SANS | Research Program

2025 SURVEY

SANS 2025 Multicloud Survey: Securing Multiple Clouds at Scale

Written by **Kenneth G. Hartman**

August 2025

RAPID7

SANS 2025 MULTICLOUD SURVEY

Key Findings

Azure Edges Ahead

91% use Azure, narrowly surpassing AWS (86%)

Azure narrowly surpasses AWS in reported usage among respondents, potentially signaling strong enterprise adoption of Microsoft ecosystems.

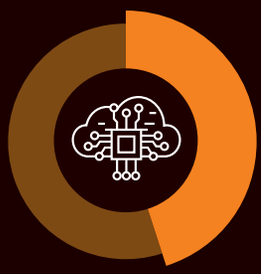
Security Maturity Is a Work in Progress

45% rate their multicloud security strategy as intermediate

Nearly half of organizations are progressing but have not yet reached mature multicloud security practices.

Complexity Is the Top Challenge

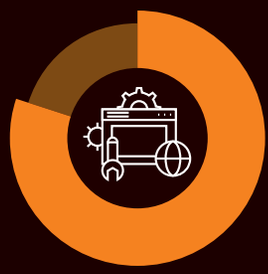
63% cite complexity as their primary challenge.



Complexity is the most cited challenge in managing multicloud security, ahead of policy consistency and visibility.

Third-Party Tools Are Essential

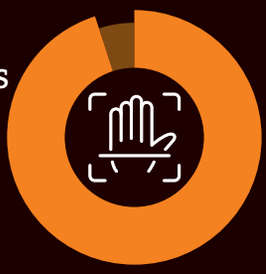
80% use or plan to use third-party security solutions.



Nearly half have implemented third-party tools, and another third are considering it, highlighting the need to supplement native cloud features.

Managing Identities Is Difficult

95% find managing identities and entitlements across clouds at least a minor challenge.



Managing identities and entitlements across multiple cloud providers is a significant operational complexity for nearly all organizations.

Adoption of AI for Security Is Emerging: Both a Promise and a Caution

Organizations recognize AI's potential in enhancing threat detection, automation, and prediction but face governance, trust, and integration challenges.

Survey Author

Kenneth G. Hartman
SANS Certified Instructor

VIEW PROFILE

CURRENTLY TEACHING

SEC510: Cloud Security Controls and Mitigations™

SEC488: Cloud Security Essentials™

Kenneth G. Hartman is a cloud security leader with over two decades of experience spanning architecture, engineering, compliance, and digital forensics. He is the owner of Lucid Truth Technologies, a Michigan-based digital private investigation and forensic consulting firm, and has held key roles at organizations such as Google, SAP Ariba, Illumina, and Visonex. Ken is a Certified SANS Instructor, teaching SEC510 and SEC488, and has co-authored multiple SANS surveys and research papers. He holds a B.S. in Electrical Engineering from Michigan Technological University and an M.S. in Information Security Engineering from the SANS Technology Institute, along with numerous GIAC certifications. Ken is passionate about advancing cloud security practices and empowering professionals to meet the challenges of rapidly evolving cloud technologies.

Expert Contributor

Simon Vernon
SANS Certified Instructor

VIEW PROFILE

CURRENTLY TEACHING

SEC510: Cloud Security Controls and Mitigations™

SEC540: Cloud Security and DevSecOps Automation™

SEC549: Cloud Security Architecture™

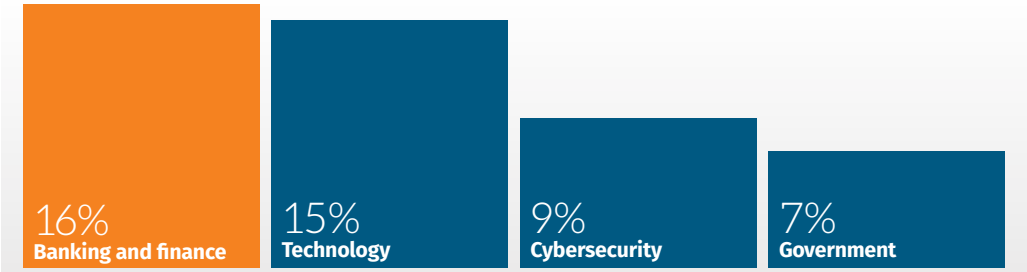
Simon Vernon is a cloud security and digital forensics specialist with significant experience in both public and private sector roles. He has contributed to the development of cloud security best practices and has played a key role in shaping security strategies for organizations navigating complex multicloud environments. Simon is known for his practical approach to security challenges and his commitment to sharing knowledge within the cybersecurity community. He regularly contributes to SANS research initiatives and brings a wealth of hands-on expertise to the Multicloud Survey as an expert contributor.

Executive Summary

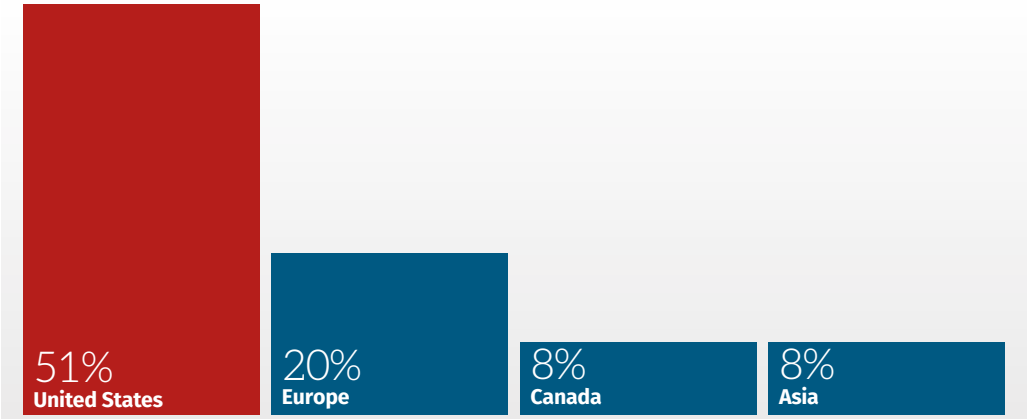
The 2025 SANS Multicloud Survey reveals a field that is steadily maturing, with organizations establishing dedicated multicloud security teams, increasingly integrating automation into their workflows, and moving toward standardized adoption of preventive controls. CSPM and CNAPP remain the leading security solutions, while SASE and automated IAM tools are gaining traction. Limited resources, increasingly complex cloud environments, and the challenge of maintaining consistent security controls across multiple providers continue to present significant hurdles for security professionals.

