FORTINET

2026

Cloud Security Report

Closing the Cloud Complexity Gap

Research by

Cybersecurity INSIDERS

Executive Summary

Cloud is a critical component of the modern enterprise and even more so as organizations look to drive their future with AI. While this strategy enables business speed and agility, it has expanded the attack surface faster than traditional security models can protect it.

Based on a comprehensive survey of 1,163 senior cybersecurity leaders and practitioners worldwide, the data reveals a widening cloud complexity gap: a structural mismatch between the velocity of modern cloud environments and security teams' ability to maintain consistent visibility, detection, and response in real time. This gap is not driven by a lack of investment. Budgets are rising, yet maturity lags. The data suggests the problem is more fundamental, driven by three reinforcing factors:

- **Fragmented defenses:** As cloud adoption expands, security tooling proliferates alongside it, often without coordination. Disconnected tools, inconsistent controls, and siloed telemetry limit end-to-end visibility and force teams to manually correlate alerts across systems that were never designed to integrate. Consequently, 69% of organizations cite tool sprawl and visibility gaps as their top barrier to effective cloud security, with exposure increasingly emerging across identity, configuration, SaaS, and data domains rather than within any single control.
- **Stretched teams:** Persistent talent shortages amplify this fragmentation. Overextended teams rely on alert-driven workflows that slow response and increase the likelihood of missed signals. For instance 74% report an active shortage of qualified cybersecurity professionals, and 59% remain in early stages of cloud security maturity.
- **Adversaries operating at machine speed:** Attackers now use automation and AI to discover misconfigurations, map permission paths, and identify exposed data faster than human-led defenses can respond. As the window between exposure and exploitation compresses, 66% of organizations lack strong confidence in their ability to detect and respond to cloud threats in real time.

The findings increasingly point toward integrated frameworks, interoperable security approaches that consolidate visibility and enable automation grounded in shared context. This approach reduces operational friction and the risk of disruption, data compromise, and regulatory exposure. The remainder of this report explores how organizations are responding to close the cloud complexity gap.

The Multi-Cloud Reality: Complexity is the New Standard

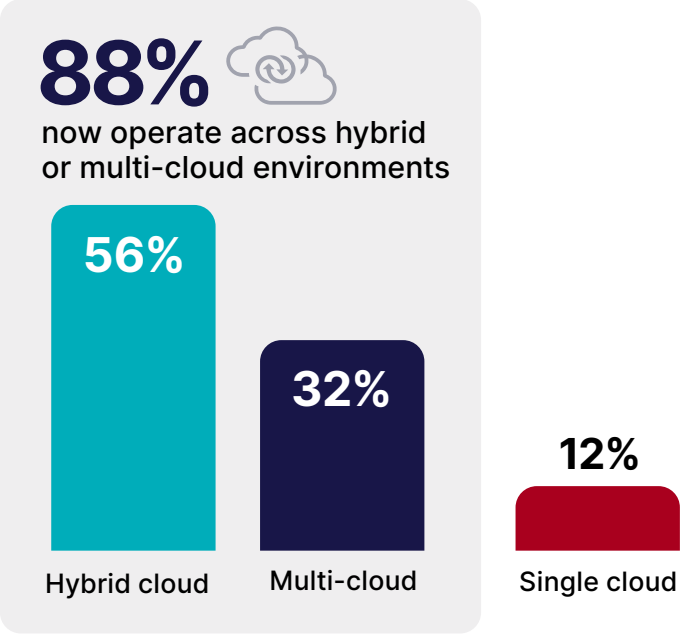
Cloud environments are no longer built around a single provider or a clear boundary. For most organizations, cloud computing now spans multiple public cloud platforms, on-premises infrastructure, Software-as-a-Service (SaaS) applications, and distributed users and devices. This hybrid, multi-cloud model is no longer an intermediate stage: it is the de facto operating model for the enterprise.

The survey confirms this reality. Eighty-eight percent of organizations now operate across hybrid or multi-cloud environments (up from 82% last year). Of these, 81% rely on two or more cloud providers to run critical workloads (up from 78% last year), while 29% report using more than three. These environments typically evolve over time through modernization efforts and business-driven expansion across teams and regions.

Hybrid and Multi-Cloud Architectures Are Now the Norm

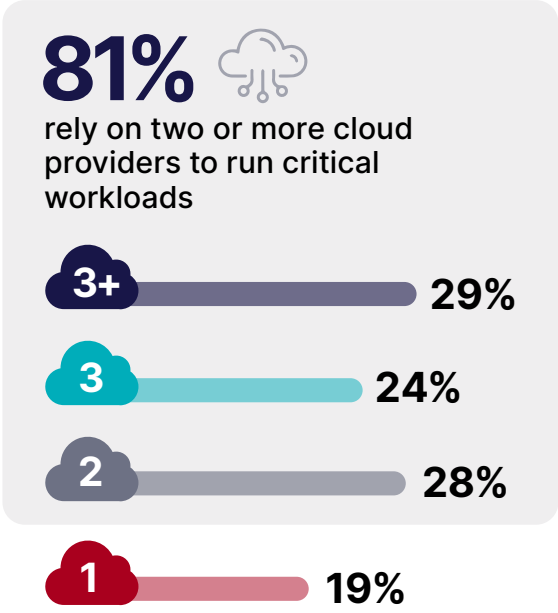
What is your organization's primary strategy for cloud deployment?

