TREND MICRO™

2025

CLOUD SECURITY REPORT

Challenges and CISO Strategies Reshaping Cloud Security in the AI Era

Research by

Cybersecurity INSIDERS

Overview

Cloud security in 2025 is defined by contradiction: persistent threats and low confidence on one side, maturing strategies and accelerating automation on the other. While the fundamentals of cloud risk remain stubbornly familiar—unauthorized access, data leakage, and phishing—security teams today are grappling with a deeper, more structural challenge: how to defend sprawling, fast-moving, multi-cloud environments with tools and processes built for a different era.

To better understand how security leaders are responding, we conducted our annual cloud security survey, gathering insights from over 500 cybersecurity professionals across Europe. We asked where their strategies are evolving, where confidence is breaking down, and which technologies—including automation and AI—they see as essential for navigating the complexity of modern cloud environments. This 2025 Cloud Security Report is the result of that effort.

Key findings include:

1. **Cloud threats are evolving—but defenses aren't keeping pace.**
   Security teams identify advanced threats like ransomware (74%) and zero-day vulnerabilities (63%) as their most pressing concerns, highlighting a dangerous escalation in attacker sophistication and urgency. At the same time, foundational threats persist, with unauthorized access (64%), data breaches (62%), and phishing attacks (60%) continuing to dominate actual security incidents. This blend of surging advanced threats and stubbornly recurring risks underscores why organizations must urgently enhance their defenses—especially around identity controls, workload security, and real-time visibility across cloud environments.

2. **Detection and response are fragmented and it's slowing teams down.**
   Only 21% of organizations feel highly confident in their visibility across workloads, and just 25% trust their tools to detect advanced threats. Root cause analysis is now the most time-consuming part of incident response (34%), and 97% report difficulty executing a unified response across providers—a direct result of both architectural fragmentation and operational overhead.

3. **Operational friction is limiting both compliance and automation.**
   Compliance efforts are held back by tool sprawl (63%), limited automation (58%), and friction integrating with DevOps pipelines (37%). Although automation is seen as the most impactful improvement to incident response (36%), only 52% of organizations currently prioritize it— exposing a gap between awareness and action.

4. **Security priorities are shifting toward unified control.**
   Top strategic priorities include data security (83%), identity and access management (77%), and threat detection (72%). Together, they reflect a shift toward embedded policy enforcement and real-time visibility—moving security from reactive posture to foundational architecture.

5. **AI is no longer aspirational—it's operational.**
   Security teams are no longer experimenting with AI—they're implementing it. The top use cases include threat detection (75%), anomaly analysis (70%), and automated response (62%). As cloud complexity scales, AI is emerging not just as a force multiplier, but as a necessary control layer for scalable, intelligent defense.

The data reveals a clear trajectory: security leaders are moving away from disconnected tools and manual workflows toward integrated platforms that converge detection, policy enforcement, and automated response. What's emerging is not just a smarter toolset, but a cloud security strategy engineered for speed, scale, and continuous control.

The following chapters unpack these trends systematically. Chapter I explores where and how cloud risk is accumulating. Chapter II examines why current detection strategies fall short in delivering effective responses. Chapter III evaluates compliance challenges in the face of operational friction, and Chapter IV highlights the strategic shift toward integrated, intelligent defense.

01

Cloud Risk: What Are We Up Against?

Today's threat landscape reflects more than just external attackers—it's the byproduct of expanding architectures, overexposed identities, and misaligned controls. This chapter maps where risk is accumulating and why it's proving hard to contain.

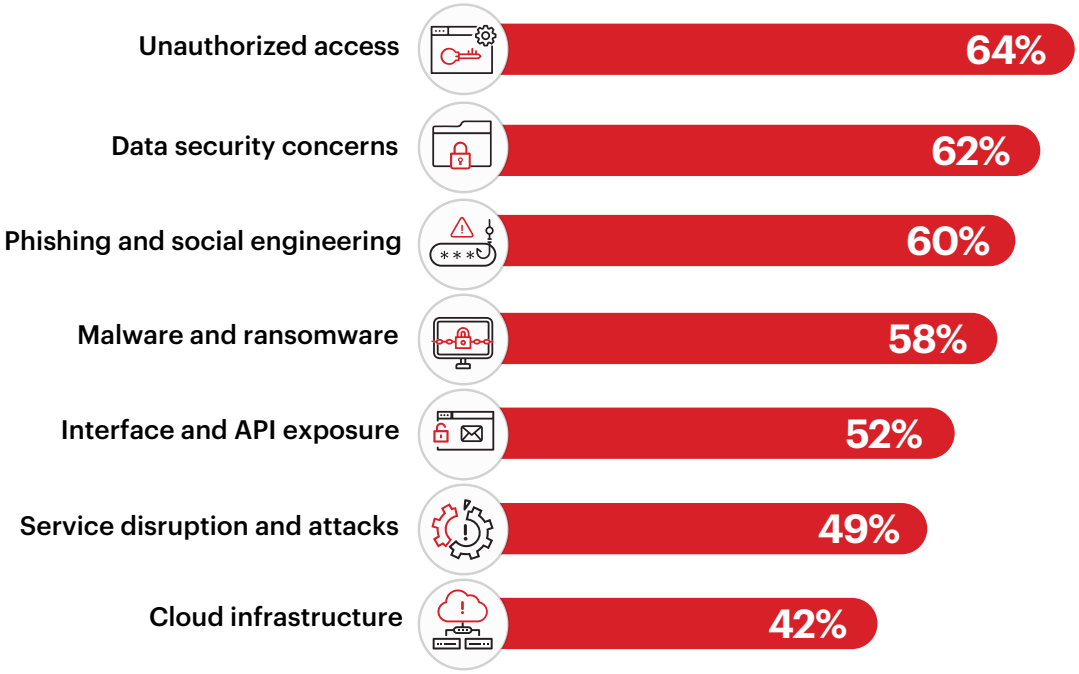
- 64% cite unauthorized access as their top cloud threat, up from 59% last year.
- The number of organizations that consider phishing and social engineering as a top threat jumped from 48% to 60%—a sharp rise in user-targeted compromise.
- Ransomware concern surged to 74%, while zero-days rank second at 63%.
- API exposure (52%) is now a top-tier concern, reinforcing that interfaces—not infrastructure—are the new edge.
- Concerns around provider dependency (41%) and disaster recovery (37%) suggest that while the cloud promises resilience, many still question their ability to control outcomes in the face of disruption.

The Threat Surface Has Shifted

Securing cloud environments means defending not just infrastructure, but identities, data, and workflows—often across loosely coupled platforms. According to respondents, the most urgent threats in the cloud stem from access and exposure: 64% cite unauthorized access as a top concern (up from 59% in the previous year), followed closely by data security (62%, up from 61% in 2024) and phishing or social engineering attacks (60%, up from 48%). These are threats that exploit not misconfigurations or code flaws alone, but identity gaps, user behavior, and weak authentication—making them especially hard to contain in a perimeterless, always-on architecture.

The next tier of concerns includes malware and ransomware (58%, up from 38% in 2024) and API exposure (52%, up from 49%), which reflect the expanded attack surface inherent in multi-cloud and containerized environments. Service disruption (49%, up from 37%) and underlying infrastructure risks (42%) follow closely, while insider threats (39%) and supply chain compromise (37%) round out a layered threat model that touches virtually every surface of the modern cloud stack.

What do you consider the biggest security threats in the cloud?



Let's explore a common configuration where access, data, and interface risks converge: a cloud workload launched with overly permissive IAM policies, exposed via a misconfigured API, and accessible with reused credentials. Without continuous validation of permissions, data flows, and API behavior, each of these risks remains latent until exploited. Defending against this landscape requires cloud-native security controls that are identity-aware, workload-centric, and continuously inspecting traffic and behavior—not just configuration. Focus must shift from chasing every new threat to enforcing consistent policy across users, services, and data wherever they operate.

