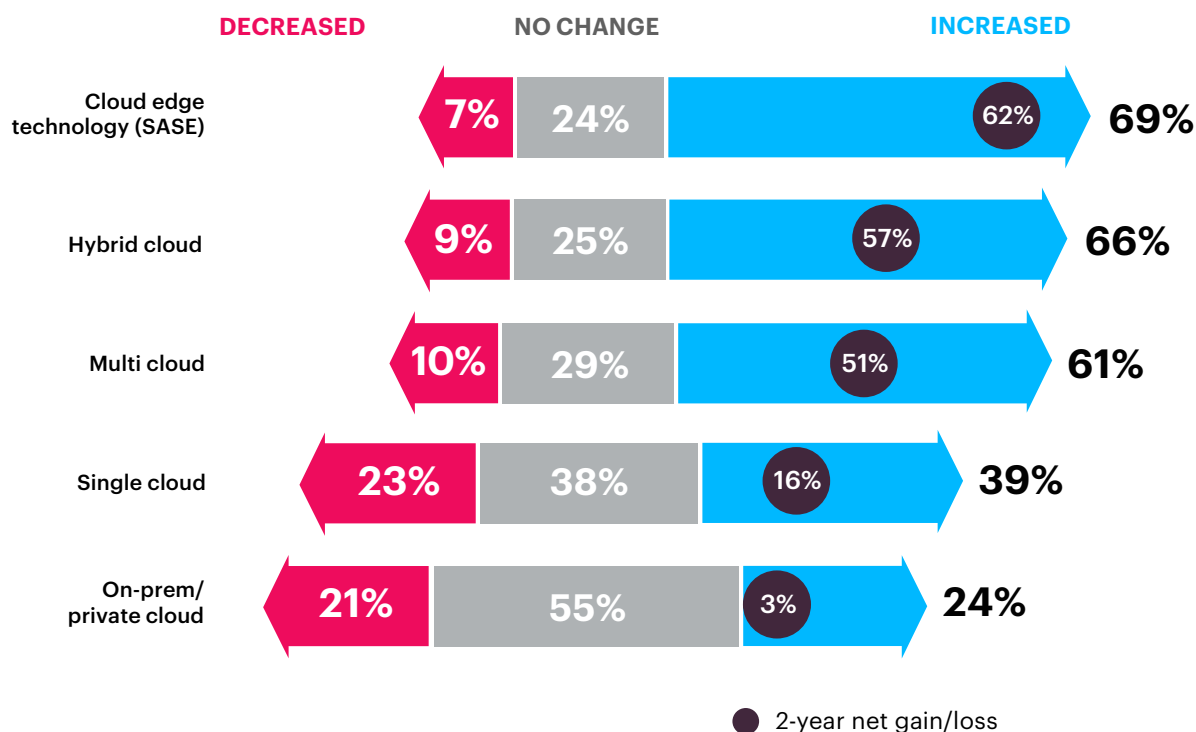
- Cloud edge technologies (62% growth), hybrid cloud (57%), and multi-cloud (51%) are expanding quickly in an effort to enhance business agility and scalability.

- Security teams must now protect data, identities, and workloads across decentralized environments with fragmented controls and shifting perimeters.

- The shift is driving top challenges like safeguarding high-value assets (43%), difficulties in visibility and detection (40%), and overall management of hybrid/multi-cloud security (38%).

Cloud Strategies Reshape Risk

As organizations increasingly rely on hybrid architectures, multi-cloud ecosystems, and cloud-edge technologies like SASE, the underlying infrastructure is becoming more fragmented, dynamic, and difficult to secure with traditional approaches.

Our data reveals a decisive architectural shift: While multi-cloud environments continue to be an integral part of the process, we see that 62% of organizations report an increased adoption of cloud-edge technologies, and 57% have expanded hybrid cloud deployments. A hybrid approach allows for more control over critical data on-premises, while less sensitive information and resources can be easily scaled up and down in the cloud.

▶ **How has your organization's use of the following cloud models changed within the past two years?**

	DECREASED	NO CHANGE	INCREASED	
Cloud edge technology (SASE)	7%	24%	62%	**69%**
Hybrid cloud	9%	25%	57%	**66%**
Multi cloud	10%	29%	51%	**61%**
Single cloud	23%	38%	16%	**39%**
On-prem/ private cloud	21%	55%	3%	**24%**

● 2-year net gain/loss

This divergence signals a critical inflection point: security teams no longer secure "the cloud" as a centralized perimeter, but a constantly shifting matrix of platforms, providers, and traffic flows that require a solid understanding of both private and public cloud technologies. That fragmentation directly fuels many of the security challenges explored throughout this report, from gaps in threat visibility to inconsistent policy enforcement and growing operational overhead.
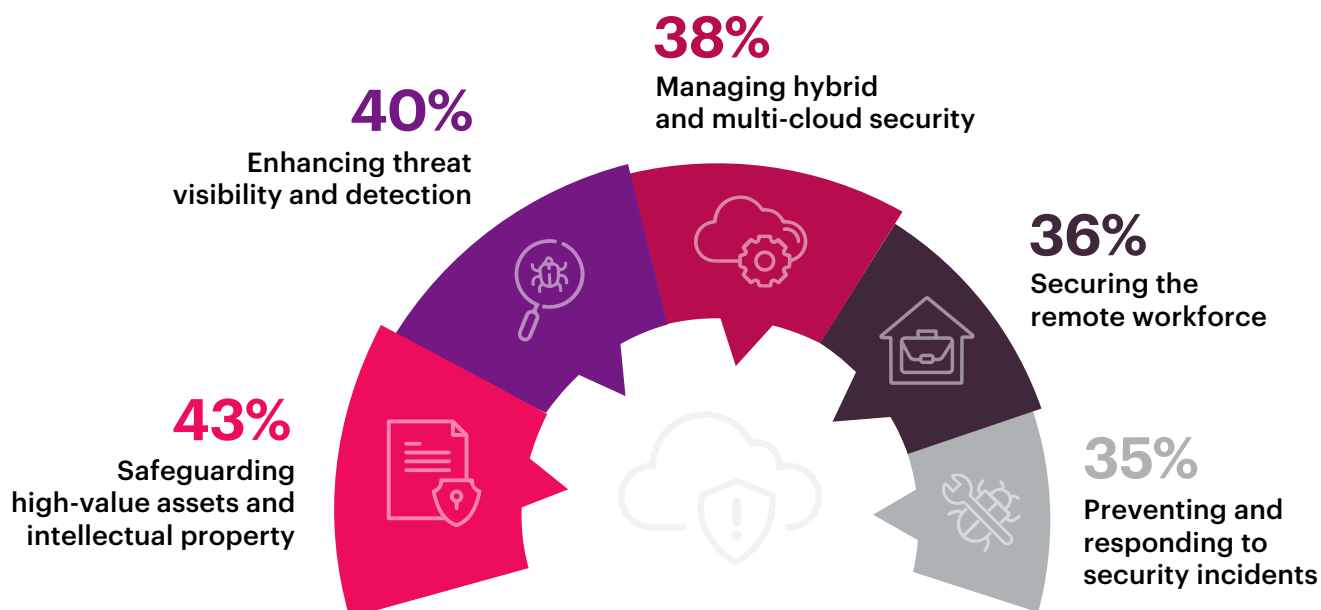
Defending Data, Identities, and Unseen Threats

Transitioning to a hybrid cloud model has brought added layers of complexity, with 38% of individuals identifying this as one of their primary cybersecurity challenges. While a hybrid cloud can strengthen security measures, it also presents new risks, particularly if data isn't properly managed and safeguarded across all environments.