Up from 82% in last year's survey



How many cloud providers does your organization currently use?

Up from 78% in last year's survey



As cloud environments grow, the attack surface expands proportionally. Every new provider, service, or identity adds configurations, permissions, and data paths. Assets change constantly, non-human identities multiply, and sensitive data moves across services and regions as part of normal operations. While cloud infrastructure scales automatically, the entire ecosystem becomes increasingly complex to understand.

This multi-cloud reality creates structural complexity across clouds, networks, and applications. It is the environment security teams are now expected to secure by design – and it sets the foundation for the visibility, confidence, and operational challenges explored in the pages that follow.

The Fragmenting Attack Surface

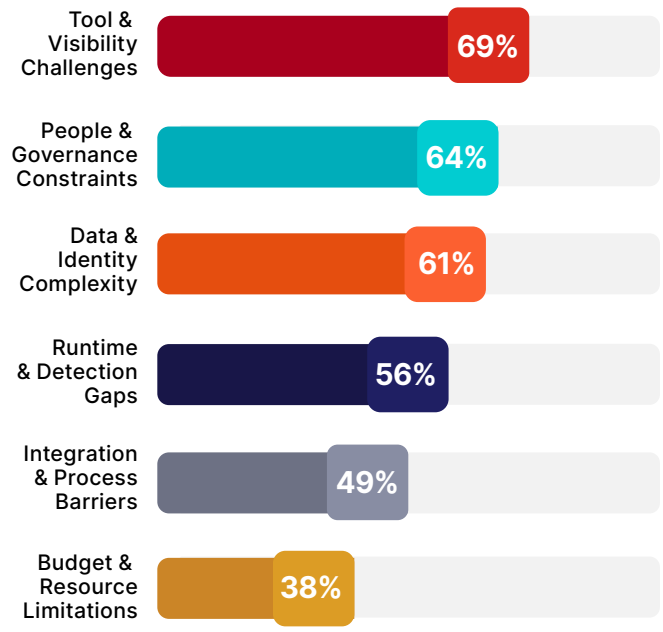
As cloud environments scale, the attack surface does more than expand - it fragments. New cloud accounts, workloads, identities, applications, and data stores are created continuously, often through automated processes and developer-driven workflows. These changes occur across cloud environments that operate independently, leaving security teams to manage exposure that shifts faster than centralized oversight can follow.

Fragmentation has become the most significant operational barrier to effective cloud security. Sixty-nine percent of organizations cite tool sprawl and visibility gaps as the top factor limiting cloud security effectiveness. Instead of reducing risk, security teams spend more time navigating multiple consoles and manually correlating alerts across disconnected systems than remediating threats.

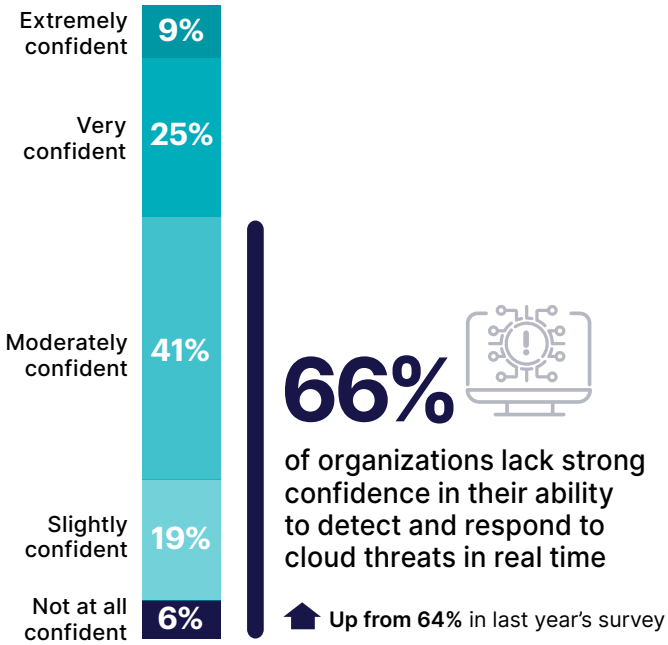
The survey shows that this fragmentation directly undermines confidence. Sixty-six percent of organizations lack strong confidence in their ability to detect and respond to cloud threats in real time – up from 64% last year. This gap highlights a fundamental structural challenge: architectural scale is increasing faster than the security team's ability to maintain situational awareness.

Cloud Complexity Has Outpaced Detection Confidence

What are the biggest challenges currently limiting your organization's cloud security effectiveness?



How confident are you in your organization's ability to detect and respond to threats across all cloud environments in real time?



Multi-cloud environments amplify the problem. With most organizations managing two or more cloud providers, visibility is often split across separate control planes, identity systems, and telemetry sources. Security teams are left to piece together risk signals manually and, after the fact, across environments that were never designed to integrate. This is where complexity becomes operational risk, and where the cloud complexity gap begins to materially affect detection, response, and outcomes. As environments grow more complex, the cost of fragmentation compounds—adding operational friction to teams already operating at capacity.