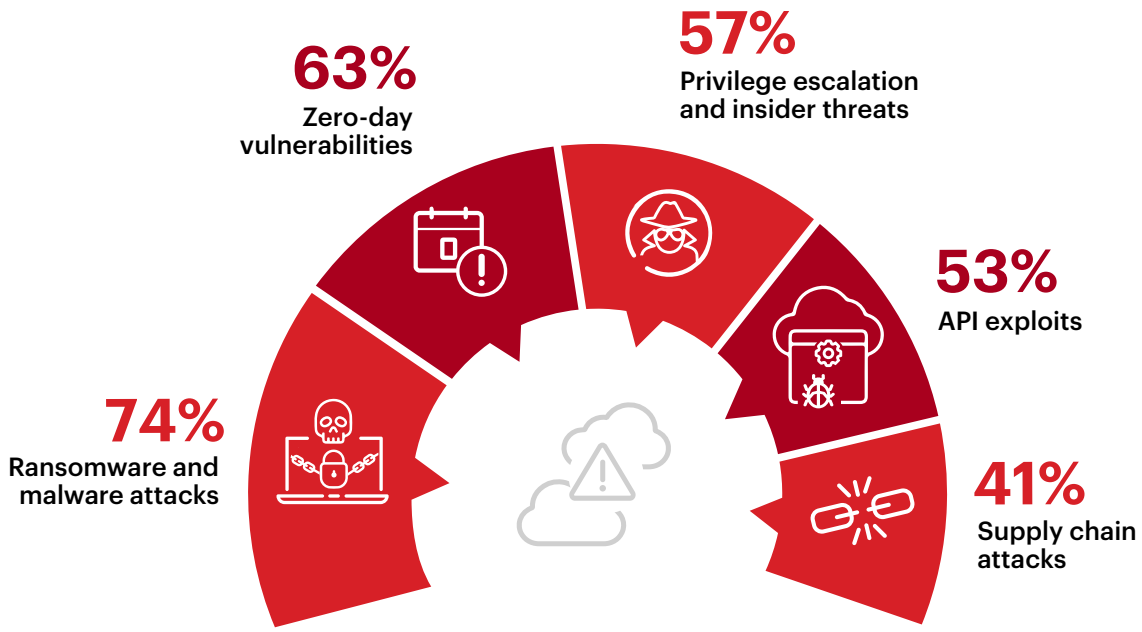
Additional responses: Insider threats (39%) | Supply chain compromise (37%)

The Multi-Cloud Threat Hierarchy

Building on the top-level risks around access and exposure, the data reveals how these broad concerns sharpen into specific, high-impact threats—particularly within the context of increasingly complex multi-cloud environments.

According to our research, ransomware and malware attacks top the list of concerns by a wide margin, with 74% of respondents flagging them as their primary threat vector. Close behind are zero-day vulnerabilities (63%) and privilege escalation or insider threats (57%), each highlighting the dual challenge of defending against both unknown external exploits and trusted-user abuse. API exploits also register strong concern at 53%, confirming that APIs—often the connective tissue of modern cloud architectures—are now viewed as strategic points of exposure.

Which type of advanced threats are you most concerned about in your multi-cloud environment?



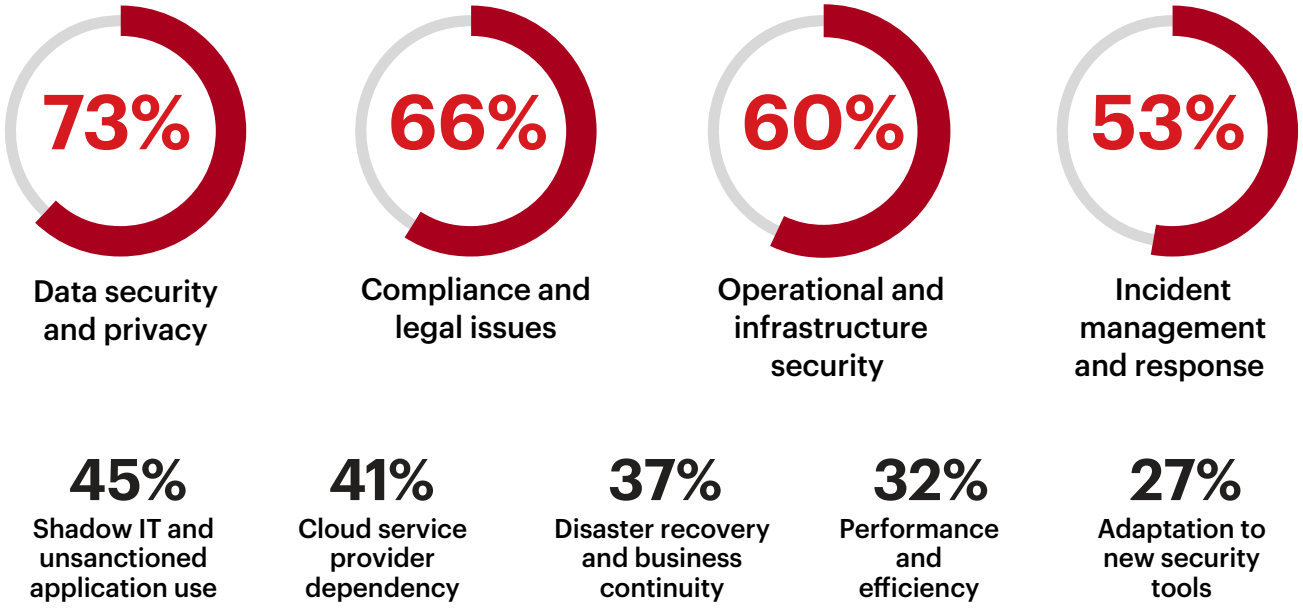
For example, a file-sharing application deployed across multiple regions may integrate with different cloud services and threat detection tools. If a zero-day vulnerability is exploited in a third-party component, inconsistent logging and response baselines can delay containment—letting a minor exploit spiral into a major data loss event.

To respond, security leaders must evolve beyond point solutions and invest in cloud-native platforms that provide continuous visibility into workload behavior, identity usage, and API interactions. Advanced threat detection alone is insufficient without integrated policy enforcement and automated containment strategies tailored for cloud-scale architectures.

Persistent Gaps in Cloud Security

While advanced threats dominate attention, security leaders remain equally concerned with systemic weaknesses that cut across architecture, governance, and operational continuity. Topping the list, 73% of respondents cite data security and privacy as a primary concern—covering everything from data loss to accidental credential exposure. This is followed by compliance and legal issues (66%), indicating that regulatory complexity and data sovereignty continue to weigh heavily on cloud strategy decisions. Operational and infrastructure security (60%) also remains a central concern, revealing ongoing discomfort with visibility gaps, service reliability, and provider transparency. Incident management (53%) and shadow IT (45%) highlight that the cloud's ease of use remains a double-edged sword, enabling agility but often bypassing oversight. Concerns around provider dependency (41%) and disaster recovery (37%) suggest that while the cloud promises resilience, many still question their ability to control outcomes in the face of disruption.

What are your primary concerns regarding cloud security?



A team may discover that a critical storage bucket was exposed for weeks due to inconsistent monitoring across providers. That single visibility gap spans data protection, compliance risk, and operational oversight all at once.

To address these overlapping priorities, cloud security strategies must be anchored in unified data controls, real-time monitoring, and policy enforcement that works across cloud environments, not just within individual environments. Resilience begins with control, and control starts with visibility that is clear, continuous, and actionable.

02

Detection Is Not Defense: Can We Respond Effectively?

Even as threat awareness grows, most organizations still struggle to respond with clarity or speed. This chapter explores where visibility, coordination, and confidence continue to break down and what's helping teams close the gap.