According to our survey, 43% of respondents reported that safeguarding high-value digital assets, including proprietary datasets, intellectual property, and customer information, is a top challenge.

Close behind, 40% point to enhancing threat visibility and detection across hybrid environments, reflecting persistent blind spots in cloud-native telemetry — the continuous collection of system and activity data used to detect threats — as well as identity-based access patterns and lateral traffic flows. Additionally, this creates complications in identity and access management (IAM) and policy enforcement, as 36% are struggling to secure a widely distributed workforce.

Lastly, 35% of our audience finds preventing and responding to security incidents to be a major issue — confirmed by the increased number of security incidents and response times cited in subsequent sections of this report.

▶ **What are your organization's biggest cybersecurity challenges?**

38%
Managing hybrid
and multi-cloud security

40%
Enhancing threat
visibility and detection

36%
Securing the
remote workforce

43%
Safeguarding
high-value assets and
intellectual property

35%
Preventing and
responding to
security incidents

Lateral Movement Remains a Hidden Risk

In cybersecurity, visibility is everything. Most organizations focus on defending their network perimeter—keeping an eye on traffic coming in and going out to stop intrusions. However, the real threat emerges when an attacker successfully infiltrates the network.

According to our survey, only 17% of organizations have full visibility into lateral traffic within their cloud environments. The rest either have partial (54%) or no visibility at all (29%), leaving a critical detection gap in the middle of the attack lifecycle. Once inside, adversaries often use legitimate credentials and lateral movement techniques to escalate access and move quietly through infrastructure. When internal traffic patterns go unmonitored, these behaviors often go undetected until serious damage is done.

▶ **What level of visibility do you have into your lateral/east-west traffic?**

17%
Full visibility

54%
Some visibility

29%
No visibility
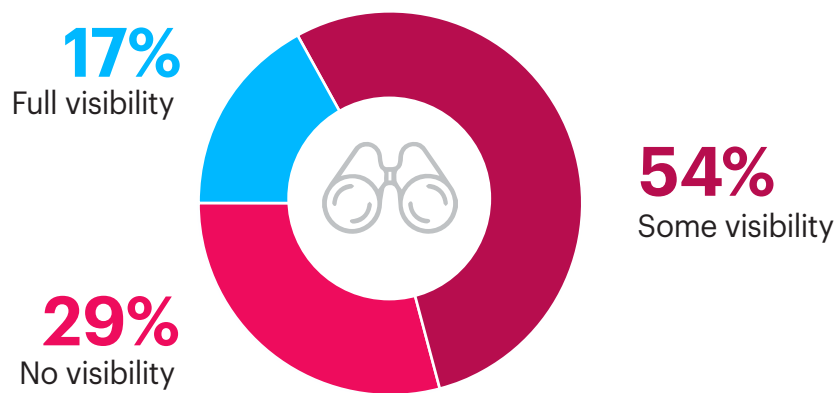
Closing this gap requires continuous inspection of east-west or workload-to-workload traffic, identity-aware segmentation policies, and real-time collection of runtime activity data — enabling security teams to detect privilege escalation, suspicious behavior, and cross-environment pivoting as it happens.
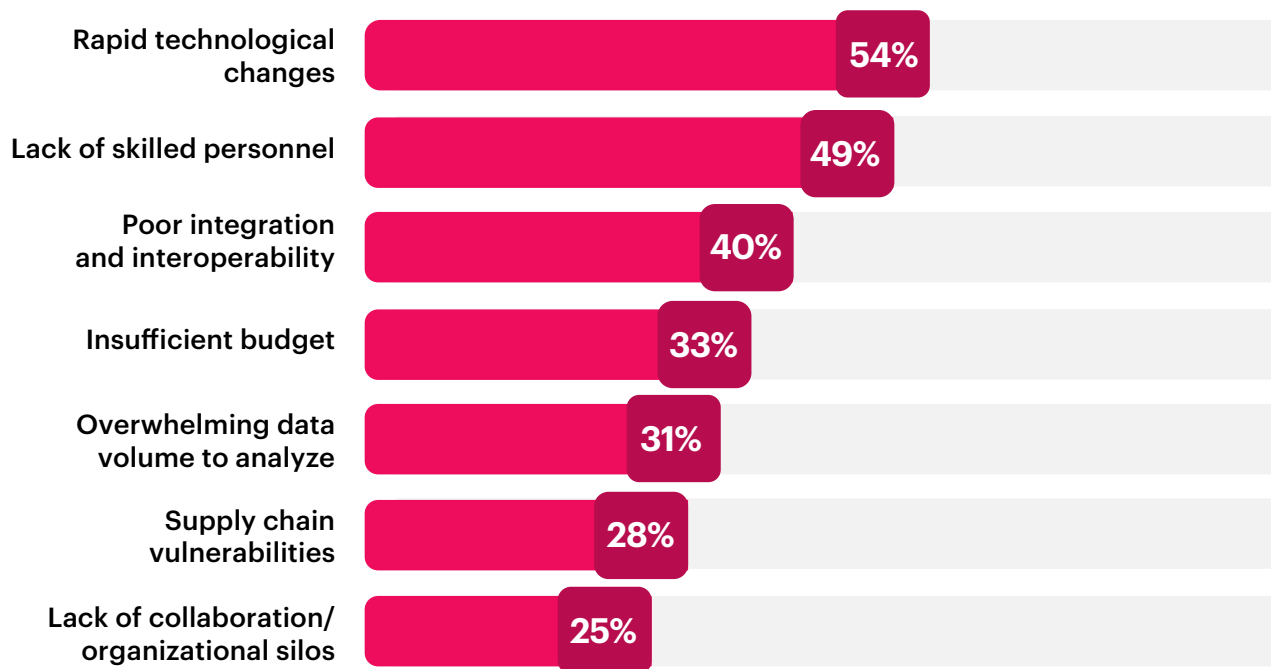
Why Security Strategies Fall Short

The cloud security challenges organizations face are well known. However, the real reasons those challenges persist — and why even the most well-resourced security programs fail — are internal limitations in skills, integration, and architectural execution.