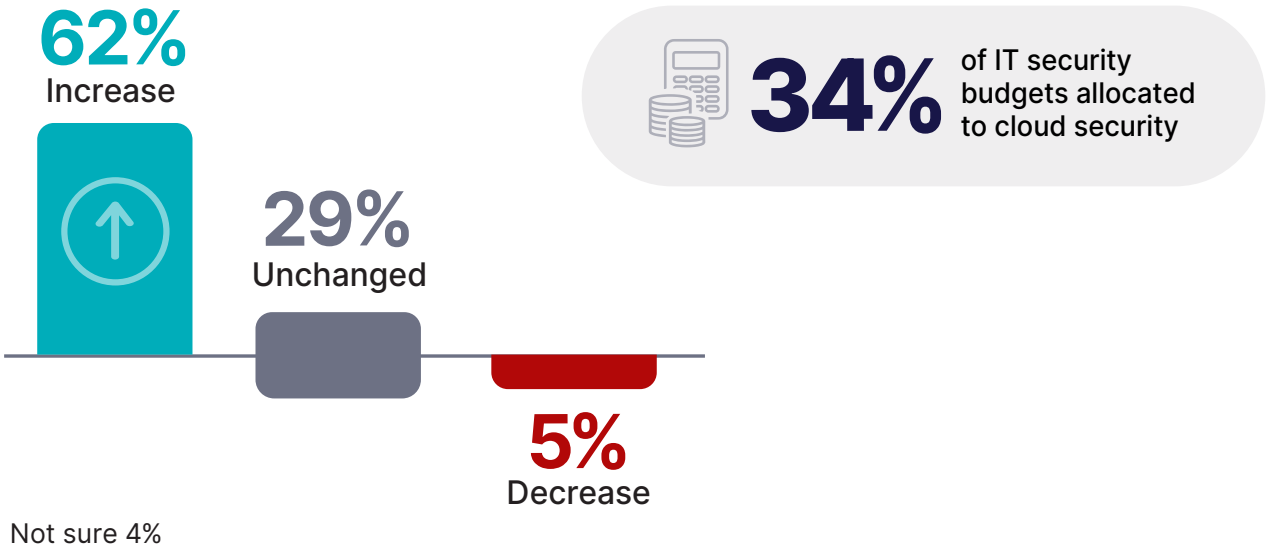
The Budget-Maturity Gap

Cloud security investment continues to grow, yet maturity has not advanced at the same pace. The survey shows that 62% of organizations expect their cloud security budgets to increase over the next 12 months; on average, cloud security now accounts for 34% of total IT security spending, reflecting the cloud's central role in enterprise operations.

However, increased spending does not always translate into improved confidence or maturity. The data shows that despite rising budgets, 59% of organizations still rate their cloud security posture at initial or developing stages—the two lowest tiers on a five-stage scale. This indicates that maturity gains lag behind investment growth.

Cloud Security Spend Is Rising, But Maturity Lags

How is your cloud security budget changing in the next 12 months, and what percentage of your IT security budget is allocated to cloud security?



Each new tool adds complexity including integration work, console management, and additional decision fatigue for already-stretched teams. Returns diminish when the underlying architecture requires manual correlation across systems that lack shared context. As investment grows, much of it is absorbed by the added operational tax of managing disconnected tools rather than by measurable improvements in security outcomes.

This pattern does not imply overinvestment. Instead, it indicates that funding alone cannot close the gap when visibility, coordination, and architectural integration remain constrained.

Complexity Outpaces Talent

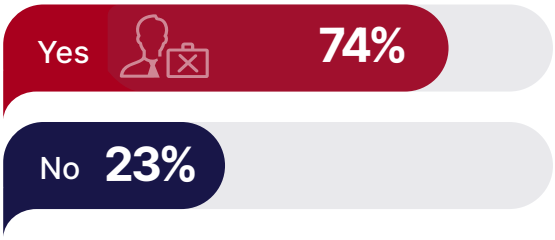
The effects of operational complexity are compounded by a persistent shortage of skilled cybersecurity professionals. The survey reveals that 74% of organizations report an active shortage of cybersecurity talent, and 77% express high concern about the industry-wide skills gap. These shortages are especially acute in cloud-specific roles, where expertise must encompass infrastructure, identity, data, and application layers.

This shortage amplifies the fragmentation problem. Disconnected tools generate a volume of alerts that exceeds the capacity of understaffed teams. Analysts are forced to expend critical hours manually correlating data across consoles—time that should be spent on higher-value analysis. Policies drift—requiring tuning across multiple platforms—and the operational burden grows while the workforce remains stagnant.

This necessitates a reactive stance. Overextended teams default to alert-driven workflows, triaging what they can and accepting that some signals will be missed. Proactive threat hunting, architecture improvement, and automation refinement are deprioritized due to a lack of capacity.