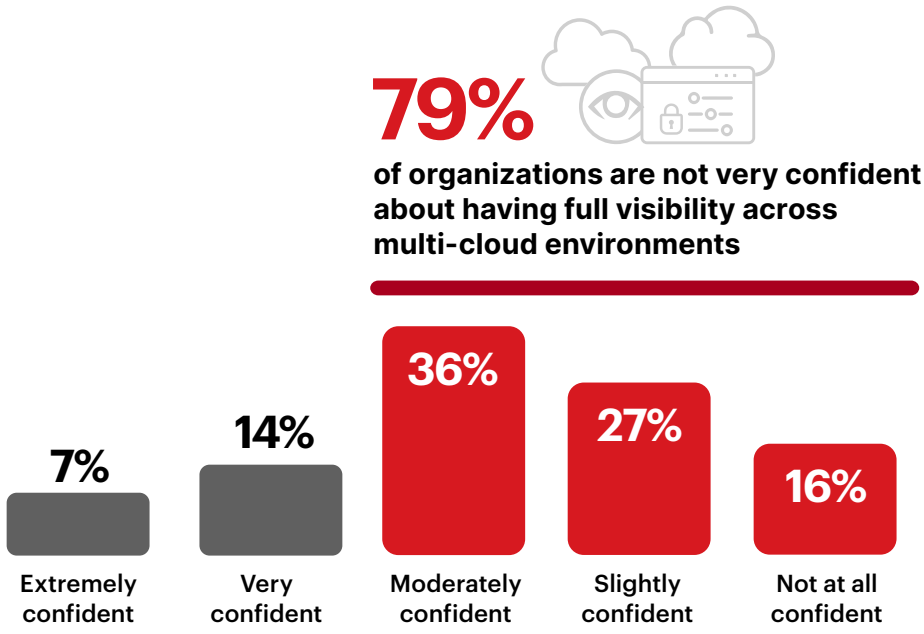
- Only 21% report strong visibility across workloads, configurations, and data flows.
- 34% say root cause analysis is the most time-consuming part of incident response.
- 97% report difficulty executing a unified response plan across multiple cloud providers.
- 75% express only moderate or low confidence in detecting and preventing advanced threats.
- Automation is the top desired improvement, cited by 36%, yet only 52% prioritize it.

Gaps in Cloud Visibility

Beneath the surface of data protection, compliance, and infrastructure concerns lies a more fundamental issue: visibility. Only 21% of cybersecurity professionals in our survey report being very or extremely confident in their visibility across workloads, data flows, and configurations, while a full 79% admit to having, at best, only moderate confidence. This widespread uncertainty reflects an industry grappling with blind spots in environments that are distributed, ephemeral, and constantly evolving.

Without comprehensive visibility, prevention and response both suffer—but it's in incident response where the impact of blind spots becomes most severe. As highlighted in earlier survey results, identifying the root cause of incidents is the most time-consuming part of the response process. That problem becomes intractable without comprehensive, real-time observability into how data moves, how systems are configured, and how workloads behave.

How confident are you that you have full visibility into all workloads, data flows, and configurations across your multi-cloud environment?



In one illustrative scenario, a team investigating a breach finds that critical logs were never captured—or worse, were scattered across consoles with no shared timeline. Triage becomes a guessing game, and recovery stalls before it begins.

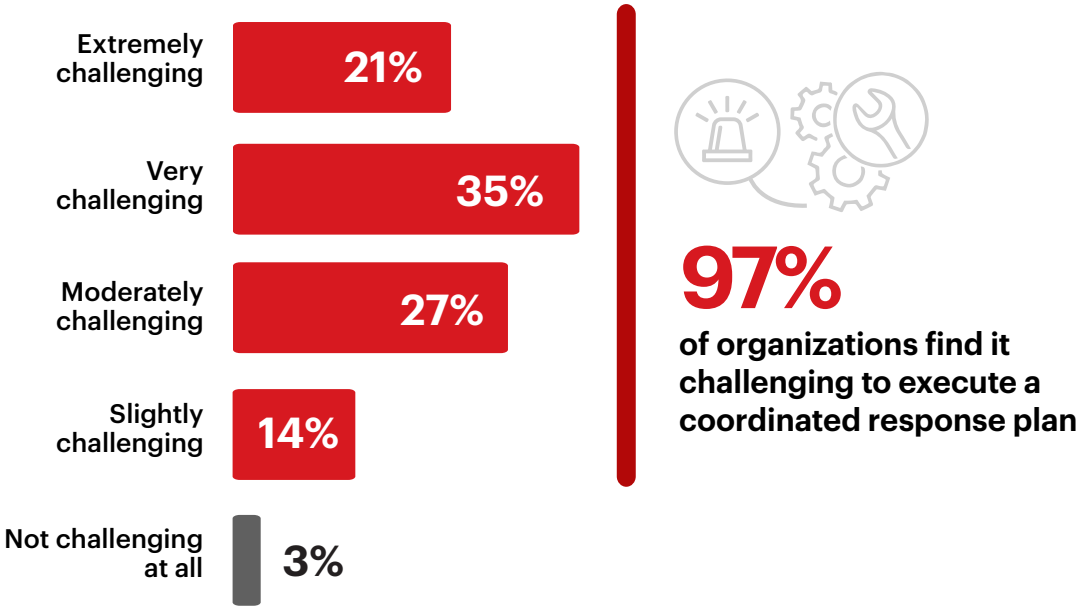
To move beyond this visibility gap, organizations must embrace agentless, API-integrated monitoring solutions that provide continuous, cloud-native insight into workload posture, misconfigurations, and data flows—especially across multi-cloud boundaries. Visualizing the unknown is no longer optional; it's the prerequisite for every control, every detection, and every response that follows.

Unifying Incident Response Across Clouds

Without unified visibility, response becomes fragmented—and nowhere is this fragmentation more evident than in efforts to coordinate incident response across multi-cloud ecosystems. This reality is starkly reflected by the survey results revealing that an overwhelming 97% of cybersecurity leaders find it challenging to implement unified response plans across their multiple cloud providers. This staggering figure underscores the friction created by fragmented tooling, misaligned policy enforcement, and disconnected telemetry.

Such coordination challenges arise from a variety of factors: incompatible vendor toolsets, visibility gaps across platforms, and conflicting compliance or data residency requirements that slow decision making in crisis scenarios.

When a security incident occurs, how challenging is it to execute a coordinated response plan that encompasses all of your cloud environments?



A breach that begins in a SaaS platform may escalate to an IaaS resource within hours. Without unified telemetry and a common response framework, security teams lose precious time aligning logs, coordinating handoffs, and building a timeline from partial signals.

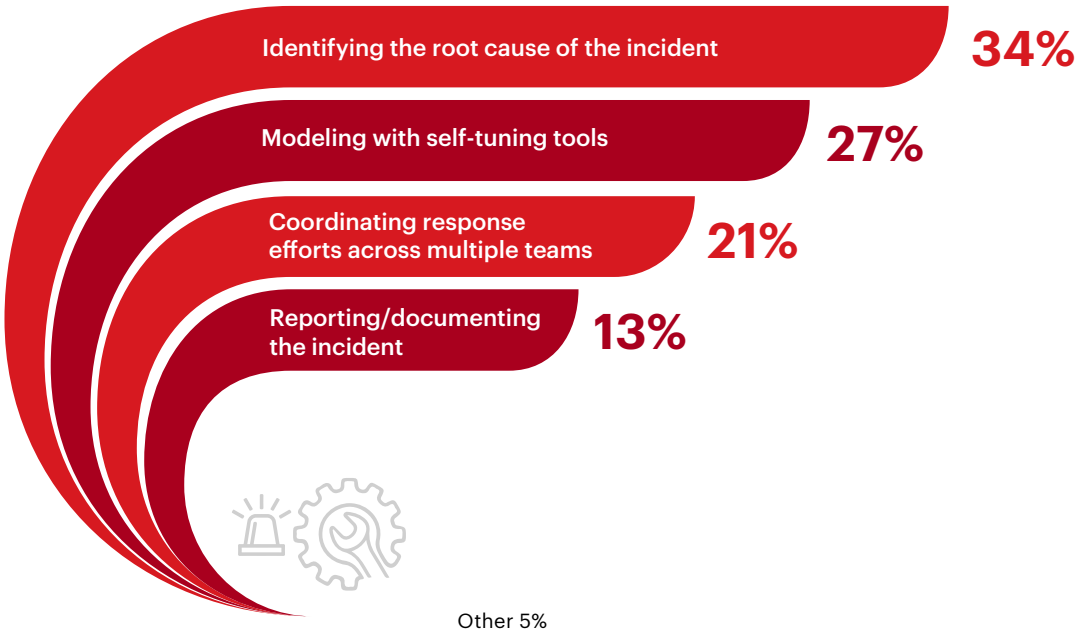
To mitigate these risks, organizations must urgently adopt centralized platforms that unify security telemetry and response orchestration across providers. Equally critical is the regular testing and refinement of incident response playbooks, tailored to today's complex, cloud-native environments. Unified visibility must be matched by unified action.

Root Cause, Real Cost

As earlier responses revealed, more than half of cybersecurity leaders find it very or extremely challenging to coordinate incident response across cloud environments—a problem compounded by limited confidence in detection capabilities. This question adds new dimension to that challenge: 34% say identifying the root cause is the most time-consuming part of incident response, 21% cite coordinating response efforts across multiple team.

