intruder

2026 Cloud Security Index

How cloud security risk differs across AWS, Azure, and Google Cloud: top misconfigurations, provider comparisons, and remediation times from 3,000 organizations

intruder.io

August 2026

The challenge of managing risk in multi-cloud environments

Cloud adoption has changed how organizations build and run infrastructure, but it has also moved more security decisions into the configuration layer. Under the shared responsibility model, cloud providers secure the underlying platform, while customers are responsible for how services, identities, networks, and data stores are configured.

That matters because seemingly minor configuration settings can create real exposure, from public network access and unrotated keys to missing encryption, exposed services, and logging gaps. Misconfiguration is consistently ranked as one of the top threats to cloud environments, and CISA now mandates baseline cloud configuration practices for US federal agencies.

For most organizations, this is not a single-provider problem. More than two-thirds of midmarket organizations operate multi-cloud environments, and this inherently makes security more complicated. Adding to the complexity is the fact that each provider handles security differently: the same issues can be surfaced in different ways, described using different terminology, and require a different fix depending on the platform.

This report looks at how cloud security risk differs across AWS, Azure, and Google Cloud, based on misconfiguration data from 3,000 organizations, including:

- The most common misconfigurations on each platform
- How risk profiles differ between providers
- How cloud security posture varies by organization size
- How quickly teams remediate what they find

Based on anonymized data from Intruder customers covering the 12 months to July 2026

Top 10 misconfigurations in AWS

Percentages represent the proportion of AWS accounts affected by at least one issue in the past 12 months.

1	S3 Does Not Enforce HTTPS	87%
2	Permissive Ingress to Sensitive Ports (via ACL)	84%
3	Overly Permissive Network ACL	83%
4	IAM Policy Allows Privilege Escalation	83%
5	VPC Endpoint Not Enabled for EC2	82%
6	Block Public Access Not Enabled (S3 Account Level)	81%
7	VPC Subnet Auto-Assigns Public IP	72%
8	Root Access Not Centrally Managed	72%
9	IAM Policy Attached To User	71%
10	IAM Access Key Not Rotated	71%

S3 Does Not Enforce HTTPS tops the list at 87%. S3 buckets are one of the most widely used cloud storage services, and while man-in-the-middle attacks are rare, it's worth ensuring plain HTTP can't be used.

Permissive firewall weaknesses rank second and third. These may not expose dangerous services today, but tightly scoped firewalls ensure that development work can't easily introduce an exposure tomorrow.

IAM Policy Allows Privilege Escalation ranks fourth. AWS IAM is notoriously complex, and managed policies that appear safe can grant broader permissions than intended.

In one recent incident, an attacker moved from exposed credentials to administrative privileges in under 10 minutes, compromising 19 AWS principals.

Top 10 misconfigurations in Azure

Percentages represent the proportion of Azure accounts affected by at least one issue in the past 12 months.

1	Storage Account Key Rotation Not Enabled	67%
2	Storage Account Access Keys Enabled	66%
3	Storage Account Public Network Access Enabled	61%
4	Entra User Without MFA	55%
5	Trusted Launch Not Enabled	45%
6	Key Vault Secret Never Expires	41%
7	Disable Public Access Not Enabled (Key Vault)	41%
8	Key Vault Not Recoverable	38%
9	Storage Blob Public Access Enabled	36%
10	Key Vault Using Legacy Access Control Model	34%

The top three issues all relate to Azure Storage Accounts, which often house sensitive data like customer personally identifiable information (PII). All three affect a similar proportion of Azure accounts—between 61% and 67%—which may suggest that where storage accounts aren't hardened, multiple controls tend to be missing.

More than half of accounts have Entra users without multi-factor authentication (MFA), which is significant since Entra ID governs access beyond just cloud resources, such as Microsoft 365, third-party SaaS apps, and on-premises systems. The 2024 Midnight Blizzard breach of Microsoft's own network began with a password spray attack against a legacy test account without MFA.

Top 10 misconfigurations in Google Cloud

Percentages represent the proportion of Google Cloud accounts affected by at least one issue in the past 12 months.

1	OS Login MFA Not Enabled	77%
2	OS Login Not Enabled	76%
3	Unused Service Account	75%
4	Overly Permissive Service Account	53%
5	Permissive Ingress to Sensitive Ports	34%
6	Service Account Key Not Rotated	31%
7	Default Network In Use	29%
8	Service Account Unused Key	29%
9	Block Project-Wide SSH Keys Not Enabled	26%
10	Shielded VM Not Enabled	21%

Identity and access management (IAM) issues dominate the top four spots, with more than three-quarters of Google Cloud accounts missing OS Login controls, which provide a more secure alternative to traditional SSH.

The rest of the top 10 is split between permissive firewalls, IAM attack surface bloat from unused or unrotated keys, and missing hardening measures for cloud compute. Their prevalence suggests many Google Cloud environments are still running a default configuration.

How do AWS, Azure, and Google Cloud compare?