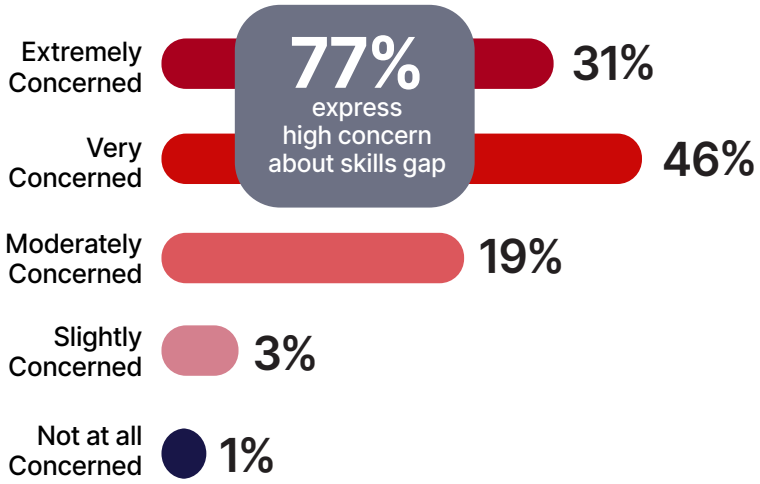
Cybersecurity Talent Shortages Are a Persistent Constraint

Is your organization experiencing a shortage in cybersecurity talent?



Not sure 3%

How concerned are you about the industry-wide skills shortage of qualified cybersecurity professionals?



Hiring alone cannot close this gap. Even organizations that successfully recruit face lengthy onboarding cycles while cloud environments evolve daily. Manual processes simply cannot scale to keep pace with environments that expand continuously and adversaries operating at machine speed.

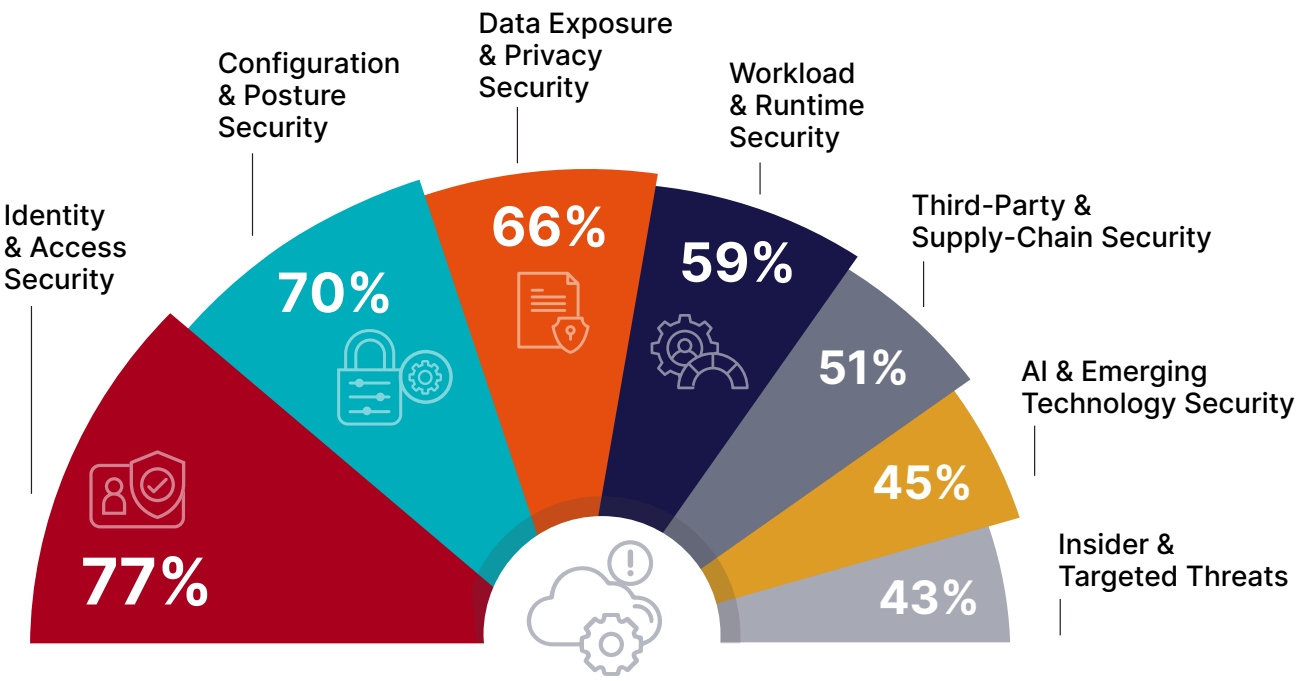
Where Cloud Risk Concentrates

Cloud security risk is concentrated in a small number of recurring areas. Identity and access security ranks as the top cloud-native concern (77%), followed closely by misconfigured cloud services (70%) and data exposure risks (66%). These three areas consistently overshadow other cloud threats, including workload exploits and supply-chain attacks.

These numbers reflect where cloud complexity is hardest to control: excessive permissions and stolen credentials create shadow access paths across environments. Misconfigurations unintentionally expose resources and even sensitive data—exposures that are often difficult to inventory and monitor consistently. As cloud estates expand, these risks become more prevalent and systematic rather than incidental.

Key Cloud Security Concerns

What cloud-native security risks pose the greatest concern for your organization in the next 12 months?



Importantly, these risks persist across every deployment model. Whether organizations operate single-cloud, hybrid, or multi-cloud environments, risk accumulates wherever visibility is fragmented and controls are inconsistent. The concentration of concern around identity, configuration, and data highlights where cloud security programs experience the greatest friction today. This sets the context for how these risks materialize in practice.