The most widely cited barrier is the pace of technological change (54%), which continues to outstrip security teams' ability to operationalize controls and enforce policies across dynamic environments. Nearly half (49%) report a shortage of skilled personnel, especially professionals with cross-domain knowledge spanning security operations, automation, and AI. Tool fragmentation compounds the problem: 40% of respondents cite poor integration between platforms, resulting in blind spots, inconsistent policies, and sluggish remediation.

Other issues include budget constraints (33%), data overload (31%), supply chain vulnerabilities (28%), and organizational silos (25%) that limit visibility and slow coordination across teams.

▶ **Which of the following barriers inhibit your organization from adequately defending against cyber threats?**

Barrier	Percentage
Rapid technological changes	54%
Lack of skilled personnel	49%
Poor integration and interoperability	40%
Insufficient budget	33%
Overwhelming data volume to analyze	31%
Supply chain vulnerabilities	28%
Lack of collaboration/organizational silos	25%

These are not just operational annoyances but structural weaknesses that attackers exploit. Before discussing better detection, faster response, or smarter automation, we must acknowledge the internal complexity that keeps many organizations stuck. The next chapter shows what happens when these internal cracks become external failures.

02

Rising Security Incidents

Cloud-related breaches are rising sharply, and most organizations are detecting them late, remediating them slowly, and discovering them reactively.

- 65% of organizations reported a cloud-related incident in the past 12 months, up from 61% the year before.

- 38% take more than 24 hours to detect an incident, and 62% need another full day or more to fully remediate.

- Only 35% discovered incidents through their security tools; the rest relied on users, audits, or third parties.

Cloud Security Incidents are Escalating

Despite years of investment in cloud security tools and strategies, incident rates are climbing, exposing an incongruence between modern cloud environments and the defenses meant to protect them.

Our survey reveals that 65% of organizations experienced at least one cloud-related security incident in the past 12 months, up from 61% the year prior. This surge shows attackers are exploiting misconfigured assets, identity governance gaps, and inconsistent enforcement across multi-cloud and hybrid deployments. The same complexity that promised agility is now eroding security visibility, fragmenting monitoring data, and slowing response — giving adversaries more room to operate undetected.

▶ **Has your organization experienced any security incidents related to cloud usage in the last 12 months?**

65%
YES

14%
NO

21%
Not sure/
can't disclose
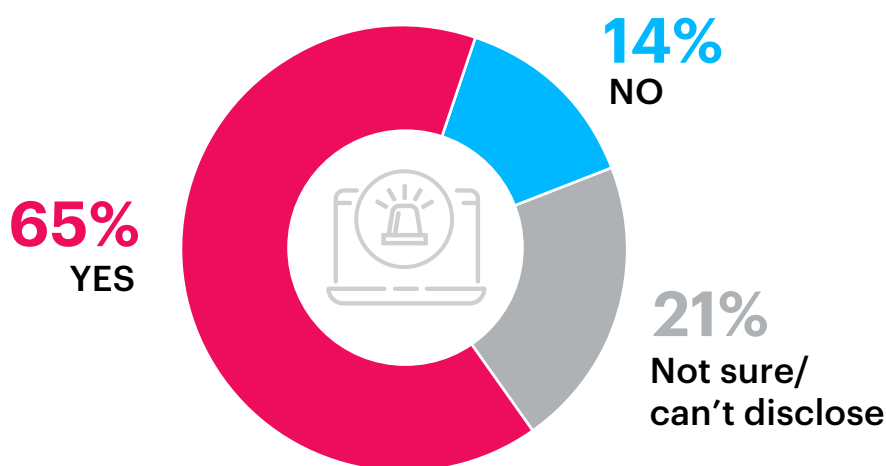
Every attack — whether exploiting a zero-day vulnerability, moving laterally, or exfiltrating data — ultimately traverses the network and application layers. By shifting focus to real-time traffic inspection, threat prevention, and AI-driven enforcement at the transport, network, and application layers, organizations can move beyond passive risk detection to proactive breach prevention.

Detection Remains Largely Reactive

In many cases, cloud security incidents are not discovered by monitoring systems but by end users, external parties, or during routine audits. This reliance on human and third-party reporting reveals a systemic weakness in how cloud threats are detected today.

Only 35% of respondents in our survey said that their cloud security tools were the first to detect a breach. The remaining 65% discovered incidents through indirect or delayed sources: 23% were flagged by affected users, 12% during incident response investigations, 10% via external notifications, and 9% during routine audits.

▶ **How did you first discover the incident?**

35%
Security monitoring tools detected it

23%
Affected users reported it

12%
Incident response investigation

10%
External notification

Routine security audit **9%**

Other 11%

These numbers suggest that most organizations cannot confidently rely on their existing threat detection stack to surface active attacks. Delayed or missed discovery increases dwell time, complicates remediation, and undermines the perceived reliability of controls that security teams depend on. The core issue isn't a lack of tools — it's failure to correlate various sources of data, detect behavioral anomalies, and continuously monitor cloud attack surfaces with real-time intelligence.

Fixing this requires more than tuning alert thresholds. Today's cloud security must extend beyond access control to secure traffic in all directions and across all layers. Only by embedding inline prevention at every ingress and connection point can we eliminate blind spots and prevent attackers from reaching sensitive systems.

Delayed Detection Widens the Blast Radius

Cloud environments pose more risk than any team can realistically mitigate in a timely manner. Vulnerabilities, misconfigurations, and excessive permissions continue to emerge while exploitation timelines shrink to minutes, leaving teams with an impossible race between detection and compromise.

The survey reveals that only 9% of organizations detected a cloud-related incident within the first hour. Just 48% caught it within the first 24 hours, 38% took longer than a full day, and 14% weren't sure how long it took. These numbers reveal more than a visibility gap: they expose the operational cost of disconnected security data streams, non-correlated alerts, and missing context. In fast-moving cloud environments, where attackers can escalate privileges and pivot laterally within minutes, delayed detection turns small intrusions into multi-system compromises.