Demographics

Top 4 Industries Represented



Regions



Top 4 Roles Represented

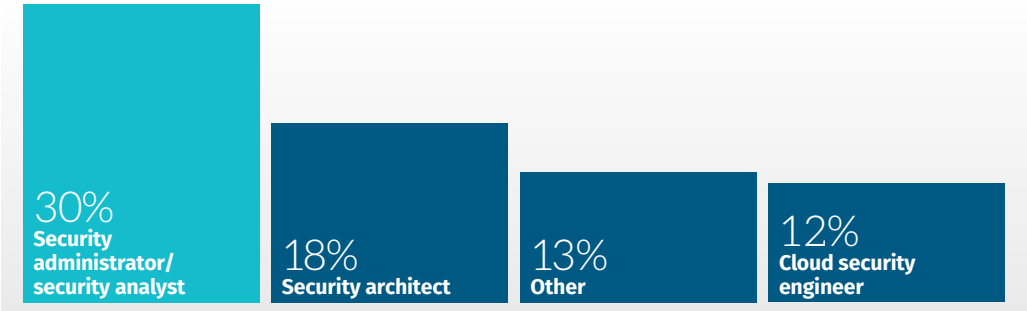


Figure 1. Demographics of Survey Respondents

Cloud Adoption and Workload Distribution

The survey respondents indicated that Azure and AWS are the dominant multicloud service providers used, with Azure currently holding a leading edge in adoption (see Figure 2) and share of the workloads (see Figure 3). Google Cloud maintains a solid third position, valued for its data analytics and AI/ML capabilities. A long tail of niche and private providers plays a supporting role, highlighting the true diversity of multicloud strategies. Over the past three years of the survey, we have noticed users shift from reporting that they were using Azure, as indicated by the usage metric, to using Azure for a significantly increased share of the workload.