The Risk Exposure Chain

A breach rarely begins and ends with a single vulnerability—attackers follow paths: a misconfiguration exposes a resource, a compromised or overprivileged identity enables access, and sensitive data becomes the target. These stages form an exposure chain of connected risks that point solutions typically only monitor in isolation.

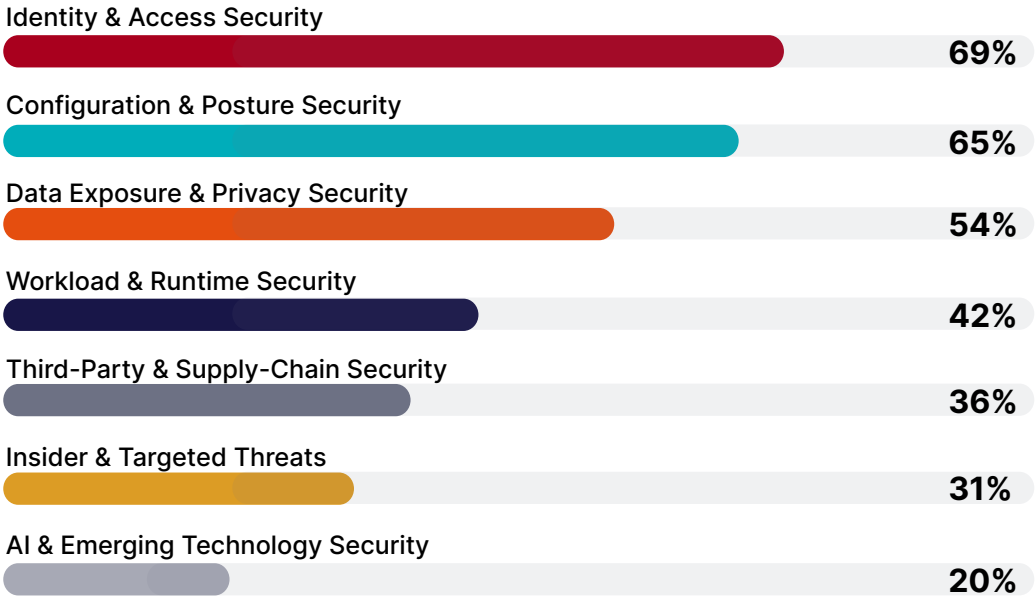
Most organizations manage these domains independently. Posture management tools catch misconfigurations. Identity tools flag excessive permissions. Data security tools classify sensitive assets. Each sees its own segment clearly, but none sees how the segments combine.

A storage bucket misconfiguration may appear low priority on its own. However, when combined with an overprivileged service account and a database containing customer records, it becomes a direct path to a breach.

This disconnect shows in the data. 77% of organizations rank identity as their top risk; the tools addressing each domain rarely share context. Configuration, identity, and data-related incidents are among the most commonly reported cloud security events. Consequently, attack paths often become visible only in hindsight, after the impact.

Cloud Security Exposure Patterns

Which types of cloud-native security incidents have your organization actually experienced in the past 12 months?



Adversaries actively target this gap, using automation to map identity paths, discover misconfigurations, and identify exposed data faster than siloed defenses can correlate the signals. Closing the exposure chain requires security models that see across domains, not just within them.

The Security Automation Gap

Most organizations have introduced automation into their cloud security workflows, but the survey reveals a critical gap between alerting and action. Thirty-seven percent describe their automation as largely alert-focused, identifying potential issues but leaving remediation to manual processes. Only 11% report autonomous remediation capabilities that can act without human intervention.

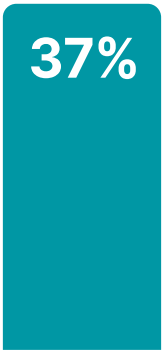
This gap becomes more consequential as cloud exposure changes continuously and attackers operate at machine speed. When automation stops at notification, security teams must still triage, investigate, and coordinate fixes manually—creating backlogs that grow faster than teams can resolve them.

The constraint is rarely automation itself, but the difficulty of trusting automated actions without consistent visibility and shared context across environments.

Cloud Security Automation Is Mostly Alert-Driven

How is your organization using AI or automation to identify and prioritize cloud risks?

No automation (manual processes)



Basic automation (alerts and recommendations)

AI-assisted prioritization (risk scoring and contextual analysis)

Fully autonomous remediation workflows

The AI Arms Race: Why Speed is the New Perimeter

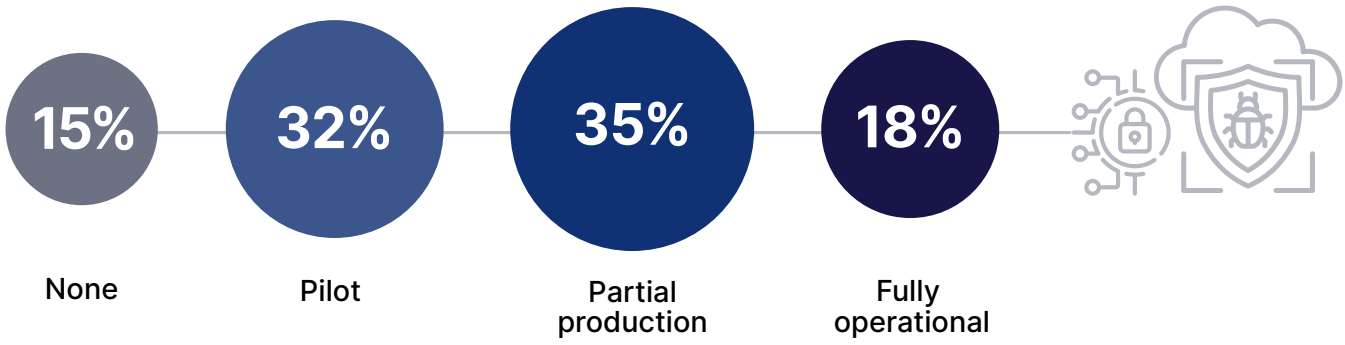
The automation gap is widening as adversaries accelerate; while many organizations are experimenting with artificial intelligence in cloud security, actual operational adoption remains fragmented.