▶ **How long did it take to detect an incident?**

< 1 hr	9%
1-12 hrs	18%
12-24 hrs	21%
1-7 days	15%
1-4 weeks	13%
+1 month	10%

38% of organizations say it takes **more than 24 hours** to detect an incident
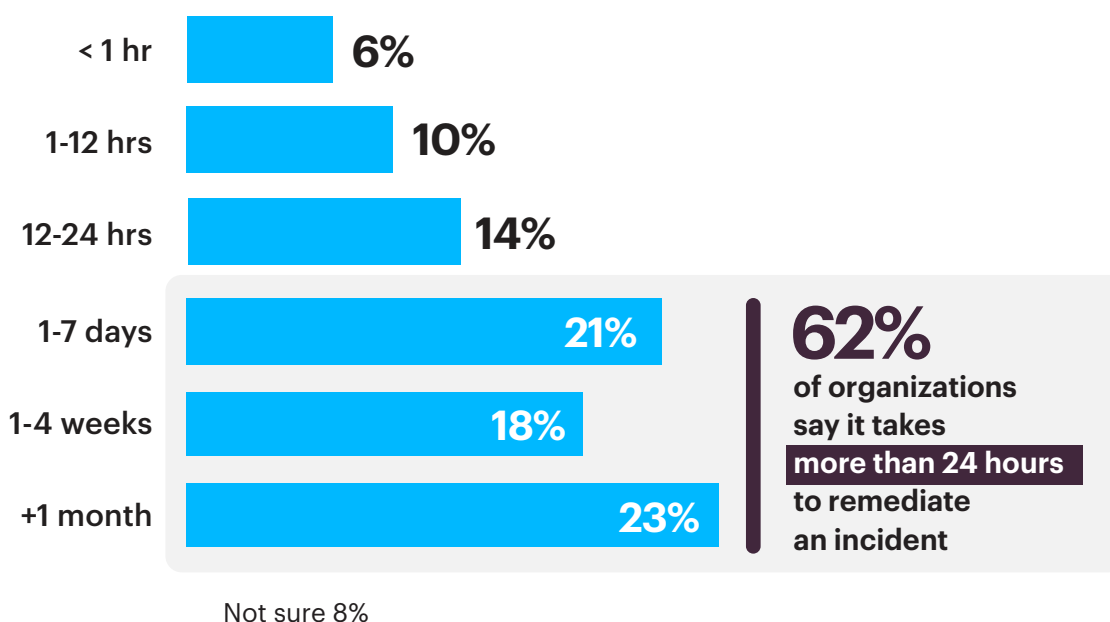
Not sure 14%

In order to eliminate the delay between detection and containment, there needs to be an immediate, coordinated response across the entire ecosystem, including both cloud and enterprise environments. This can be accomplished by decentralizing security and network architecture where security controls and policy enforcement are embedded directly into distributed network nodes—across edge devices, branches, clouds, and data centers—while still integrating with centralized services as needed. This way a threat identified in one area or account can trigger policy adjustments across the entire organization, effectively stopping attackers on a global scale.

Slow Remediation Extends Risk Exposure

Detecting a breach is only the first hurdle. For most organizations, resolving the incident — restoring systems, validating integrity, and neutralizing lateral spread — takes far longer than it should.

Only 6% of organizations in our survey remediated a cloud-related incident within the first hour. Just 30% closed the incident within 24 hours, while 62% took longer — with many lacking automated rollback, policy revalidation, or real-time containment capabilities to accelerate recovery. These delays are rarely due to technology alone. Manual handoffs between teams, inconsistent controls across environments, and limited runtime visibility all contribute to slower response, giving attackers more time to escalate access, pivot across workloads, and exfiltrate sensitive data. In dynamic multi-cloud ecosystems, where assets interconnect and change frequently, every hour of remediation delay expands dwell time, business disruption, and forensic uncertainty.

▶ **How long did it take to remediate an incident?**

< 1 hr	**6%**
1-12 hrs	**10%**
12-24 hrs	**14%**
1-7 days	**21%**
1-4 weeks	**18%**
+1 month	**23%**

62% of organizations say it takes **more than 24 hours** to remediate an incident

Not sure 8%

Given the understaffing and skill gaps in both cloud and security teams, organizations must eliminate the need for human intervention in threat response. To accomplish this, threat containment must be automated to prevent attacks from escalating. This entails making immediate adjustments to security policies, automatically isolating compromised systems, and updating firewall rules on the fly to block ongoing threats. Furthermore, automation should not be limited to cloud environments but should also integrate with on-premises security measures, VPN access policies, and third-party security tools. This comprehensive approach ensures cohesive security management across the enterprise, with real-time updates to network and access controls to stop threats before they cause harm.

03

The Hidden Cost of Cloud Complexity

Cloud security spending is rising — not just in dollars, but in time, complexity, and burnout. Tool sprawl and staffing inefficiencies are draining resources without improving outcomes.

- 71% of organizations use more than 10 tools to secure their cloud environments, and 16% use more than 50.

- 89% say the cost of managing cloud security across multiple providers is moderately to extremely significant.

- The challenge isn't just consolidation — it's integrating tools that share intelligence, reduce redundancy, and support consistent policy enforcement.

Fragmentation Drives Up Security Costs & Complexity

Scaling security across multiple clouds has introduced a cost paradox: as coverage expands, so do financial overhead and complexity — fueled by disconnected tools, parallel staffing, and platform-specific training requirements.

According to our survey, 89% of organizations rate the cost of managing cybersecurity consistently across cloud environments as moderately to extremely significant. A combined 48% rate it as very or extremely significant, reflecting the real impact of licensing duplication, redundant tooling, and siloed security processes.

Instead of achieving economies of scale, many teams are forced to maintain specialized skills for each cloud provider and security tool, support overlapping systems, and manage inconsistent policies — all of which increase the cost of both technology and human capital. These inefficiencies are compounded by constant context-switching across consoles, vendors, and workflows, draining analyst capacity and reducing strategic visibility.

▶ **How significant is the cost overhead (tooling, staffing, training) of managing cybersecurity consistently across multiple clouds?**

89%
organizations rate the cost of managing security as moderately to extremely significant

14%	34%	41%	7%	4%
Extremely significant	**Very significant**	**Moderately significant**	**Slightly significant**	**Not significant**

Solving this problem requires more than budget reallocation. Organizations need to simplify the operating model itself — consolidating threat prevention, policy enforcement, and security training within a unified framework that lowers overhead and drives consistency across every cloud, workload, and identity.

Tool Sprawl Weakens Cloud Defense

In an effort to secure every layer of the cloud stack, most organizations have accumulated dozens of point solutions — often deployed in response to specific threats or compliance demands, rather than deliberate strategic design. The result is a fragmented toolset that increases overhead, slows detection, and reduces overall effectiveness.

Our survey shows that 71% of organizations use more than 10 security tools to protect their cloud environments, with 16% using more than 50 tools! This dramatic sprawl leads to duplicated alerts, inconsistent policy enforcement, and siloed visibility across networks, workloads, and applications.

It also creates operational friction: normalization of monitoring data breaks down, configuration changes cause unintended conflicts, and SIEM/SOAR pipelines become overloaded with uncorrelated signals. Analysts often spend more time managing tools than managing threats.