Despite growing investment in detection, attribution remains slow and workflows remain fragmented. These delays are intensified in multi-cloud environments, where siloed telemetry, inconsistent log formats, and incompatible detection engines obstruct end-to-end visibility.

What is the most time-consuming aspect of incident response in your multi-cloud environment?



A failed login to a SaaS application may seem routine—until that same identity is later used to access a misconfigured IaaS resource. The threat crosses environments, but the signals don't converge. By the time the pieces are connected, data has already been compromised.

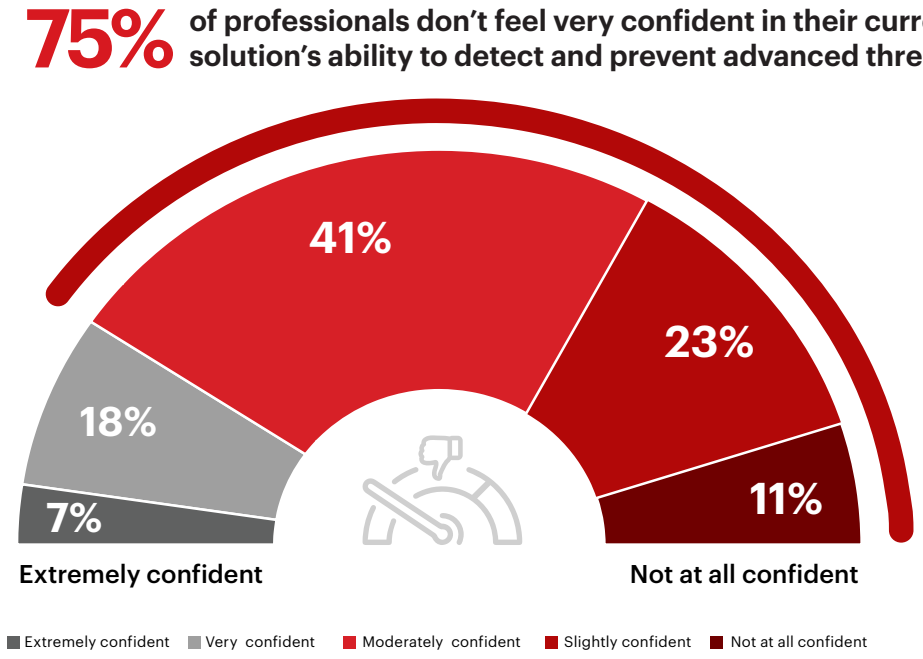
To reduce both time to root cause and friction between response teams, organizations must operationalize centralized telemetry ingestion and real-time correlation across their environments. When combined with runtime context, identity-aware policy enforcement, and shared playbooks, this foundation enables faster triage and a more cohesive response, regardless of where the incident begins.

Confidence Deficit in Cloud Threat Detection

The friction seen in incident response reveals a deeper weakness: limited confidence in detection. According to the data, 75% of security teams are, at best, only moderately confident in their current tools' ability to detect and prevent advanced threats. This confidence gap reflects both architectural complexity and limitations in traditional detection tooling.

In many environments, a misconfigured IAM role may trigger low-priority alerts in one domain, only to be exploited days later in another. Without cross-environment correlation, the warning signs remain fragmented and unresolved.

How confident are you in your current solution's ability to detect and prevent advanced threats (e.g., zero-days, ransomware) across all your cloud environments?



Security teams relying on siloed tools often miss these linkages. What looks like a harmless escalation in one system may in fact be the precursor to malware deployment or credential abuse elsewhere.

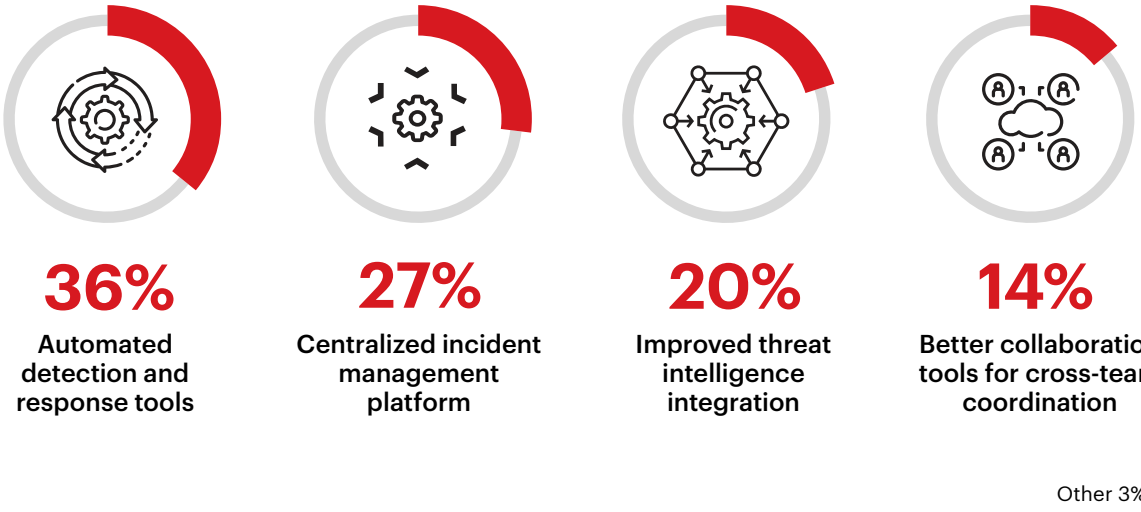
To close this gap, organizations should invest in integrated security platforms that deliver unified visibility, behavior-based detection, and automated containment. These systems must go beyond rule matching by ingesting cloud-native telemetry and enriching detections with threat intelligence and runtime context. The result is faster recognition of what matters and faster decisions on how to act.

Automation as the Force Multiplier

The combined weight of visibility gaps, coordination failures, and detection delays points to a clear bottleneck—one that automation is well-positioned to resolve.

Thirty-six percent of security leaders say automated detection and response would most improve their incident handling, followed by centralized response platforms (27%) and threat intelligence integration (20%). The message is clear: response needs to move faster, and human-only workflows won't scale.

What would improve your organization's incident response capabilities in a multi-cloud environment?



A privilege escalation alert in one cloud may be followed by a lateral movement attempt in another. Without automated correlation and containment, the pieces remain isolated. By the time the response comes together, the attacker has already moved.

Organizations should focus on event-driven automation that operates across cloud environments—triggering containment actions, enforcing policies, and escalating high-risk anomalies without delay. Embedding these capabilities directly into runtime layers, especially for identity and API control, turns detection into immediate defense.

03

Compliance Under Pressure: How to Operationalize It

Compliance has become the real-time audit of your architecture. This chapter reveals how automation, drift detection, and integration gaps are defining success—or failure—in cloud governance.

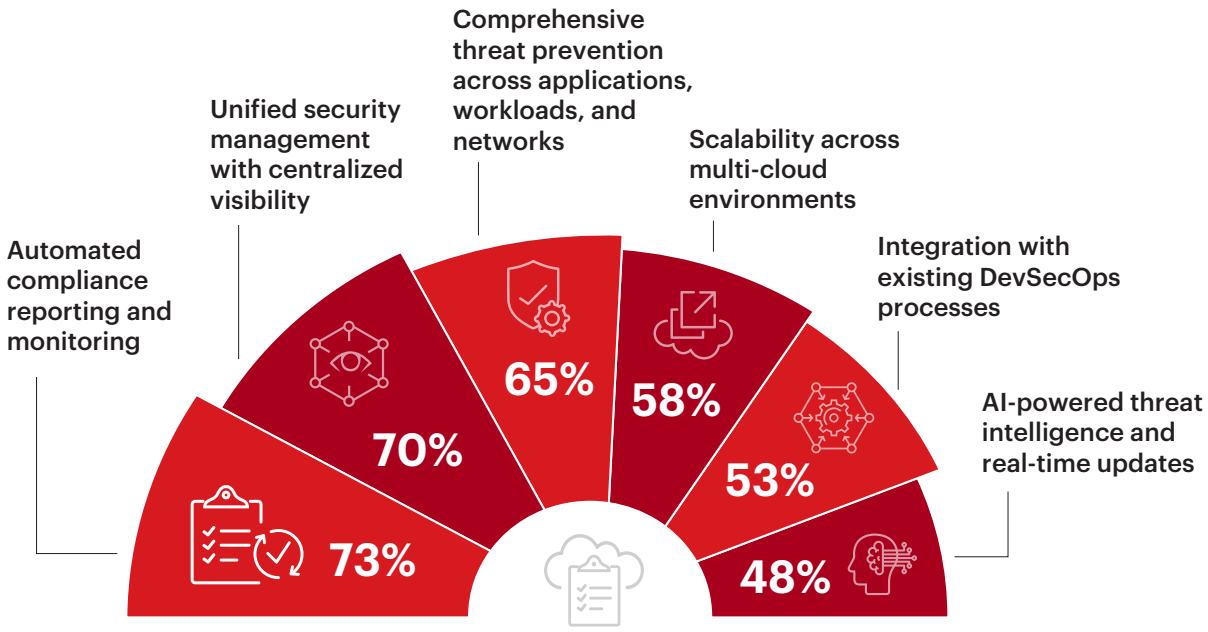
- 73% prioritize automated compliance monitoring as a top requirement.
- 63% cite tool complexity as a primary challenge in managing compliance.
- Only 37% have challenges embedding security controls into CI/CD pipelines.
- 58% say compliance checks remain too manual, despite their shift to cloud-native stacks.
- 55% report inadequate threat detection as a barrier to effective compliance enforcement.