Thirty-two percent report that their AI adoption is limited to pilot efforts; only 18% describe AI-driven detection as fully operational across their cloud environments. Consequently, the majority of organizations rely on human-paced workflows to defend environments that change continuously.

Attackers face no such constraints: as AI tools allow them to scan for misconfigurations, map permission paths, and identify exposed data, the time between exposure and exploitation continues to compress. In this context, defenses that depend on manual analysis or delayed response simply cannot keep up. The challenge is no longer whether threats can be detected, but whether they can be contained fast enough to prevent damage.

AI-Driven Cloud Threat Detection Remains Early-Stage

To what extent are you using AI or machine learning for cloud threat detection or anomaly analysis?



Closing the gap requires a foundation of consolidated visibility and control. When identity, posture, data, and runtime signals flow into a shared analytics layer, defensive AI can finally operate with the accuracy and speed it needs to be effective.

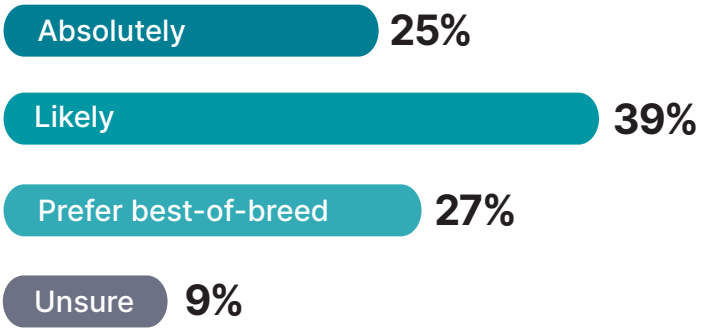
Platform Shift – the Case for Consolidation

As cloud security challenges become more structural, organizations are reassessing how their security architectures are designed. The survey reveals a clear shift away from function-specific point tools managed in isolation—toward unified security ecosystems.

When asked how they would build their security strategy if starting fresh today, nearly two-thirds (64%) of organizations say they would choose a single-vendor platform that unifies network, cloud, and application security. In contrast, only 27% would continue with a ”best-of-breed” approach involving disparate, function-specific tools managed independently.

The Shift to Unified Security Architectures

If you could start over, would you prefer a single-vendor platform that unifies network, cloud, and application security?



64%
of organizations say they would choose a single-vendor platform

This preference reflects operational reality: security teams are simply exhausted by integration overhead. They are seeking fewer platforms that can share telemetry, policy, and context across domains. Importantly, unification does not imply a single monolithic product. Instead, it points to a demand for open, interoperable platforms that integrate through shared data models and coordinated enforcement.

The data suggests that consolidation is increasingly viewed as a way to reduce operational friction and restore visibility, rather than an exercise in tool reduction alone.

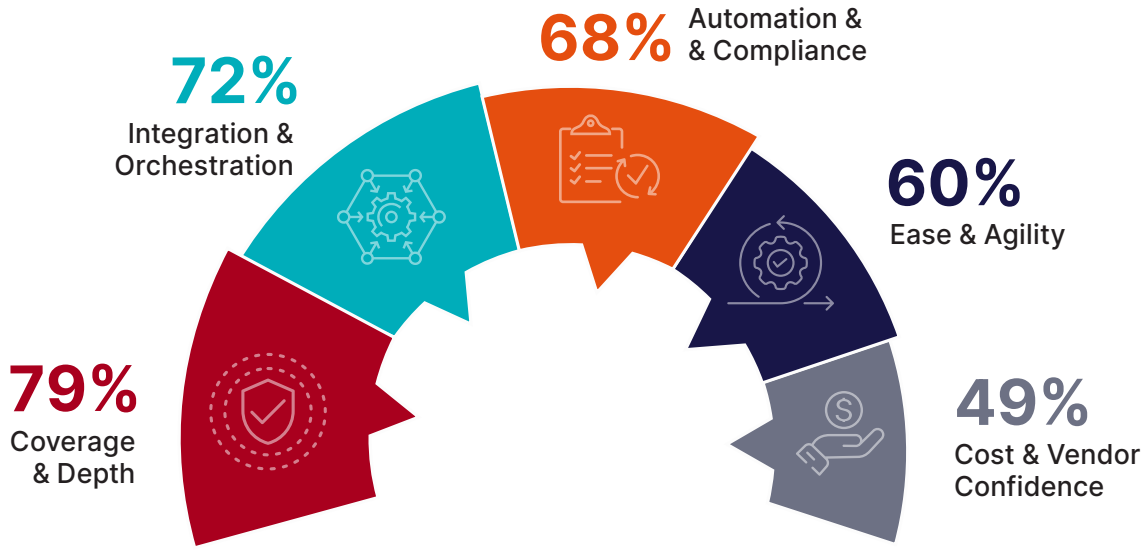
Beyond the Silos: The Unified Security Fabric

The growing preference for consolidation raises a fundamental inquiry: what do security leaders actually mean by "unified" security in practice? The survey shows that organizations are not looking for a single "magic bullet" to replace every tool. Instead, when evaluating cloud security platforms, buyers prioritize coverage and depth across cloud environments (79%), integration and orchestration across security domains (72%), and automation and compliance capabilities (68%)—superseding ease of use or cost considerations.