▶ **How many different security tools does your organization use to secure its entire cloud environment?**

71% of organizations use more than 10 security tools to protect their cloud environments

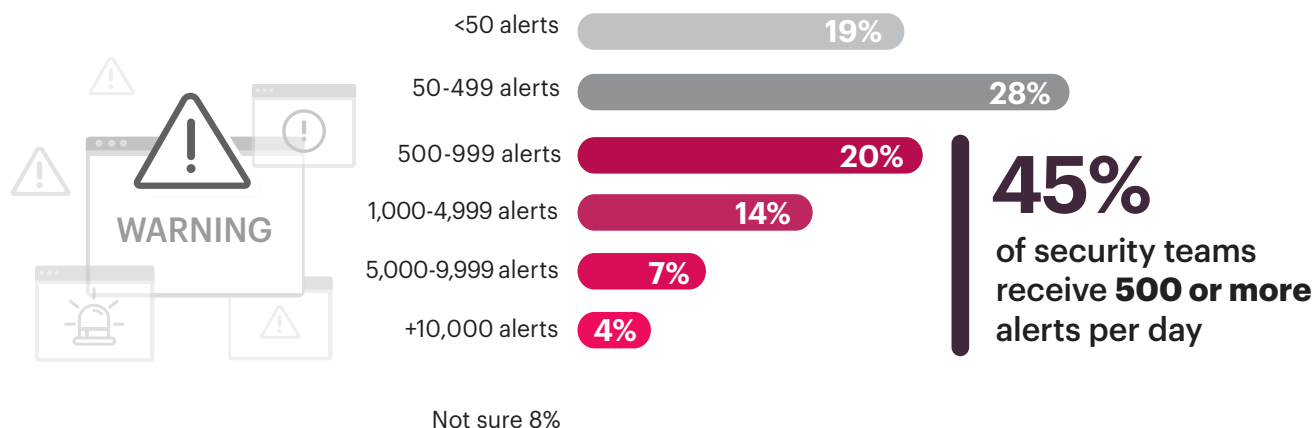| 24%	36%	19%	12%	4%
1-10 tools	11-25 tools	26-50 tools	51-100 tools	+100 tools

Not sure 5%

Tool Fatigue Leads to Alert Fatigue

The volume of alerts flowing in from disconnected tools, often with overlapping or redundant signals, is interfering with the ability to focus on and prioritize alerts. And that's exactly when things slip through the cracks.

Our survey shows that almost half of organizations receive at least 500 security alerts per day. One in four report over 1,000 alerts daily, with 4% handling more than 10,000 — a deluge of alerts that makes it nearly impossible to prioritize threats in real time. Only 19% report receiving fewer than 50 alerts a day.

Without correlation, enrichment, and context, alert volume becomes a liability, increasing the likelihood of missed threats, delayed triage, and burnout among response teams.

▶ **How many security alerts does your security team receive on an average day?**

Alert volume	Percentage
<50 alerts	19%
50-499 alerts	28%
500-999 alerts	20%
1,000-4,999 alerts	14%
5,000-9,999 alerts	7%
+10,000 alerts	4%
Not sure	8%

WARNING

45% of security teams receive **500 or more alerts per day**

Traditional approaches focus on identifying risk by scanning workloads, code, and configurations in search of vulnerabilities before attackers find them. However, this creates alert fatigue, drains security resources, and still leaves environments vulnerable to zero-days and rapidly evolving exploits. Worse, it places undue security enforcement burden on developers and DevOps engineers, whose primary focus is not threat mitigation.

What's needed is defense in depth, not defense in sprawl: a unified, intelligent architecture that consolidates enforcement across layers and environments without relying on a dozen disconnected point products or siloed teams. All attacks traverse the network and application layers. That is where proper protection must live — inline, autonomous, and operated by the security team. Prioritize security solutions that share intelligence and enforce policies together, both in house and with other vendors in the market, to create an 'open garden' platform.

Finally, even with a super-tuned system that presents analysts with a package of alerts, they still need to investigate, understand, and come to conclusions. This is where automating AI and machine learning can give security teams that added layer of insight and protection.

04

AI Security Modernization

AI is rapidly becoming a core security priority — but defenders still feel outpaced by AI-powered threats and blocked by implementation challenges.

- 68% of organizations rank AI adoption as a cybersecurity priority, yet only 25% feel confident defending against AI-driven attacks.

- Only 43% have adopted AI/ML-based WAF capabilities, while 61% of organizations primarily use signature-based WAF detection. These results reflect a slow shift toward modernization, but the dominance of static models leaves application and API surfaces vulnerable to fast-moving attacks.

- Top AI adoption barriers include lack of skilled personnel (62%), integration friction (56%), and limited model explainability (32%).

AI Rises as a Security Priority

After years of battling alert overload, signal noise, and delayed incident response, security leaders are no longer treating AI as optional. It's becoming a top priority for scaling detection and automating defense in cloud environments that now move faster than humans can manage.

Up from 54% last year, 68% of organizations now rank AI adoption as a cybersecurity priority — including 21% (13% in 2024) who say it's their top initiative. This shift reflects a clear mandate: legacy detection models and human-driven triage can't scale to meet modern cloud threats.

AI-powered techniques — from behavioral modeling and anomaly scoring to automated correlation and predictive threat identification — offer a way to reduce alert volume, surface high-risk activity faster, and trigger faster containment actions.

▶ **How does AI adoption rank among your organization's cybersecurity priorities?**