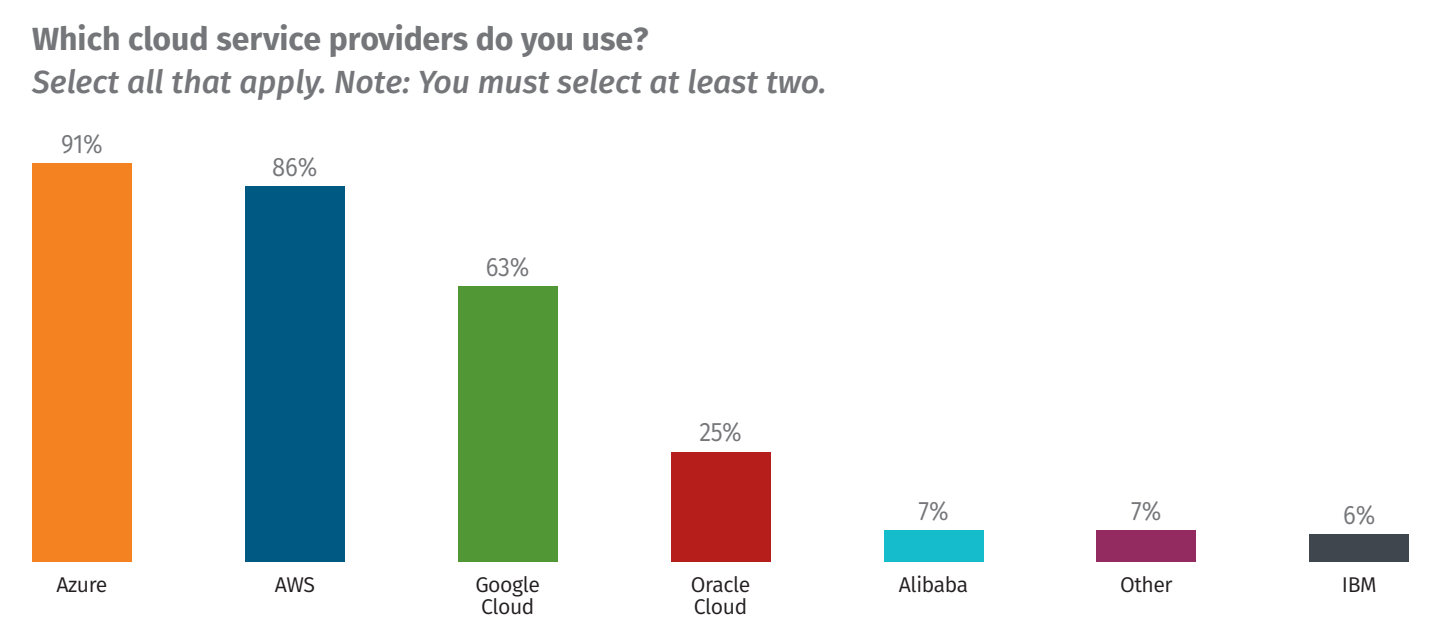


Figure 2. Cloud Service Providers in Use

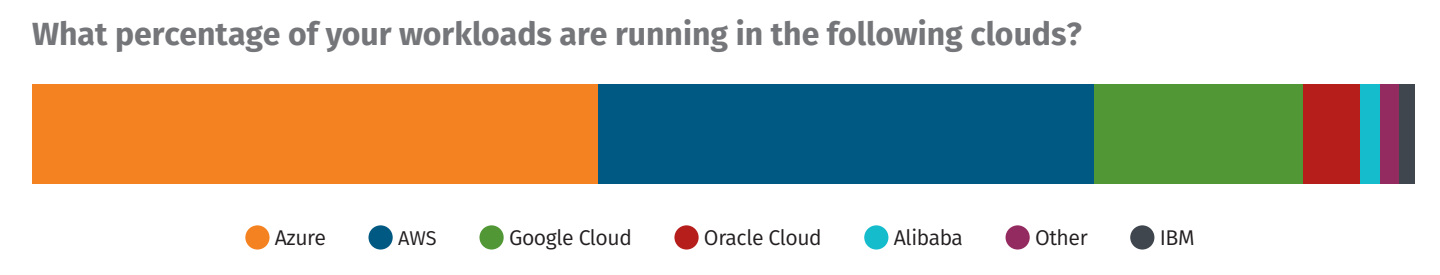


Figure 3. Cloud Service Providers' Share of the Workload

Expert Corner

The difference between 'intermediate' and 'mature' cloud security lies in dedicated ownership. With 51% of organizations already operating a dedicated multicloud security team—and another 25% planning to—leaders who delay will find themselves exposed to uncontrolled complexity and policy drift. The 25% with no plans for such teams risk fragmented responsibilities that attackers readily exploit. Effective cloud security isn't a side-desk activity—it's foundational to resilience and risk reduction.

Terrence Williams
SANS Certified Instructor; Security Engineer, Investigations at Meta

VIEW PROFILE

Multicloud Security Strategy: A Work in Progress

Many organizations still treat multicloud security as an extension of their single-cloud practices—and it shows (see Figure 4). Nearly half rate their strategy as only "intermediate," meaning they've moved past pilots but haven't built resilient, preventive architectures. This plateau is dangerous because attackers aren't pausing while security matures.

Self-assessment of multicloud security maturity reveals that cohesive security governance is still in development despite broad multicloud adoption.

Figure 4. Multicloud Security Maturity

Expert Corner

Each of the major cloud providers have radically different approaches to assigning permissions, pivoting between identities, and logging activity. Building reliable detections and conducting investigations require security professionals to truly be subject matter experts in each platform to be effective. What concerns me most is the growing trend of companies adopting a multi-cloud strategy as an operational decision, without fully understanding the complexity that each individual cloud brings from a monitoring perspective.

Ryan Thompson
SANS Certified Instructor Candidate; Senior Cloud Security Researcher at CrowdStrike

VIEW PROFILE

Dedicated Teams for Multicloud Security Management

The presence of a dedicated multicloud security team is a strong indicator that an organization understands the complexity of operating across multiple cloud providers. With 51% of respondents already having one in place and another 25% planning to build one, most organizations recognize the need for specialized focus (see Figure 5).

However, the other 25% with no plans or uncertainty signals a serious gap in governance. Without clear experience or ownership, multicloud security often becomes fragmented, reactive, and heavily reliant on native defaults. A dedicated team isn't just a resource decision—it's foundational to consistent policy enforcement, automation, and long-term risk reduction.

Does your organization have a dedicated team or role for multicloud security management?

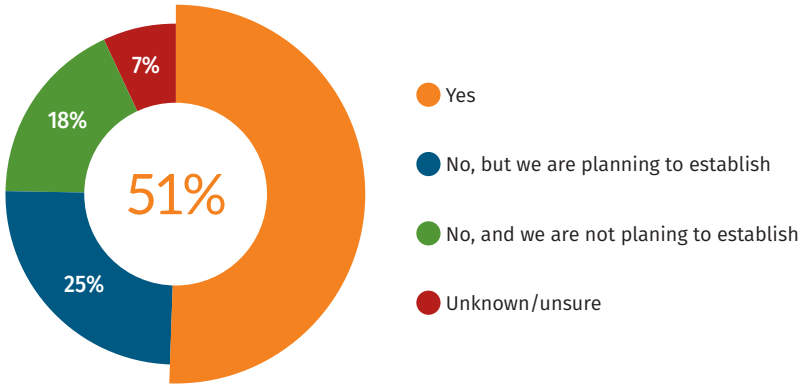


Figure 5. Dedicated Team/Role for Multicloud Security Management

Complexity Is the Core Challenge—and It's Not Going Away

When it comes to multicloud security, complexity isn't just a challenge, it's the root cause of nearly every other problem. Whether it's policy inconsistency, limited visibility, or persistent skill gaps, these are all symptoms of sprawling environments that lack unified control (see Figure 6).

What are the primary challenges your organization faces in managing security across multiple clouds?

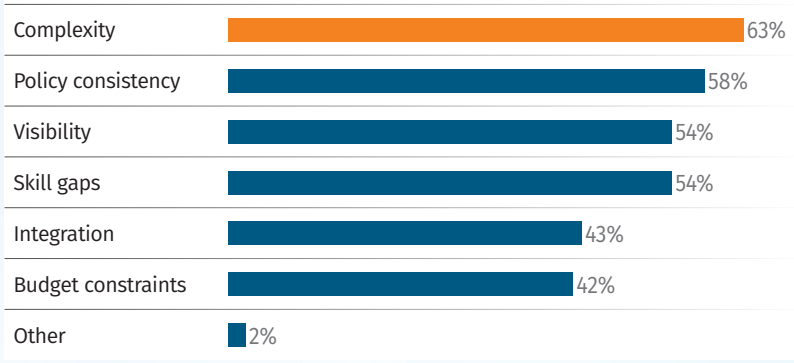


Figure 6. Challenges in Managing Multicloud Security

Complexity can quickly outpace even well-resourced teams. As organizations layer new providers, services, and tools, integration becomes harder, not easier. And without standardization and automation, security teams end up fighting fires instead of reducing risk. Budget constraints only amplify the issue, forcing trade-offs that often leave critical gaps in coverage.

If organizations are serious about securing multicloud at scale, they must start treating complexity as an architectural challenge, not just an operational headache.