These priorities reflect practical operating requirements. Security teams require unified observability across identity, configuration, data, and workload activity, with uniform policy enforcement across environments. They also expect security platforms to interoperate with existing network and application controls and integrate into developer workflows, rather than operate in isolation.

Unified Security Priorities

When evaluating cloud security platforms, which criteria and capabilities are most important to your organization's selection process?



In practice, unification means orchestrated systems and shared context, not monolithic architectures. The heavy emphasis on integration and interoperability underscores that security leaders are optimizing for operational synchronization and outcomes rather than simply reducing the number of tools they manage.

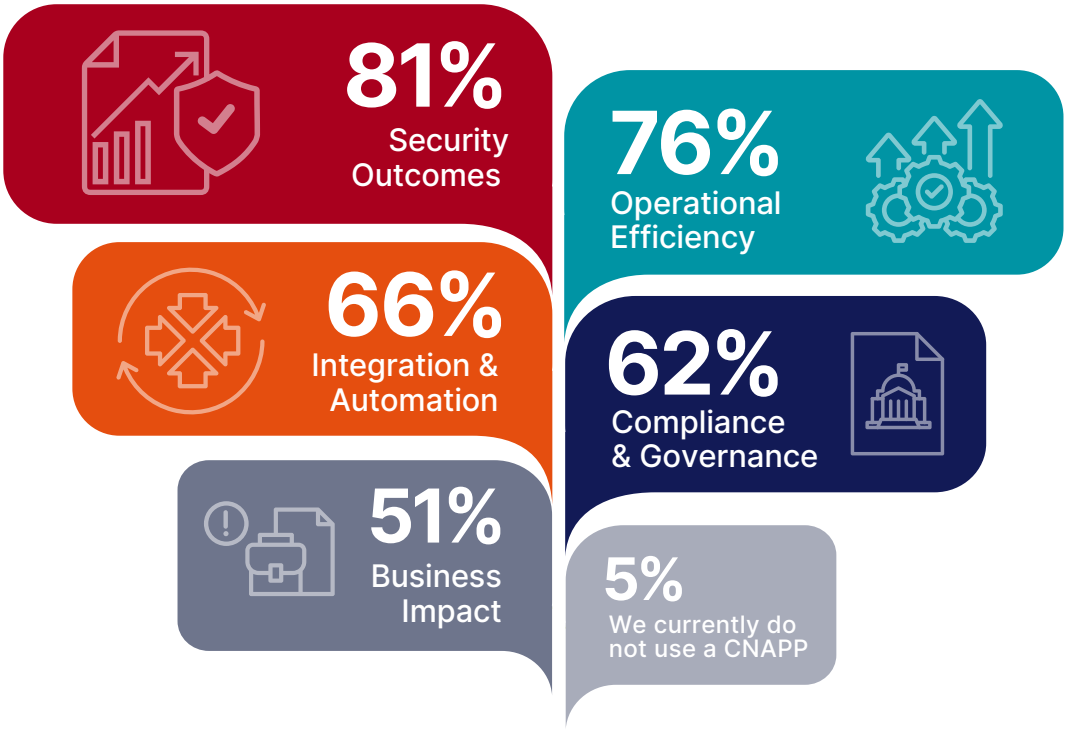
A Blueprint for Convergence: From Fragmented to Unified

The survey results suggest a fundamental maturity shift: organizations are defining cloud security success less by the tools they buy and more by the outcomes they achieve.

Eighty-one percent prioritize security outcomes, such as fewer misconfigurations and reduced excessive permissions. Seventy-six percent emphasize operational efficiency, including accelerated detection and diminished alert noise. Furthermore, 66% highlight integration and automation as essential to scaling security, while 62% identify continuous compliance and governance as a core requirement.

Security Outcomes and Operational Efficiency Define Success

If you use a cloud security platform (CNAPP), which outcomes will define success for your organization?



Together, these responses point to a consistent definition of what “effective” cloud security looks like in practice. Programs that achieve maturity focus on reducing exposure, improving operational efficiency, integrating controls across domains, and enabling automation that teams can trust. Success is measured by unified visibility, control, and response - not by the number of tools deployed.

From Insight to Action: Cloud Security Principles

Taken together, the findings in this report point to a clear pattern. Organizations making progress are not chasing individual tools or isolated capabilities; they are reshaping how cloud security operates day-to-day: the principles below reflect what effective programs consistently prioritize when dealing with scale, fragmentation, and machine-speed threats—practical operating choices grounded in the realities surfaced by the survey.