Operationalizing Compliance

With foundational gaps in visibility and control well established, many teams are now turning to compliance not just as a reporting requirement, but as a measure of operational readiness. A dominant 73% prioritize automated compliance reporting and monitoring, closely followed by 70% who value unified security management with centralized visibility. This shift reflects a broader strategy: using compliance automation to embed control into day-to-day operations.

The convergence of priorities for comprehensive threat prevention (65%) and scalable multi-cloud coverage (58%) suggests that compliance is no longer about proving alignment—it's about maintaining it. Preferences for DevSecOps integration (53%) and AI-powered threat intelligence (48%) reinforce the move toward speed, automation, and enforcement that can keep pace with infrastructure changes.

Which features do you prioritize when selecting a cloud security solution to ensure compliance?



Imagine a security team racing to prepare audit evidence across four cloud providers, each with different visibility, logging, and policy enforcement standards. Without centralized mapping to frameworks and real-time drift detection, compliance becomes reactive, incomplete, and high risk.

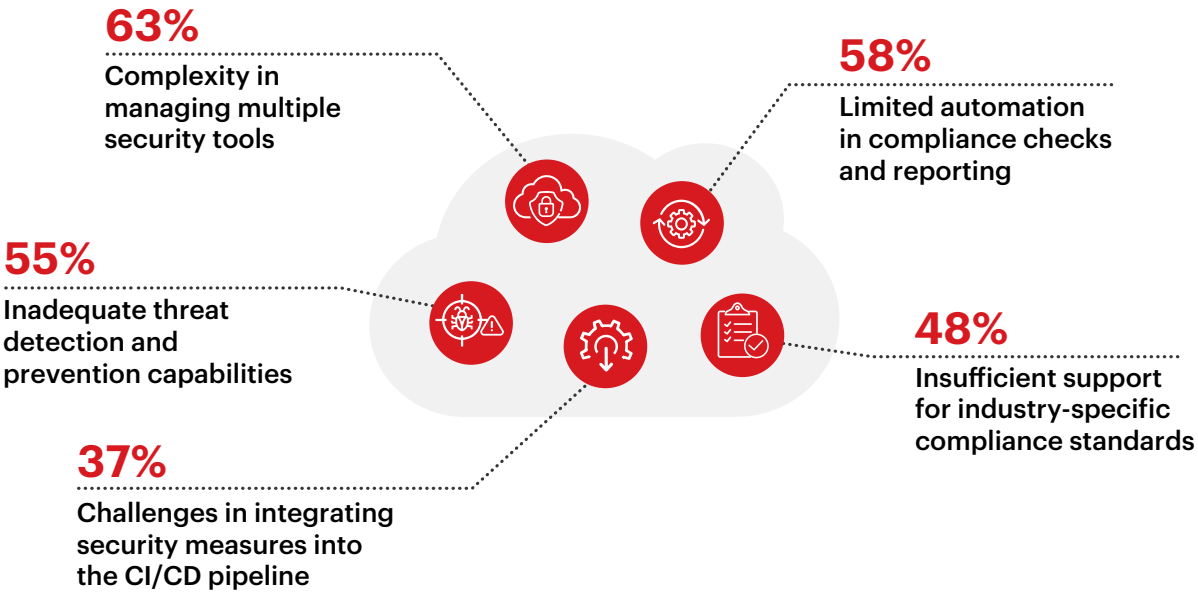
To meet modern cloud compliance expectations, teams must shift from periodic inspection to continuous enforcement. That means automating reporting, validating configuration against policy in real time, and surfacing violations before they trigger incidents or audits. When treated as a live system, compliance becomes a force for resilience—not just a checkbox.

Why Cloud Compliance Stalls

Despite strong recognition of compliance automation's value, practical implementation stalls when teams confront fragmented tools, legacy workflows, and integration barriers—issues that often only surface during high-pressure audits or incidents. The top complaint, cited by 63%, is the complexity of managing multiple security tools. Another 58% point to limited automation in compliance checks, while 37% highlight persistent friction when embedding controls into DevOps pipelines. The result is a compliance process that remains brittle, delayed, and vulnerable to drift.

Inadequate threat detection (55%) and weak support for industry-specific standards (48%) show that many solutions stop at surface-level enforcement, leaving deeper regulatory alignment unresolved.

What pain points are you experiencing with your current cloud security solutions regarding compliance?



A new service deployed in AWS might pass basic scans but trigger a compliance violation weeks later when access policies drift. Without real-time enforcement or CI/CD guardrails, teams discover these issues too late—often during an audit or after a breach.

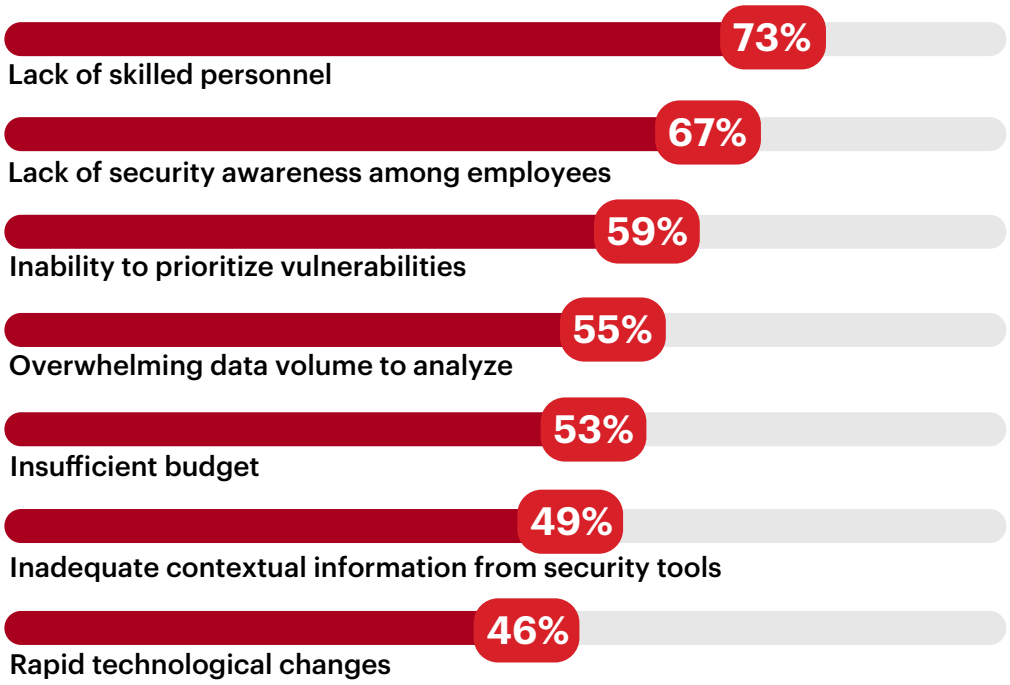
To move forward, organizations must consolidate compliance and security into a shared platform. That means adopting solutions that support compliance-as-code, offer prebuilt mappings to key frameworks, and dynamically enforce policy throughout the deployment lifecycle. Simplification isn't just operational, it's strategic.