Cloud Security Tooling Trends Toward Convergence, But Fragmentation Persists

Respondents indicated that cloud platform security management (CSPM) still leads as the most common solution deployed (see Figure 7). Organizations are moving toward converged platforms that unify posture management, workload protection, and identity, a necessary evolution as multicloud complexity outpaces the capabilities of siloed tools. Automation and network-centric solutions like security automation and orchestration (SAO) and secure access service edge (SASE) are also gaining traction, while cloud workload protection platforms (CWPP) and cloud infrastructure entitlement management (CIEM) still lag, often due to deployment friction or ownership ambiguity.

Figure 7. Cloud Services Deployed

But as Figure 8 illustrates, the multivendor reality complicates this picture. Many organizations use overlapping tools within the same category, not by accident, but by necessity. Regulatory demands, M&A activity, functional gaps in native tools, and organizational structure all drive duplication. In my experience, this multivendor approach is often a deliberate choice for resilience and flexibility, but it comes at a cost. Integration, training, and governance become harder to scale, especially when tool sprawl goes unmanaged. Until organizations unify control planes and streamline tooling, multicloud security will remain operationally burdensome and strategically fragmented.

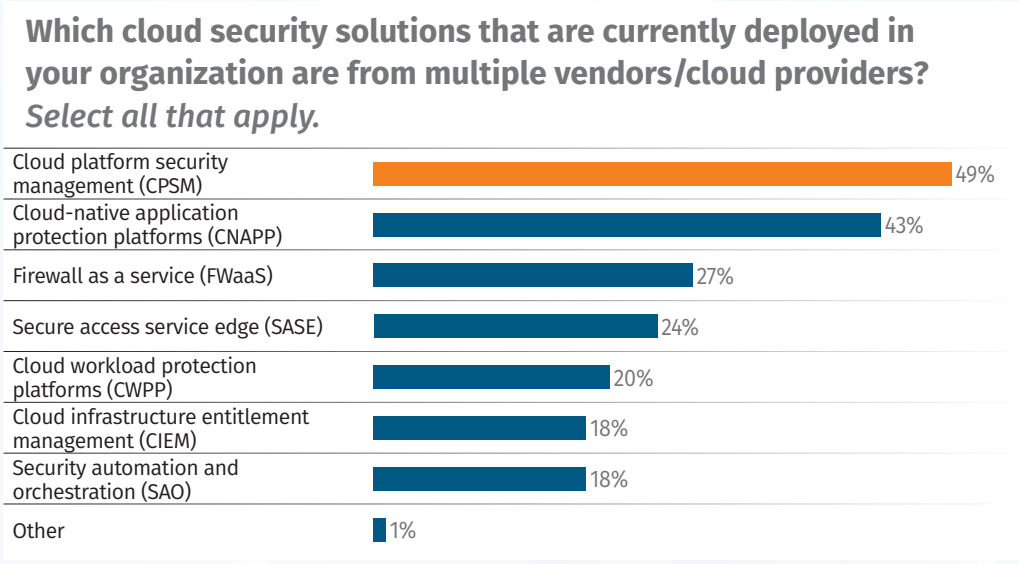


Figure 8. Cloud Solutions from Multiple Vendors

Cloud-Native Tools Alone Aren't Enough

A large portion of respondents (77%) rated cloud-native solutions as only "somewhat effective" or "neutral"—a clear signal that native controls often fall short in complex multicloud environments (see Figure 9). This reflects a fundamental truth: No single cloud provider offers complete, cross-platform visibility or unified policy enforcement out of the box.

That's why nearly 80% of organizations either use or plan to use third-party tools. These platforms are increasingly essential for organizations that need consolidated dashboards, deeper analytics, and consistent controls across providers. But tool adoption alone isn't enough, these technologies must be properly staffed and supported. Without skilled personnel who understand how to operationalize CNAPP and related solutions, even the best tools underdeliver.

Organizations need to approach third-party tools not as bolt-ons, but as integral components of a scalable, multicloud security strategy.

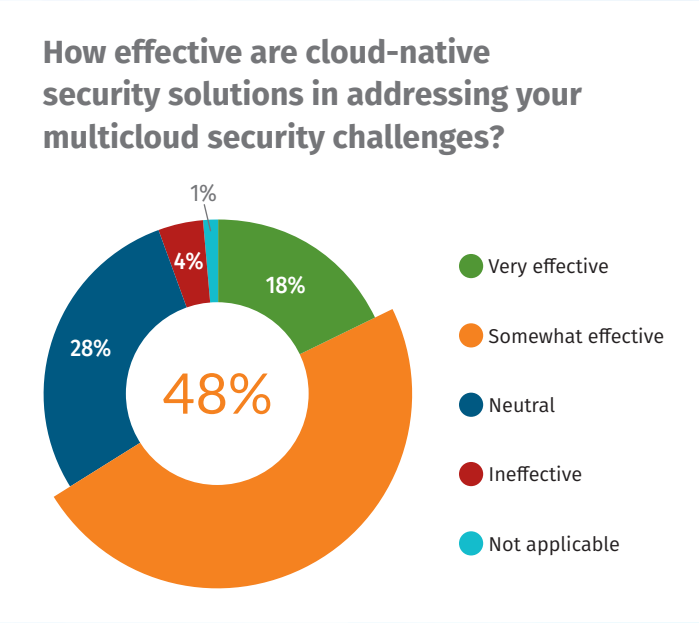


Figure 9. Effectiveness of Cloud-Native Solutions

Expert Corner

Adopting third-party cloud security solutions should signal strategic intent, not tactical patchwork. Too often, organizations treat these as point solutions to address immediate concerns, rather than foundational elements of a coherent multicloud security architecture. CSPM tools provide continuous visibility, detect misconfigurations, and support compliance needs. However their true value is realized when skilled staff can interpret and act on findings, enabling timely remediation and meaningful risk reduction.

Jason Larkin
SANS Certified Instructor Candidate; Head of Platform Security Architecture

VIEW PROFILE

Identity and Access Management

Identity and access management (IAM) is evolving rapidly, with many organizations adopting advanced capabilities and moving toward automation. Yet as IAM maturity grows, so does complexity, especially in multicloud environments where fragmented tools, inconsistent policies, and legacy dependencies remain common. The following sections explore these trends, highlighting both the progress made and the persistent operational challenges.