21%
Top priority

47%
High priority

26%
Medium priority

6%
Low/not a priority

68%
of organizations now rank AI adoption as a cybersecurity priority
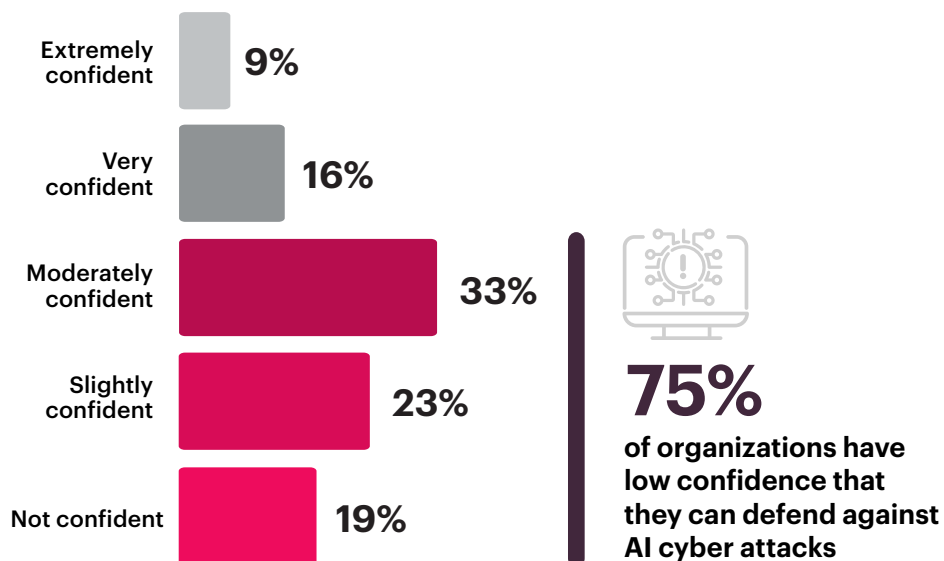
↑ Up from 54% last year
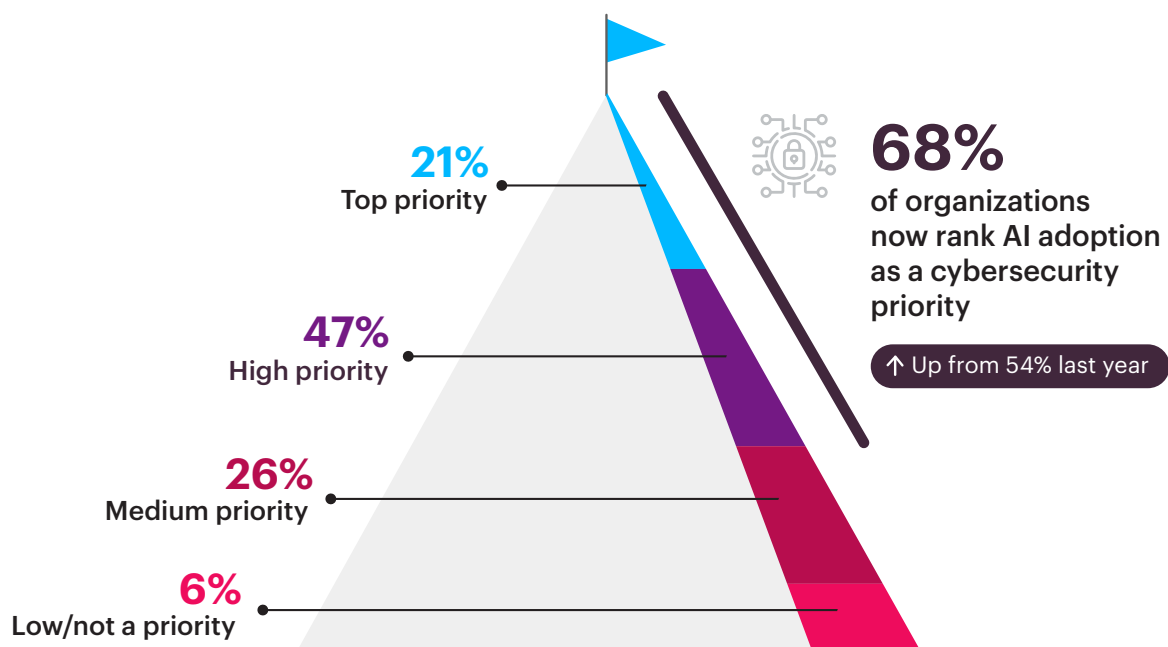
Real impact depends on more than adopting AI tools. Organizations must embed AI into their operational workflows, ensuring it can access real-time activity data across workloads, analyze behavior in the moment, and trigger precise response actions across detection systems, identity layers, and workload protections — without adding complexity or added vulnerabilities to already overburdened teams.

Most Organizations Feel Unprepared for Adversarial AI

Despite prioritizing AI for their own defenses, most organizations feel under-equipped to handle the wave of attacks powered by adversarial machine learning and automated decision engines.

Only 25% of organizations feel confident in their ability to defend against AI-powered threats. The rest cite growing concern over malware, automated evasion tactics, AI-generated phishing, and synthetic identity creation — attack types that adapt in real time and bypass static defenses with ease. This gap in capability is growing wider: defenders are still working within human-paced investigation and rule tuning, while AI-enabled attackers automate reconnaissance, payload mutation, and target selection in seconds.

▶ **How confident are you in your organization's ability to defend against AI powered cyber attacks?**

Confidence Level	Percentage
Extremely confident	9%
Very confident	16%
Moderately confident	33%
Slightly confident	23%
Not confident	19%

75% of organizations have low confidence that they can defend against AI cyber attacks

Bridging this gap requires defense strategies that can match machine-speed threats with machine-speed response, delivering visibility, risk assessment, and real-time data loss prevention across the entire cloud infrastructure. This will reduce the time needed for security tasks, such as threat hunting, analysis, and resolution, driving toward a goal of true autonomous zero trust.

WAF Strategies Slowly Shift Toward AI

Cloud applications rely on APIs and web interfaces as their primary communication channels, making the Front Door (Internet Edge) the most exposed attack surface in the cloud. Despite these growing threats, many organizations still rely on legacy WAF detection models that struggle to keep up with evasive and dynamic AI-powered attack techniques.

According to our survey, 61% of organizations primarily use signature-based detection in their WAFs — a method well suited for known exploits, but easily bypassed by polymorphic payloads, logic-based attacks, and API abuse. This is followed by 56% that have adopted behavioral analysis to detect abnormal usage patterns and 54% that integrate cloud-based threat intelligence to stay current with emerging threats. Nearly half (49%) use rate limiting and bot mitigation to defend against credential stuffing, scraping, and inventory hoarding, while 43% apply AI/ML-driven techniques to detect previously unseen attacks.

▶ **Which detection and protection methods does your Web Application Firewall (WAF) primarily use?**