Human Limits to Cloud Defense

Behind many of the issues discussed—compliance gaps, delayed response, alert fatigue—lies a deeper constraint: human capacity. The top barriers to adequate cloud defense are overwhelmingly organizational: 73% cite lack of skilled personnel and 67% point to low security awareness among employees. These aren't technology failures—they're structural limitations that weaken security from the inside out.

Closely following are difficulty prioritizing vulnerabilities (59%) and data overload (55%), signaling that even well-staffed teams are often overwhelmed by fragmented signals and unclear risk. Budget limitations (53%) and tool integration challenges (38%) further compound the issue, breaking visibility and slowing response.

What barriers inhibit your organization from adequately defending against cyberthreats?



Picture a security team juggling ten consoles, hundreds of alerts per hour, and no shared scoring or playbooks to prioritize action. The result isn't just burnout, it's breach exposure.

To overcome these limitations, organizations must focus on operationalizing defense. That means prioritizing automation that extends human capacity, investing in integration over point tools, and enriching alerts with contextual insight that reduces noise. Success in cloud defense no longer depends on throwing more people at the problem—it depends on building systems that help those people move faster, with greater certainty.

Additional responses: Difficulty justifying additional investment (41%) | Poor integration and interoperability between security solutions (38%)

04

Strategic Priorities: Security Is Shifting from Tools to Intelligence

In 2025, security priorities reflect a clear shift from stacking point tools to designing integrated systems that can scale, adapt, and act with speed. Identity, data, visibility, and automation remain at the core, but AI is now becoming the connective tissue between them, driving detection, triage, and response in real time. The best-performing teams are no longer just setting priorities, they're operationalizing them through platforms that adapt, automate, and act.

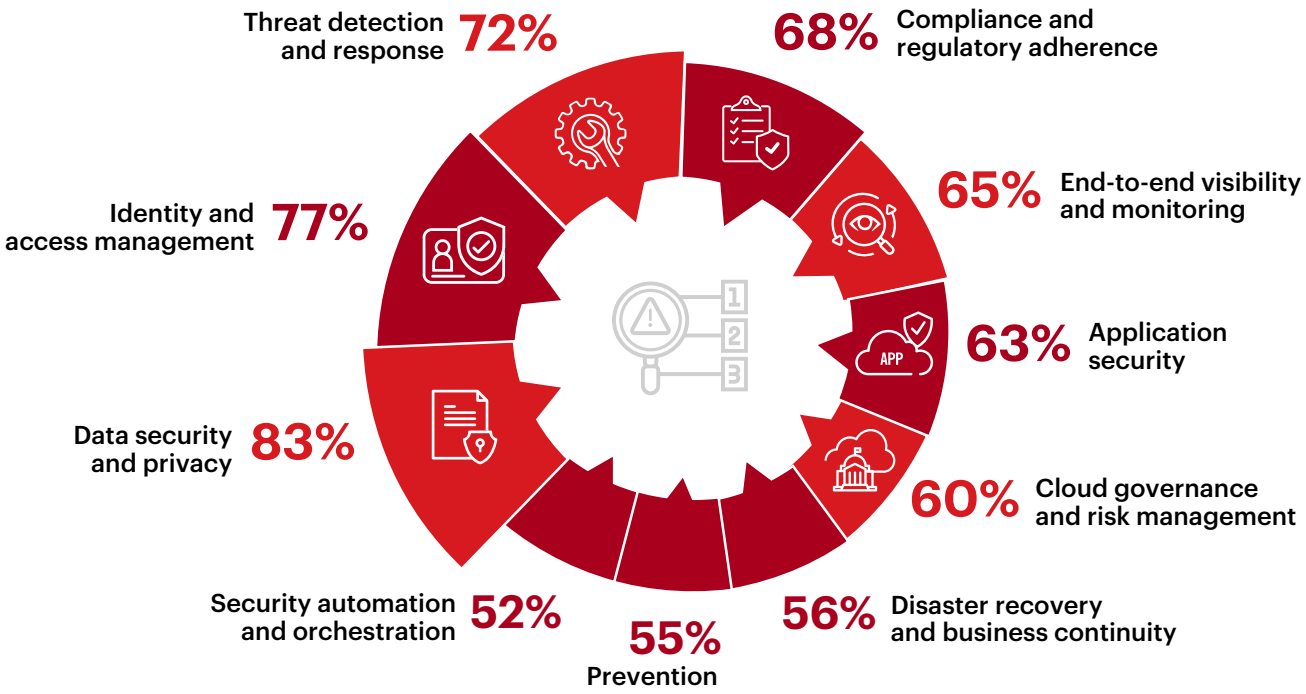
- Data security (83%) and identity and access management (77%) top all cloud security priorities.
- Threat detection and response ranks high at 72%, but only 52% prioritize orchestration—exposing a strategy–execution gap.
- 75% consider AI for threat detection most valuable; 70% value anomaly detection; and 62% value automated respons.
- Explainable AI (66%) is the top-ranked technique, showing demand for clarity and trust in machine-led decisions.
- AI is valued most not for its novelty, but for speed, precision, and its ability to scale human capacity across complex environments.

Cloud Security Priorities: Data, Identity & Control

Against a backdrop of operational friction and growing regulatory pressure, the data shows where security leaders are focusing and how priorities are shifting from reactive measures to foundational control. At the top, 83% of respondents prioritize data security and privacy (up from 75% in 2024), followed closely by identity and access management (77%, up from 63%) and threat detection and response (72%, up from 61%). This convergence reflects a clear evolution: protecting what matters most, controlling who gets near it, and catching anything that slips through.

Trailing just behind are compliance (68%), end-to-end visibility (65%), and application security (63%), reinforcing that cloud security is no longer an operational add-on. It's becoming architectural—designed into systems, not layered on top. Yet only 52% of organizations currently prioritize automation and orchestration, revealing a continued lag between visibility and action.

What are your top cloud security priorities?



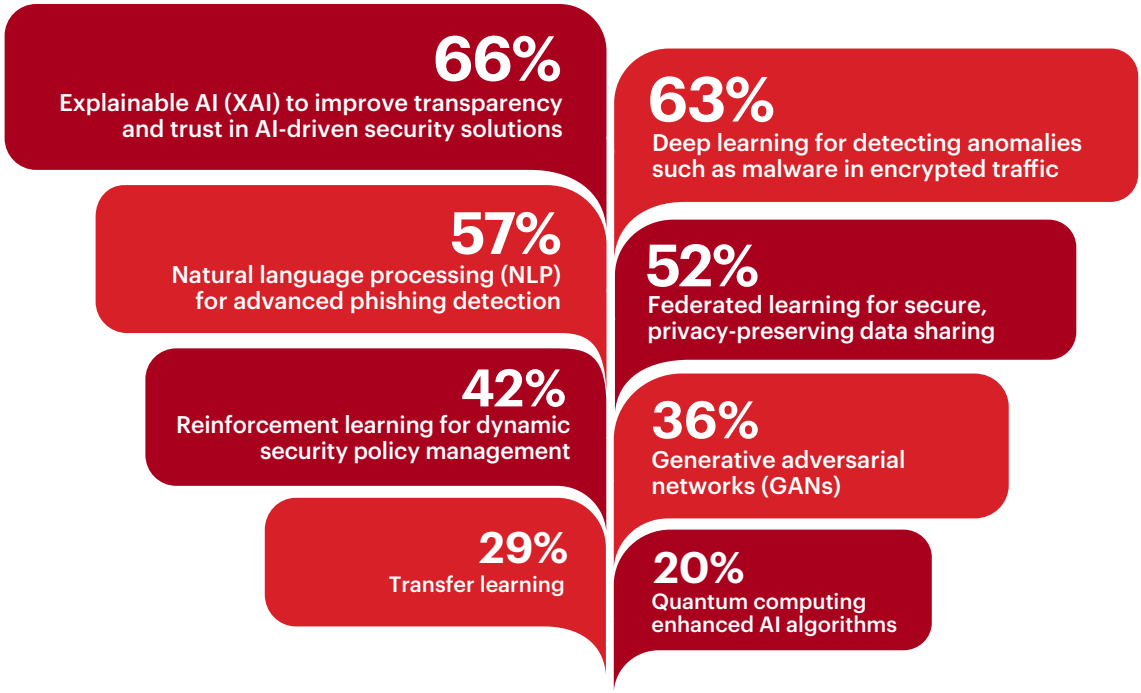
In a dynamic cloud environment, identities may shift by the hour, workloads may scale up or down across regions, and sensitive data may traverse services without triggering alerts. Without continuous identity enforcement and live telemetry, these blind spots persist—and risk compounds. To stay ahead, organizations must treat cloud security as a system of control, not a collection of tools. Identity, data, and detection need to operate in concert, driven by automation, supported by platform integration, and adaptable to the pace of cloud infrastructure. Priorities are no longer just strategic, they're operational mandates.