PRINCIPLE	WHAT EFFECTIVE PROGRAMS DO	WHY IT MATTERS NOW
1 **Treat visibility as a foundation**	Establish unified visibility across cloud accounts, identities, data stores, and workloads as a baseline operating requirement.	Without shared visibility, detection slows, investigations fragment, and maturity stalls.
2 **Reduce fragmentation**	Rationalize overlapping tools and consolidate around shared telemetry, policy, and context across environments.	Tool sprawl is the top operational barrier: each added console increases friction and operational load.
3 **Connect the risk domains**	Assess identity, configuration, and data exposure together rather than as isolated control areas.	Cloud attacks exploit relationships across domains that point solutions cannot detect in isolation.
4 **Automate for outcomes**	Focus automation on resolving low-risk, high-volume issues rather than generating notifications that require manual follow-up.	Alert-only automation shifts burden to teams and cannot keep pace with machine-speed threats.
5 **Extend integration beyond cloud boundaries**	Integrate cloud security with network, SaaS, and endpoint visibility to reflect the full attack surface.	The attack surface spans environments; fragmented integration constrains effective detection and response.

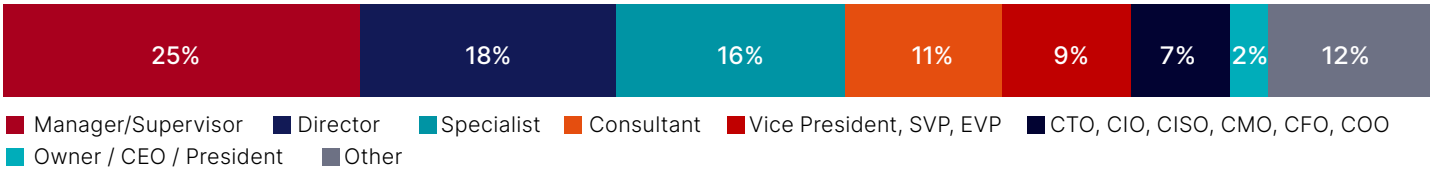
Methodology and Demographics

The 2026 Cloud Security Report is based on a comprehensive survey conducted in late 2025, gathering insights from 1,163 IT and cybersecurity professionals across a range of countries and industries, including technology, financial services, healthcare, and government. The cohort represents a broad spectrum of organizational scales—from mid-market to large enterprises—and a diverse range of roles, from frontline security specialists to C-level executives.

The survey, conducted online, explored key trends, challenges, and priorities in cloud security. The findings provide a comprehensive benchmark of how organizations are navigating the complexities of cloud environments and evolving their security technologies to address emerging threats.

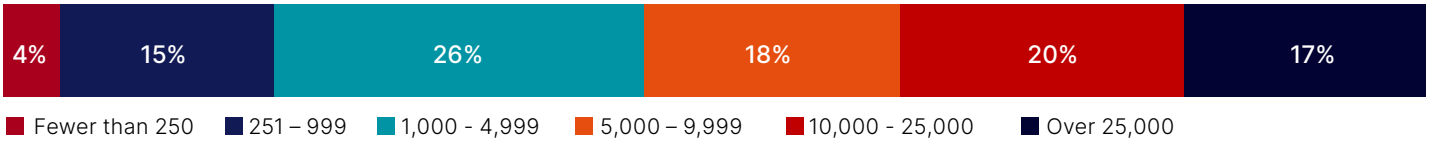
For multi-select questions, percentages may exceed 100% to reflect all options selected by respondents.

CAREER LEVEL

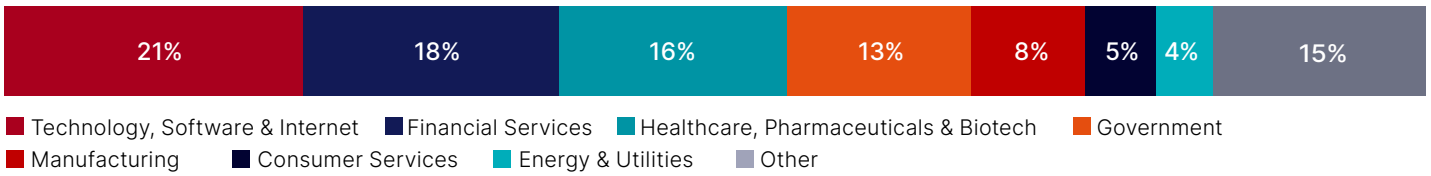


DEPARTMENT

COMPANY SIZE



INDUSTRY



Fortinet (NASDAQ: FTNT) secures the largest enterprises, services providers, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networks, application, multi-cloud, or edge environments. Fortinet ranks #1 as a security company, with more than 900,000 clients who trust their solutions and services to protect their businesses.

www.fortinet.com

Cybersecurity
INSIDERS

STRATEGIC INSIGHT FOR CYBERSECURITY LEADERS

Cybersecurity Insiders provides independent research and analysis focused on the operational reality of enterprise cybersecurity. We gather insights from senior security and IT leaders to examine how high-level strategies translate into day-to-day execution. Our analysis identifies the measurable gaps between intended strategy and actual risk exposure, offering a credible, data-driven foundation for security decision-making and industry benchmarking.

For more information, visit
cybersecurity-insiders.com

Jan 2026 // Version 2.0