Behavioral analysis
Cloud-based threat intelligence
Rate limiting and bot mitigation
Signature-based detection
AI/ML-driven detection
56%
54%
61%
49%
43%
We do not use a WAF
8%
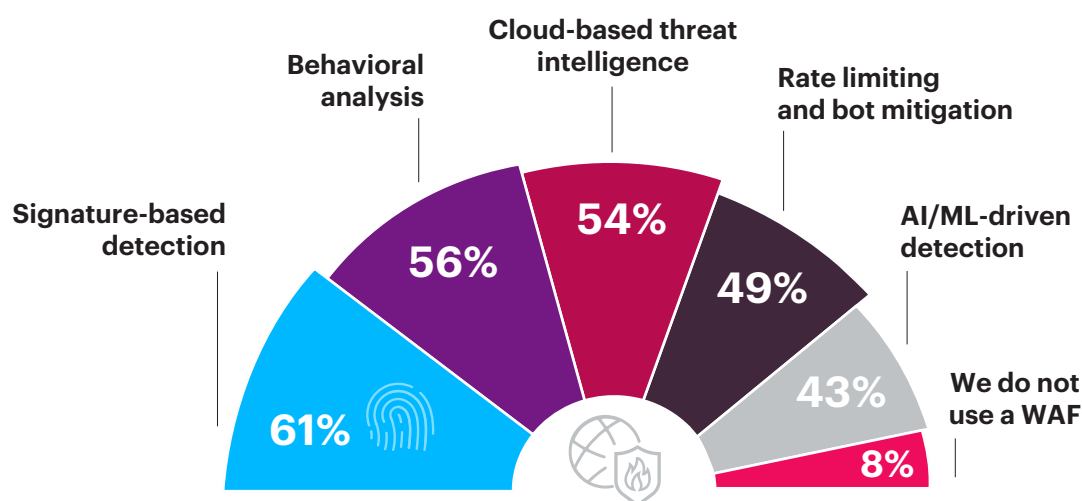
These trends indicate a slow uptick in the usage of AI-driven WAF technology, but they also highlight a significant shortfall in signature-based methods. Today's attacks employ sophisticated methods and protocols to avoid detection; for instance, Log4j had seven different attack methods. Signature-based WAF rules are often either too narrow, missing emerging threats, or too broad, causing false positives and requiring many exceptions for the application to function properly. This is a very labor-intensive process.
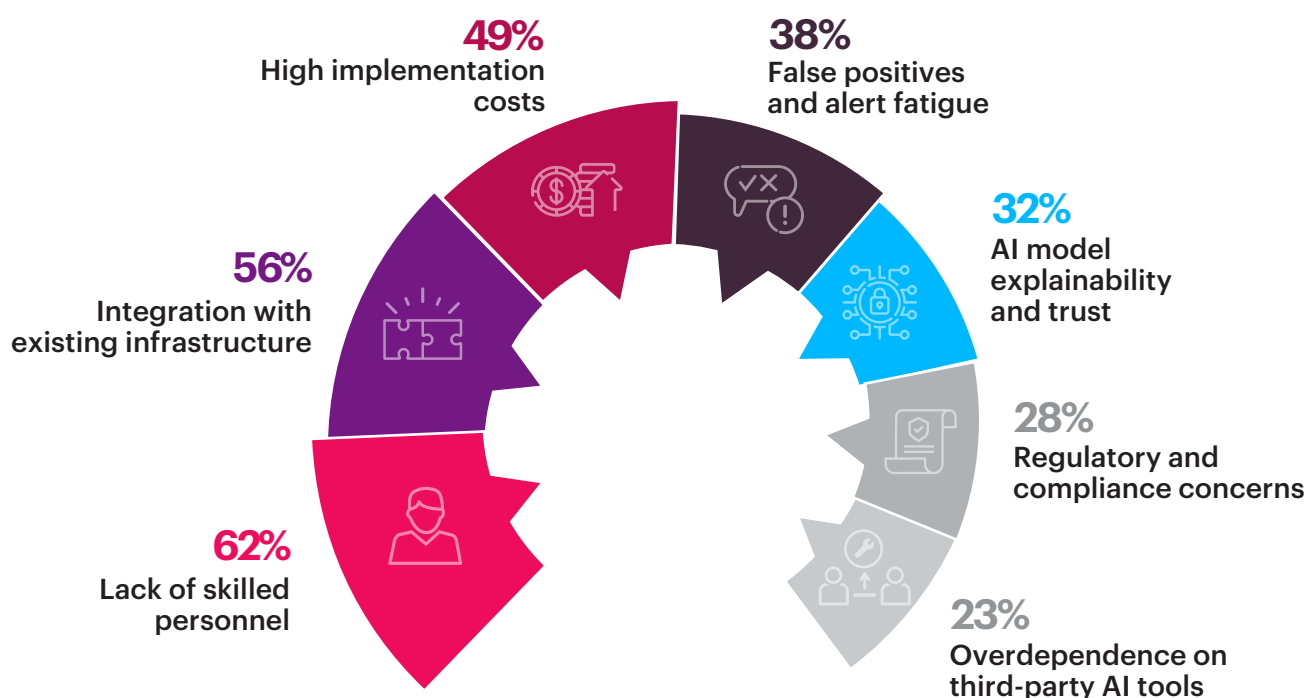
Without prior knowledge of an attack's characteristics, it is impossible to create an effective signature for zero-day attacks. This leads to missed attacks and an abundance of false positives. To stay ahead, WAF strategies must incorporate AI/ML driven detection with API discovery and schema validation that give full visibility into API state. This is the only way to predict and prevent zero-day attacks.

AI Roadblocks Reveal Gaps in Talent, Trust, and Integration

Organizations may be prioritizing AI — but their ability to implement it effectively is being held back by fundamental gaps in people, process, and architecture.

According to our survey, the top implementation challenge is a shortage of skilled personnel (62%), especially professionals who understand both AI models and real-world security operations. Integration friction follows closely (56%), as many teams are still working with legacy stacks that lack the interfaces, data flow access, or orchestration capabilities to support AI-driven detection and response. Nearly half (49%) cite high implementation costs, while 38% struggle with excessive false positives and 32% lack confidence in how AI models make decisions — a major hurdle in operationalizing AI without explainability or traceability. Compliance and governance issues (28%) and overdependence on third-party AI tools (23%) round out the picture.

▶ **What are the top challenges your organization has faced trying to implement AI/ML into your security operations?**

49%
High implementation costs

38%
False positives and alert fatigue

32%
AI model explainability and trust

56%
Integration with existing infrastructure

28%
Regulatory and compliance concerns

62%
Lack of skilled personnel

23%
Overdependence on third-party AI tools

AI is the most valuable tool for analyzing, detecting, preventing, and predicting threats. Security teams need to invest in platforms that can aggregate and analyze large-scale activity data alongside millions of indicators of compromise (IOCs). Look for solutions that are being fueled by massive amounts of connected networks and end point devices that are closely monitored by research teams throughout the world. This ability to synchronize IOCs across all enforcement points is crucial in maintaining security and mitigating threats in real time.

Turning Insight into Action: Cloud Security Priorities for 2025

The following priorities reflect what security leaders across industries are focusing on to close the gap between cloud complexity and effective defense.

1 **Architect security for a decentralized cloud**
As hybrid, multi-cloud, and edge adoption accelerate, static security models collapse under the complexity. With 38% citing hybrid complexity as a top challenge, teams must shift to a more distributed security approach that supplies security where it's needed, when it's needed.

2 **Network security is more crucial than ever**
Only 17% of organizations have full visibility into east-west traffic, giving attackers space to move undetected. Embed real-time inspection and lateral movement detection directly into cloud workloads — not just at the perimeter.