IAM Maturity Is Rising, but Complexity Still Dominates

Survey respondents indicated a broad adoption of core IAM capabilities like multi-factor authentication (MFA), single sign-on (SSO), privileged access management (PAM), and identity federation (see Figure 10). This is a promising sign that many organizations have moved beyond basic access controls. However, the use of multiple vendors across IAM domains introduces significant friction. Policy enforcement becomes inconsistent, life cycle management gets fragmented, and integration efforts increase.

Which identity and access management (IAM) solution types does your organization use? Which are from multiple vendors/cloud providers for the same type? ***Select all that apply.***

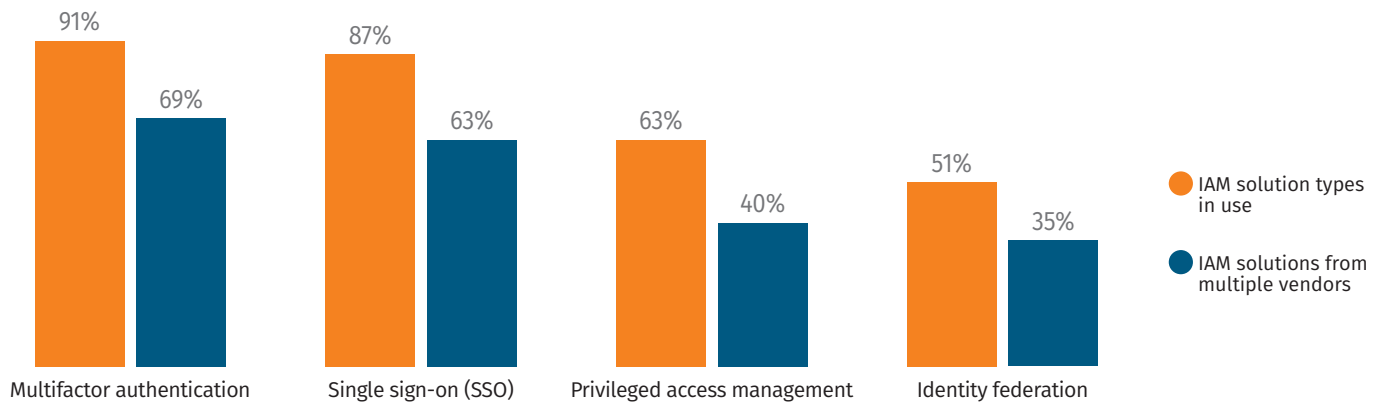


Figure 10. IAM Solutions In Use and From Multiple Vendors

Managing identities across multicloud environments remains one of the most difficult operational tasks in cloud security (see Figure 11). The complexity of coordinating users, roles, and policies across disparate platforms continues to pose significant challenges for security teams.

How significant is the challenge of managing identities and entitlements across multicloud service providers in your organization?

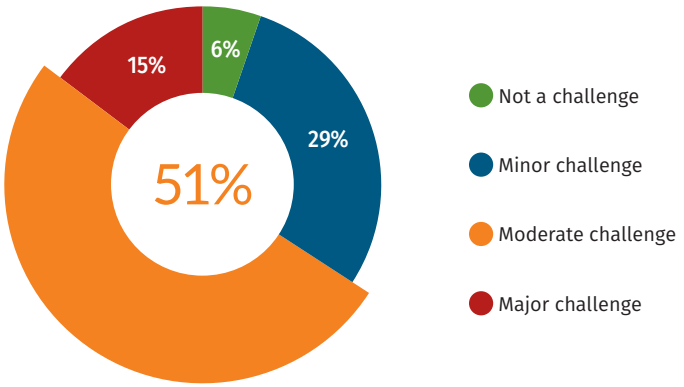


Figure 11. The Challenge of Managing Identities

This is why the strong momentum toward automation (see Figure 12) is so critical. More than 80% of organizations are either implementing or planning automated IAM tools. This marks a necessary shift toward scalable, policy-driven identity orchestration. It is not just about efficiency; it is about reducing standing privilege and maintaining control in dynamic environments.

Have you integrated any automated identity and access management (IAM) tools into your security workflows for managing user identities, enforcing least privilege access, detecting unauthorized access attempts, and dynamically adjusting permissions based on policies?

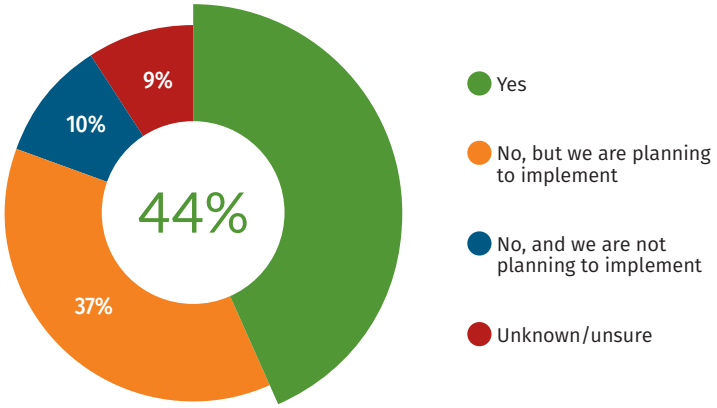


Figure 12. Automated IAM Tools

Directory strategies are also evolving (see Figure 13). Although a growing number of organizations (42%) have adopted fully cloud-based identity platforms, nearly 40% remain tied to on-premises Active Directory with no current plans to decommission. Hybrid models are still common. In many cases, this is not due to inertia, but because business requirements, legacy dependencies, and compliance obligations demand it. Identity architecture must reflect operational realities, not just aspirational cloud-first goals.