AI Priorities for Cloud Defense

To effectively combat today's sophisticated threats, security teams are rapidly turning to AI. However, the effectiveness of AI solutions depends on clearly aligning them with practical security priorities. The following AI and machine-learning techniques have emerged as the most promising for addressing specific, real-world cloud security challenges. At the top of the list, 66% of respondents see promise in explainable AI (XAI), reflecting a growing demand not just for smarter detection, but for models that can be understood, audited, and trusted—especially as AI begins influencing automated response.

Deep learning for anomaly detection (63%) reflects the growing need to surface threats hidden in noisy, encrypted environments where traditional rules fall short. Natural language processing (57%) and federated learning (52%) reflect more specialized priorities such as detecting phishing by understanding attacker language patterns, or enabling secure, privacy-preserving data collaboration across platforms. Lower on the list but still noteworthy are reinforcement learning (42%) and GANs for threat simulation (36%), signaling interest in more adaptive, proactive defenses.

Which emerging AI and ML techniques do you believe hold the most promise for enhancing cybersecurity defenses?



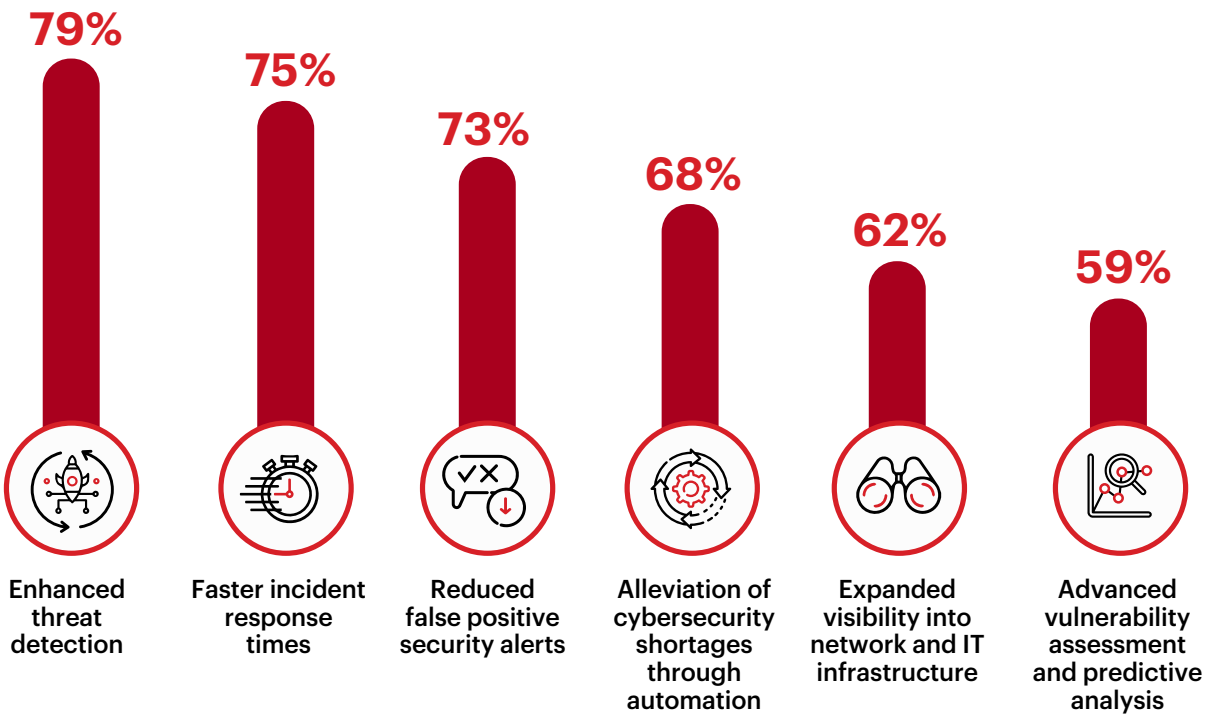
Consider a phishing email that mimics a CEO's tone and cadence. Without NLP-based AI tuned to detect language manipulation, the system sees just another message. But with explainable detection layered in, the anomaly is flagged and the SOC knows exactly why. To deploy AI securely and effectively, organizations should focus first on techniques that strengthen core workflows: detection, enrichment, correlation, and response. Transparency, context, and adaptability—not black-box automation—will define the next generation of cloud defense.

AI's Value in Security Operations

AI's appeal becomes clearer when viewed through the lens of modern cloud security demands: speed, scale, and fatigue. Security teams aren't chasing AI for novelty—they're turning to it to amplify their reach, reduce noise, and act faster under pressure. Top benefits cited include enhanced threat detection (79%), faster incident response (75%), and reduced false positives (73%), confirming that AI's value lies in turning volume into clarity and action.

Close behind is automation's ability to offset cybersecurity talent shortages (68%)—a constraint echoed throughout the survey. Other benefits include expanded visibility (62%) and predictive analysis (59%), showing that AI isn't just reactive. When used well, it helps teams anticipate and outmaneuver threats before they escalate. Picture a SOC overwhelmed by tens of thousands of daily events. Instead of sorting alerts manually, AI narrows the field to the handful tied to suspicious behavior, correlates them across identities and workloads, and initiates response workflows—all before an analyst logs in.

What do you see as the most significant benefits of incorporating AI into cybersecurity operations?



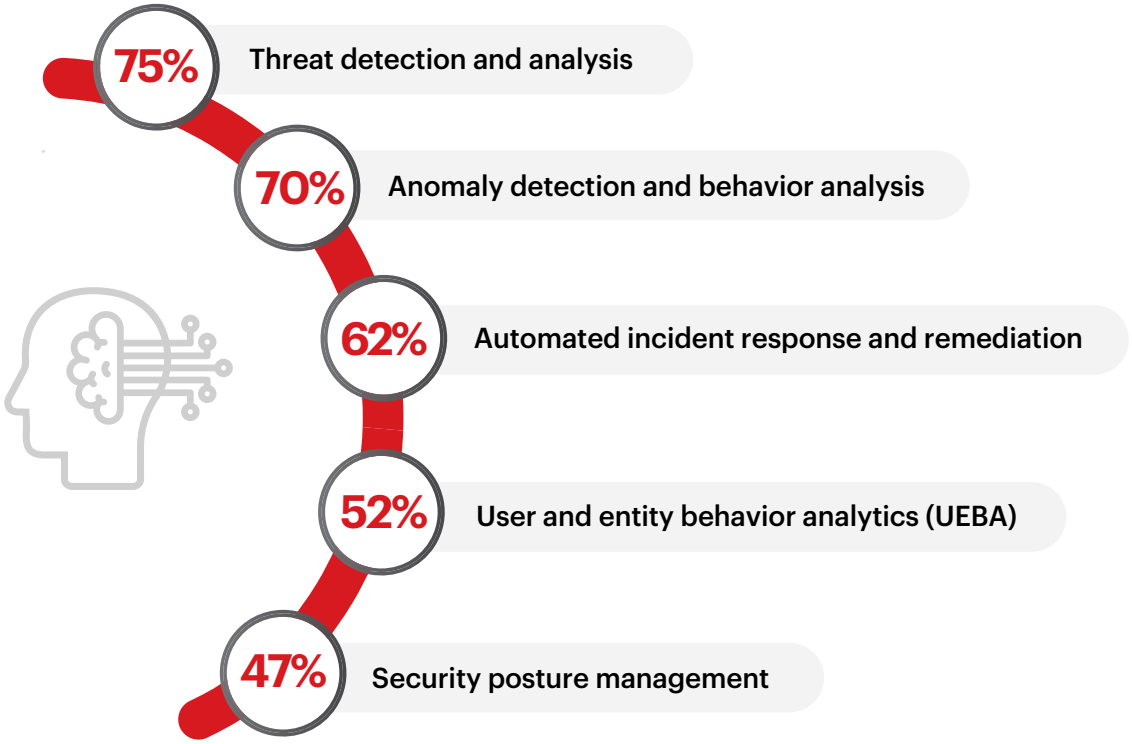
To realize this value at scale, organizations should embed AI into the operational core: telemetry pipelines, correlation engines, and response orchestration. That's where AI turns insight into speed—and speed into security.