3 **Break the alert fatigue cycle**
Almost half of teams (45%) are flooded with 500+ alerts per day, making it harder to spot real threats. Apply a hybrid mesh layer that connects and automates the entire ecosystem, transforming alerts into real-time action and eliminating the delay between detection and containment.

4 **Integrate before you consolidate**
71% of organizations use over 10 tools, but 40% still struggle with poor interoperability. Prioritize security solutions that share intelligence and enforce policies together— both in house and with other vendors in the market to create an 'open garden' platform.

5 **Use AI to accelerate defense, not just analytics**
While 68% prioritize AI adoption, only 25% feel confident defending against AI-powered attacks. To ensure the safe use of powerful AI tools look for a solution that provides comprehensive security and compliance features, specifically designed to manage the unstructured and conversational nature of GenAI prompts.

6 **Modernize app-layer defenses before attackers do**
With 61% still relying on signature-based WAFs, APIs and apps remain exposed to evasive attacks. Shift to WAF strategies that use AI/ML to detect behavior anomalies, adapt to new attack patterns, and secure traffic across APIs and microservices.

The best practices outlined here aren't just smart — they're grounded in the frontline experience of the security leaders who contributed to this report. Their message is clear: securing the cloud in 2025 means simplifying what's become unmanageable, automating where humans can't keep up, and aligning architecture, identity, and threat prevention into one coordinated defense strategy.
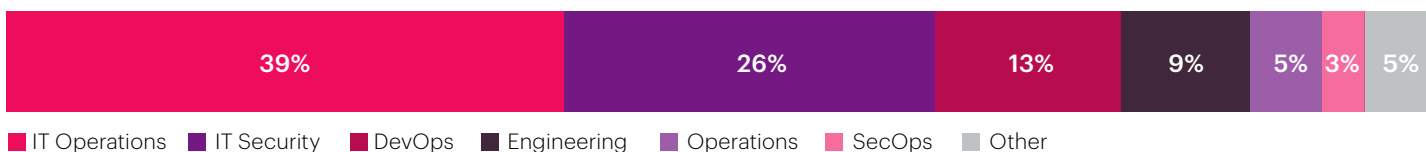
Methodology and Demographics

This cloud security survey was conducted in early 2025 and gathered responses from 937 cybersecurity professionals across a wide range of industries and organization sizes. Respondents included CISOs, cloud architects, security analysts, and IT leaders responsible for securing hybrid, multi-cloud, and SaaS environments.

A stratified sampling approach ensured balanced representation across roles and segments, yielding a 95% confidence level with a ±3.2% margin of error to ensure valid industry representation. Some questions used a "select all that apply" format, so some totals exceed 100% — reflecting the overlapping, multi-dimensional nature of modern cloud security challenges.
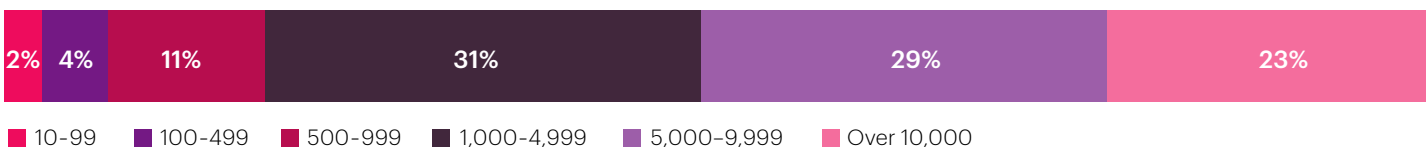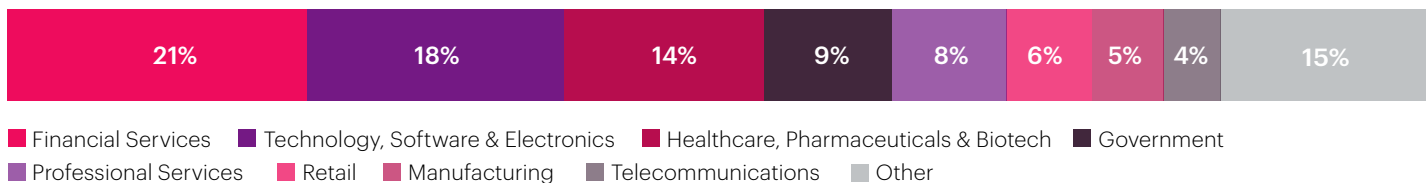
CAREER LEVEL

27%	23%	19%	9%	6%	4%	12%

■ Specialist ■ Manager/Supervisor ■ Director ■ CTO, CIO, CISO, CMO, CFO, COO ■ Consultant ■ Owner/CEO/President
■ Other

DEPARTMENT

39%	26%	13%	9%	5%	3%	5%

■ IT Operations ■ IT Security ■ DevOps ■ Engineering ■ Operations ■ SecOps ■ Other

COMPANY SIZE

2%	4%	11%	31%	29%	23%

■ 10-99 ■ 100-499 ■ 500-999 ■ 1,000-4,999 ■ 5,000–9,999 ■ Over 10,000

INDUSTRY

21%	18%	14%	9%	8%	6%	5%	4%	15%

■ Financial Services ■ Technology, Software & Electronics ■ Healthcare, Pharmaceuticals & Biotech ■ Government
■ Professional Services ■ Retail ■ Manufacturing ■ Telecommunications ■ Other

Check Point Software Technologies Ltd. checkpoint.com is a leading protector of digital trust, utilizing AI-powered cyber security solutions to safeguard over 100,000 organizations globally. Through its Infinity Platform and an open garden ecosystem, Check Point's prevention-first approach delivers industry-leading security efficacy while reducing risk. Employing a hybrid mesh network architecture with SASE at its core, the Infinity Platform unifies the management of on-premises, cloud, and workspace environments to offer flexibility, simplicity and scale for enterprises and service providers.

www.checkpoint.com

Cybersecurity

I N S I D E R S

TURNING CYBERSECURITY INSIGHTS INTO STRATEGIC INFLUENCE

Cybersecurity Insiders delivers evidence-backed insights that empower security leaders to make informed, strategic decisions. Backed by over a decade of research and a global network of 600,000+ cybersecurity professionals, we provide actionable intelligence to help leaders navigate emerging threats, evaluate new technologies, and shape forward-looking strategies with confidence.

For cybersecurity vendors, we turn research into results — delivering credibility, visibility, and demand through high-impact formats such as:

- Data-powered market reports that establish thought leadership,
- Webinars that build trust with buyers through credible, expert-led narratives,
- CISO guides that showcase best practices,
- Product reviews that independently validate solutions,
- How-to articles that educate buyers, and
- Award programs that elevate brand reputation.

By combining this content with built-in distribution, we help brands earn trust, amplify awareness, and drive demand in a crowded cybersecurity market.

For more information visit

cybersecurity-insiders.com