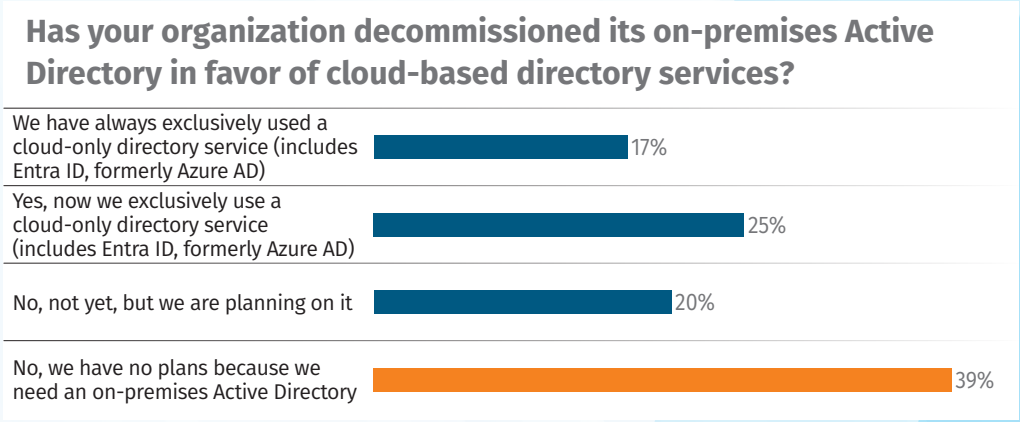


Figure 13. Decommissioning On-Premises Active Directory

Related SANS Course:

SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise™

To build resilient, scalable IAM across multicloud environments, professionals need to understand both architectural patterns and control implementation. SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise offers deep insight into designing secure identity systems that align with business needs, cloud-native capabilities, and compliance objectives. This course is especially relevant for those grappling with federated identities, policy enforcement, and automation at scale.

Workload Identity Federation: Underutilized but Strategically Important

Workload identity federation remains an emerging and underutilized capability. Nearly 40% of survey respondents remain unsure if it is even in use within their environments. This uncertainty suggests that federation has yet to become mainstream, despite its growing importance.

This is a missed opportunity. Federation offers a scalable, secure alternative to legacy secrets management by eliminating static credentials and replacing them with short-lived, centrally managed tokens issued through an organization's existing identity provider. As Simon Vernon notes, this enables fine-grained access, comprehensive audit trails, and a dramatically reduced attack surface. It is a cornerstone capability for secure-by-design, secure-by-default architectures—particularly in complex, multicloud environments.

Of the 31% of organizations that use workload identity federation, only a small portion report full enterprise-wide implementation (21%), while many are still in early or partial rollout phases.

As organizations continue to mature in their cloud adoption, workload identity federation should be considered a key component of any modern identity strategy. Its adoption is not just a technical enhancement but a strategic investment in reducing risk and improving operational resilience.

Security Benefits of Workload Identity Federation

- **Eliminates static credentials by using short-lived, federated tokens, reducing secret sprawl and risk of compromise.**
- **Enables precise, auditable access through scoped, policy-based authentication for workloads.**
- **Supports secure cross-cloud identity in multicloud environments, aligning with zero trust principles.**

Expert Corner

Workload identity federation empowers enterprises to eliminate static credentials by issuing short-lived, centrally managed tokens through their existing identity provider—enabling fine-grained, least-privilege access, comprehensive audit trails, and a dramatically reduced attack surface. It is a fundamental element of secure by design, secure by default.

VIEW PROFILE

Simon Vernon
SANS Certified Instructor

CURRENTLY TEACHING

SEC510: Cloud Security Controls and Mitigations™

SEC540: Cloud Security and DevSecOps Automation™

SEC549: Cloud Security Architecture™

Specialized Security Technologies

As organizations mature their cloud security strategies, the focus is shifting toward integrated, scalable solutions that can keep pace with cloud complexity. Emerging trends in SIEM, SASE, infrastructure as code (IaC), and SAO reveal a strong push toward consolidation, visibility, and efficiency. The following sections explore how these technologies are being adopted, the challenges that remain, and why integration and alignment are key to realizing their full potential.

SIEM Adoption Shifts Toward the Cloud

As shown in Figure 14, cloud-hosted SIEMs—especially single-vendor—now dominate, reflecting a shift toward centralized visibility and efficiency. Hybrid models remain common, often due to cost, compliance, or transitional needs, but they add operational complexity.

What stands out to me is the 15% with no SIEM coverage or uncertainty. That's a critical visibility gap in environments where real-time monitoring is essential. Cloud-first SIEM is clearly the direction of travel, but it must be paired with strong integration and clear ownership to deliver real value.