AI: From Insight to Intervention

With the strategic promise of AI clearly defined, attention now turns to where it's delivering operational results. Leading the list are threat detection and analysis (75%, up from 71% in 2024), followed closely by anomaly detection and behavior analysis (70%, up from 54%). These priorities reflect growing reliance on AI not just to see threats, but to understand them in real time.

Automated response and remediation (62%, up from 61%) also ranks high, highlighting a shift toward AI not just as a detection engine, but as a response layer. Meanwhile, user and entity behavior analytics (52%) and security posture management (47%) round out the list, reflecting broader interest in AI systems that improve context and reduce exposure over time.

Which AI-driven cloud security features do you consider most valuable?



Imagine a cloud workload that begins communicating in unusual ways late at night, following a recent IAM change. An AI engine flags the anomaly, ties it to behavioral drift, and launches a targeted response—all before human review is required.

To fully capitalize on these capabilities, organizations should focus on integrating AI into the telemetry stream and decision logic, not as an overlay, but as a system-level function. When used with precision, AI becomes more than an insight engine—it becomes the speed layer in cloud defense.

Cloud Security Best Practices for 2025

The best practices outlined here distill the report's findings into actionable strategies. They directly address the top challenges identified by our survey—visibility gaps, fragmented detection and response, compliance friction, and operational overload. Each practice is not only recommended, it's essential for effective cloud security in 2025.

1. **Enforce identity continuously:** Access control shouldn't stop at login. In cloud environments where identities and permissions shift constantly, real-time enforcement is essential. Implement contextual access policies and revoke unused privileges automatically. With 77% prioritizing IAM, it's clear this is now a frontline control, not a background function.

2. **Automate high-risk response paths:** Manual response can't keep up with threats like lateral movement or API abuse. Automate detection-to-containment workflows where speed matters most, especially for identity and runtime threats. Thirty-six percent of leaders say automation would have the greatest impact on incident response—underscoring where the industry sees the greatest opportunity for impact.

3. **Unify visibility across your cloud footprint:** Fragmented telemetry makes root cause analysis slow and incomplete. Centralize observability across clouds using API-driven tools that track workload behavior, data flows, and configurations. Only 21% of organizations report strong visibility—a persistent foundation weakness.

4. **Make compliance continuous:** Periodic checks no longer cut it. Embed policy enforcement into DevOps workflows and trigger real-time alerts on misconfigurations and drift. With 73% prioritizing automated compliance monitoring, it's time to treat compliance as a live system, not a scheduled task.

5. **Reduce tool sprawl**: Disconnected tools create gaps and delay response. Consolidate around platforms that integrate detection, policy enforcement, and remediation across your cloud stack. Sixty-three percent of respondents cite tool complexity as a major barrier—it's not just about cost, it's about control.

6. **Use AI where it drives action:** AI should clarify, not complicate. Focus on high-value use cases like anomaly detection, signal enrichment, and automated remediation. With 75% citing AI for threat detection and 62% for response, the value is no longer hypothetical—it's operational.

Closing Summary

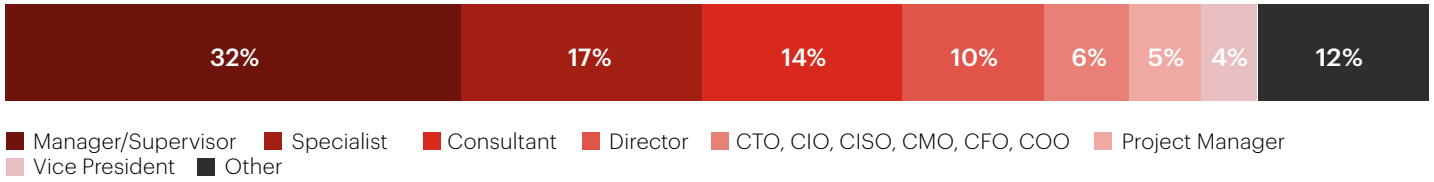
Cloud security in 2025 is no longer defined by how quickly teams detect threats—it's defined by how fast they can act. The data in this report reflects a clear evolution away from reactive, tool-heavy architectures toward integrated, adaptive systems that operate at cloud speed.

Methodology and Demographics

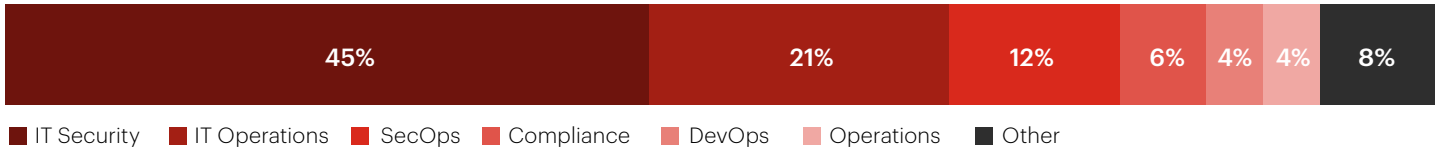
The 2025 Cloud Security Report is based on an online survey conducted in early 2025, gathering responses from 512 cybersecurity professionals across Europe. Participants included CISOs, security directors, architects, analysts, and IT leaders from diverse sectors such as technology, financial services, healthcare, manufacturing, government, and professional services.

A stratified sampling approach ensured balanced representation, achieving a 95% confidence level with a ±4.1% margin of error. Some questions allowed respondents to "select all that apply," resulting in percentages exceeding 100%. This methodology provides a comprehensive snapshot of cloud security challenges, strategies, and emerging AI-driven trends.

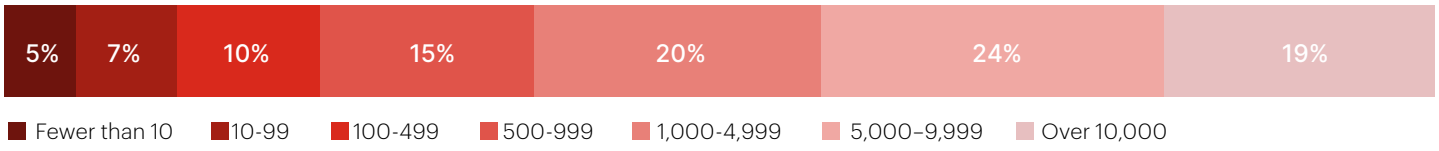
CAREER LEVEL



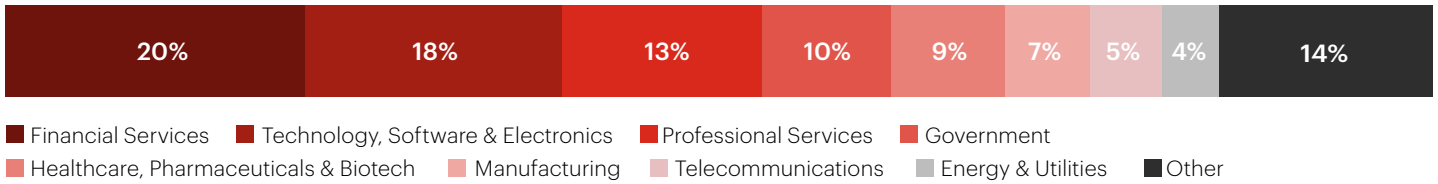
DEPARTMENT



COMPANY SIZE



INDUSTRY



At Trend Micro, we believe cloud security must evolve as fast as the threats it faces. That's why we've reimagined protection for the modern enterprise—uniting cloud, SecOps, and AI into a single, adaptive platform.

Trend Vision One™ Cloud Security delivers continuous visibility, real-time detection, and automated response across multicloud, on-premises, and hybrid environments. Whether you're scaling DevOps, navigating compliance, or defending against advanced threats, we help you move faster, act smarter, and stay resilient.

As a global cybersecurity leader, our platform, threat intelligence, and services are deployed by over 500,000 enterprise customers across 175 countries and recognized by third-party reviewers and industry analysts.

www.trendmicro.com

Cybersecurity
INSIDERS

STRATEGIC INSIGHT FOR CYBERSECURITY LEADERS

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,
- Thought leadership 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