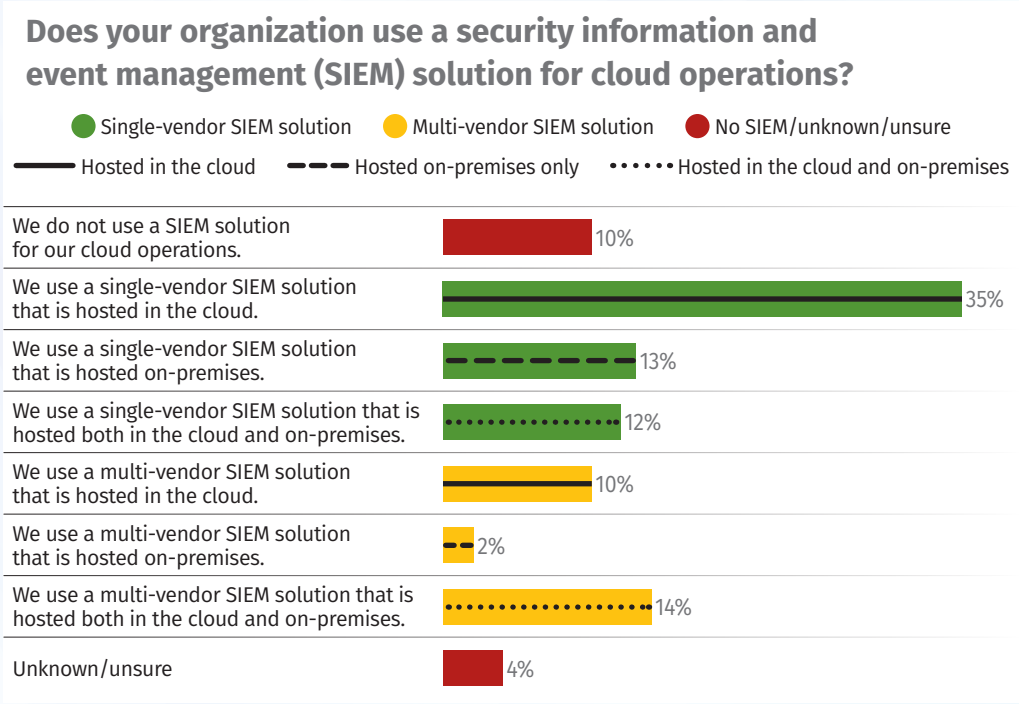


Figure 14. Deployment Models for SIEM in Cloud Operations

Secure Access Service Edge Adoption Signals Shift Toward Converged Cloud Security

SASE continues to gain traction as organizations seek to unify networking and security through cloud-delivered architectures. Figure 15 shows that more than one-third of organizations have adopted SASE, with another 29% planning to follow.

That momentum is backed by user feedback as most respondents report a positive impact on their overall security posture.

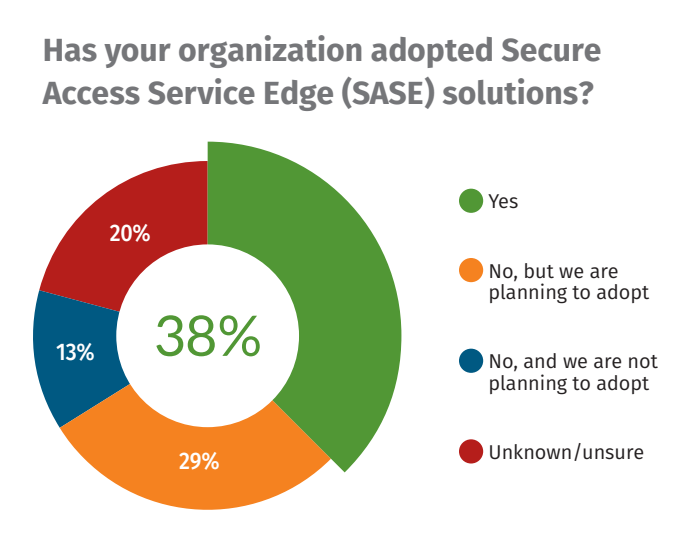


Figure 15. Adoption Status of SASE Solutions

SASE represents more than a tooling trend. It's a response to the reality of distributed workforces, hybrid apps, and shifting perimeter boundaries. Early adopters are already deploying key components like zero trust network access (ZTNA), cloud access security brokers (CASB), and SD-WAN. Although full adoption remains a work in progress, the growing deployment of ZTNA and CASB suggests that organizations are prioritizing user-centric and cloud-aware controls. The challenge now is to ensure these components are integrated and policy-aligned, rather than operating in silos.

Infrastructure as Code: Essential but Incomplete

IaC is now foundational for secure, scalable cloud deployments. Adoption is strong and most find the tools effective, but gaps remain. Integration into CI/CD and continuous tuning of rulesets are critical to prevent misconfigurations and enforce governance across multicloud environments.

Security Automation and Orchestration: Critical for Cloud-Scale Defense

SAO is no longer optional in multicloud environments. About a third use SAO, and another third plan to, indicating SAO is a strategic priority for nearly 70% of organizations to improve operational efficiency.

As shown in Figure 16, organizations are prioritizing automation in threat detection, vulnerability management, and incident response—areas where manual effort simply can't keep up with cloud velocity. This isn't just about efficiency; it's about survivability. Without automation, security teams can't scale, risk accumulates, and response times lag. SAO is becoming the backbone of modern security operations, enabling consistency, speed, and resilience in increasingly complex environments.

Benefits of Automating Security Processes

Why Automation is Essential for Modern Security Operations

Improved Efficiency and Time Savings
- Save time
- Reduced manual workloads

Enhanced Threat Detection and Response
- Fast incident detection
- More proactive

Consistency, Accuracy, and Reduced Human Error
- Automation enforces uniform processes, reducing variation and minimizing mistakes

Operational Scalability
- Adoption at scale with scaling teams
- Security can grow with infrastructure demands—without proportionally growing the team

Analyst Experience and Retention
- Less-frustrated analysts
- Relief from alert fatigue and mundane tasks improves morale and retention

Cost Control and Risk Reduction
- Reduced operational expenditures

Which aspects of security operations have been automated in your organization?
Select all that apply.

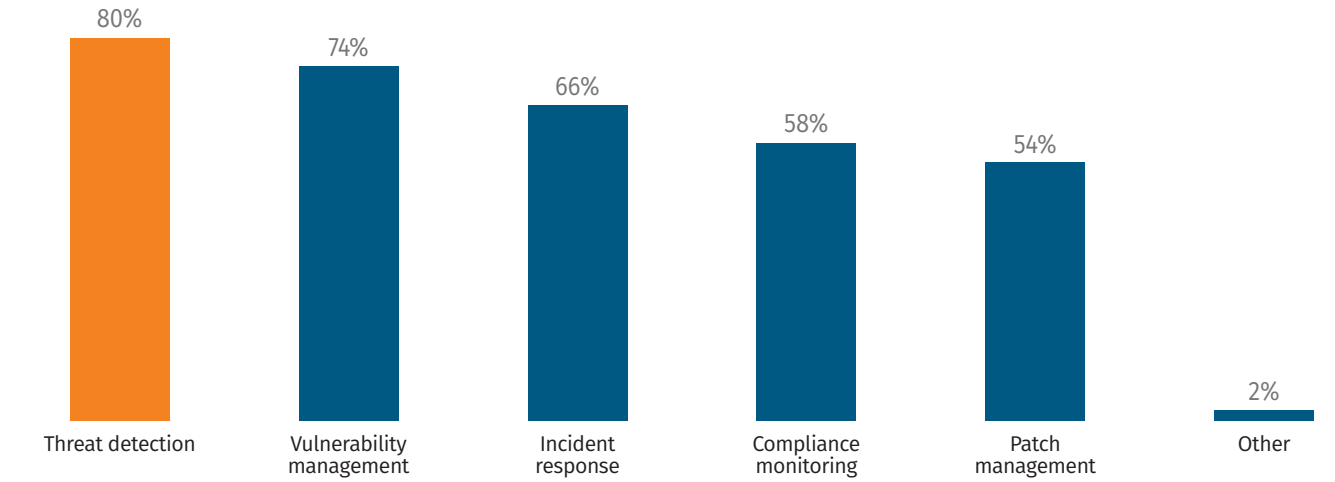


Figure 16. Security Operations Automation by Category

Governance and Barriers: Strategic Alignment Is the Differentiator

Overcoming barriers to cloud security adoption goes beyond adding new tools. Instead, it demands a coordinated, organization-wide transformation. Success hinges on aligned leadership, skilled teams, and strategic investments that clearly deliver value. Without this foundation, even well-resourced efforts can lose momentum. Real progress requires cultural change and strong governance alongside smart technology decisions.

AI illustrates this perfectly. Although it's increasingly seen as a force multiplier, particularly in detection, automation, and response, adoption remains inconsistent. Generative AI introduces new challenges around governance, trust, and integration. These aren't just technical hurdles; they're strategic ones. Without clear frameworks and ownership, AI risks becoming another disconnected capability rather than a driver of proactive defense.

In both traditional and AI-enabled security programs, the lesson is the same: Success depends on strategic clarity, phased implementation, and measurable outcomes. Organizations that treat these as technical problems will fall behind. Those that treat them as leadership and execution challenges will move faster, with greater confidence.

AI in Multicloud Security

AI for Threat Detection and Anomaly Detection

- Real-time log analysis
- Behavioral analytics
- AI-enhanced SIEM/SOAR

Automation and Incident Response

- Automate triage/remediation
- SOAR case summaries
- Self-healing

Generative AI (GenAI) and LLM Use Cases

- Summarizing events
- Code assistance
- Chatbots for SOAR

Posture Management and Configuration Compliance

- Detect/prioritize misconfigurations
- Recommend least privilege

Predictive Analytics and Proactive Security

- Forecast vulnerabilities
- Predict workload anomalies

Actionable Insights for CIOs and CISOs

- **Prioritize complexity management—**Streamline governance, ensure policy consistency, and enhance visibility through standardized frameworks and automation to tackle complexity—the top challenge cited by 63% of respondents.
- **Accelerate security maturity through dedicated roles—**Move beyond intermediate maturity by clearly defining dedicated multicloud security teams or roles to enhance strategic execution and governance effectiveness.
- **Strategically evaluate third-party security tools—**Given 80% of organizations either currently utilize or plan to adopt third-party solutions, CIOs and CISOs should rigorously assess these tools to complement and enhance native cloud provider offerings.
- **Consolidate and automate IAM practices—**Address the significant challenge (95%) of managing cross-cloud identities by consolidating IAM solutions, implementing automated identity management, and enforcing uniform policies across clouds.
- **Implement AI with clear governance frameworks—**Actively explore AI-driven tools for improved threat detection, automated responses, and predictive security analytics while establishing robust governance, integration strategies, and measures for trust management.

Conclusion: Securing Multiple Clouds at Scale

The SANS 2025 Multicloud Survey highlights a key trend: Organizations are advancing in cloud security, yet many are still grappling with complexity, fragmentation, and reactive approaches. Core technologies such as CSPM, CNAPP, SASE, and MFA are widely deployed, but their effectiveness is often constrained by integration challenges, talent gaps, and uneven governance.

These challenges are technical and structural. Complexity remains the top obstacle, underscoring the need for simplified architectures, cross-cloud visibility, and unified policy enforcement. IAM continues to strain teams as they contend with siloed platforms, diverse user populations, and the need to reduce standing privilege. Meanwhile, security automation and orchestration are emerging as force multipliers, helping teams scale operations in the face of growing demand.

The shift toward automation, convergence, and workload identity federation reflects a broader pivot toward sustainable, scalable multicloud security. But progress depends on more than tools. It hinges on dedicated leadership, clear strategy, and ongoing investment in people and processes. AI is beginning to reshape this space, but without trust, governance, and integration, it risks becoming yet another layer of complexity.

Geopolitical dynamics add further uncertainty. Export controls, regulatory divergence, and global trust concerns are forcing organizations, especially outside the United States, to rethink their cloud dependencies and provider strategies.

Organizations that succeed in this environment will be those that treat multicloud security not as an IT function, but as a business enabler. That means aligning teams, automating where it counts, and continuously adapting to new risks. The journey isn't easy, but it is necessary.

Use the insights in this report to benchmark maturity, identify gaps, and drive forward with purpose. Security at scale requires more than technology. It demands leadership, clarity, and the resilience to keep improving.

Sponsor

SANS would like to thank this survey's sponsor:

RAPID7

SANS | Research Program

About the SANS Research Program

The SANS Research Program is a key initiative by the SANS Institute and a premier global provider of cybersecurity research and information. SANS Research Program is designed to provide cybersecurity practitioners and leaders with data-driven insights, thought leadership, and solutions that help them better understand and respond to evolving security challenges. All content is authored by SANS instructor experts from around the world who apply their years of experience from hands-on practitioner work in the field, advisory roles, and the classroom to provide education, guidance, and actionable insights that help make the cyber world a safer place.

To learn about sponsorship opportunities for research, content, and in-person or virtual events, email us at **Sponsorships@sans.org** or go to **www.sans.org/sponsorship**.