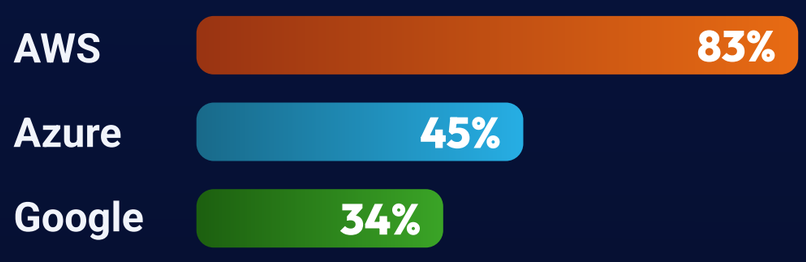
We grouped cloud issues into six categories—weak IAM controls, missing logging and alerting, misconfigured services, permissive firewalls, exposed services, and weak encryption—and compared prevalence across the three providers.

Weak IAM controls

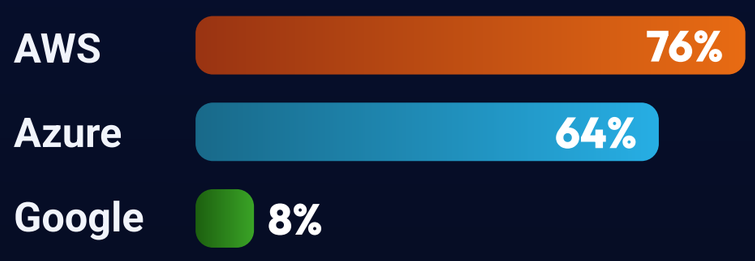
Missing logging and alerting

Misconfigured services

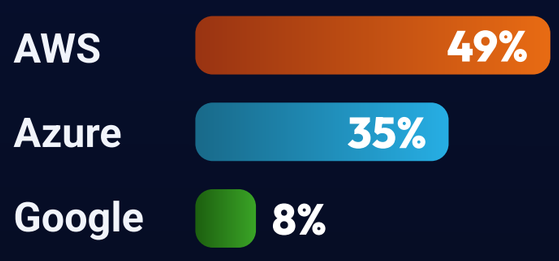
Permissive firewalls



Exposed services



Weak encryption



The pattern suggests that the breadth of a provider's service offering directly correlates with misconfiguration risk. AWS leads in prevalence across five of the six categories. As the largest cloud provider by range of services, it offers the most configuration options, and with that the most opportunities for misconfiguration. Google Cloud has the lowest prevalence across four categories and also offers the fewest services.

Weak IAM controls and missing logging and alerting affect 80–98% of accounts across all three providers. Getting these right is time-intensive and expensive. IAM requires constant management, and at larger organizations it can require dedicated headcount. Even small changes to an environment can reintroduce weaknesses.

The biggest gap across the major cloud providers is exposed services, which affect 76% of accounts on AWS, compared with 64% on Azure and just 8% on Google Cloud. Permissive firewalls and weak encryption follow a similar pattern, with AWS highest and Google Cloud lowest in both.

Beyond having a smaller service catalogue, Google Cloud also takes a different approach to shared responsibility, with what it calls a ‘Shared Fate' model that includes more secure default configurations out of the box. On the other hand, independent assessments have found that AWS places more responsibility on users to implement secure settings, which may explain its higher prevalence of misconfigurations.

Cloud security posture by organization size

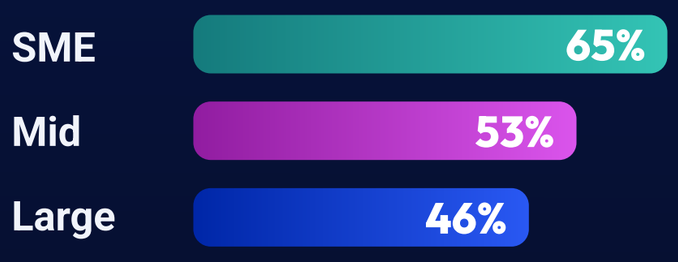
Percentage of organizations with at least one issue per category, comparing SMEs (1–250 employees), midmarket organizations (251–10K employees), and large enterprises (10K–100K+ employees).

Weak IAM controls

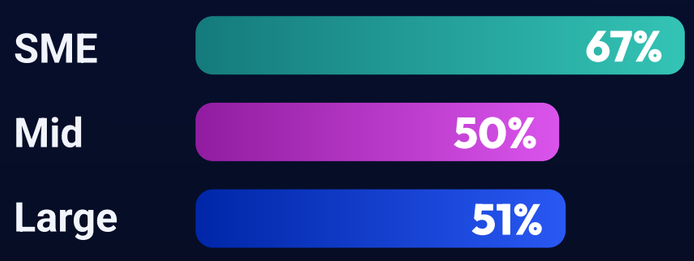
Missing Logging and alerting

Misconfigured services

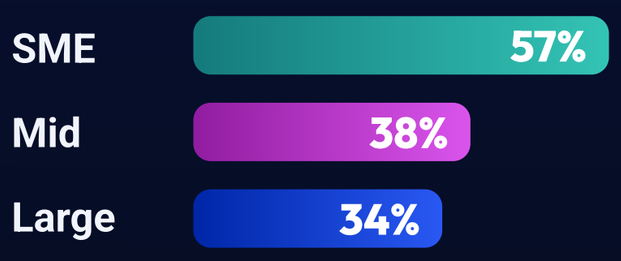
Permissive firewalls



Exposed services



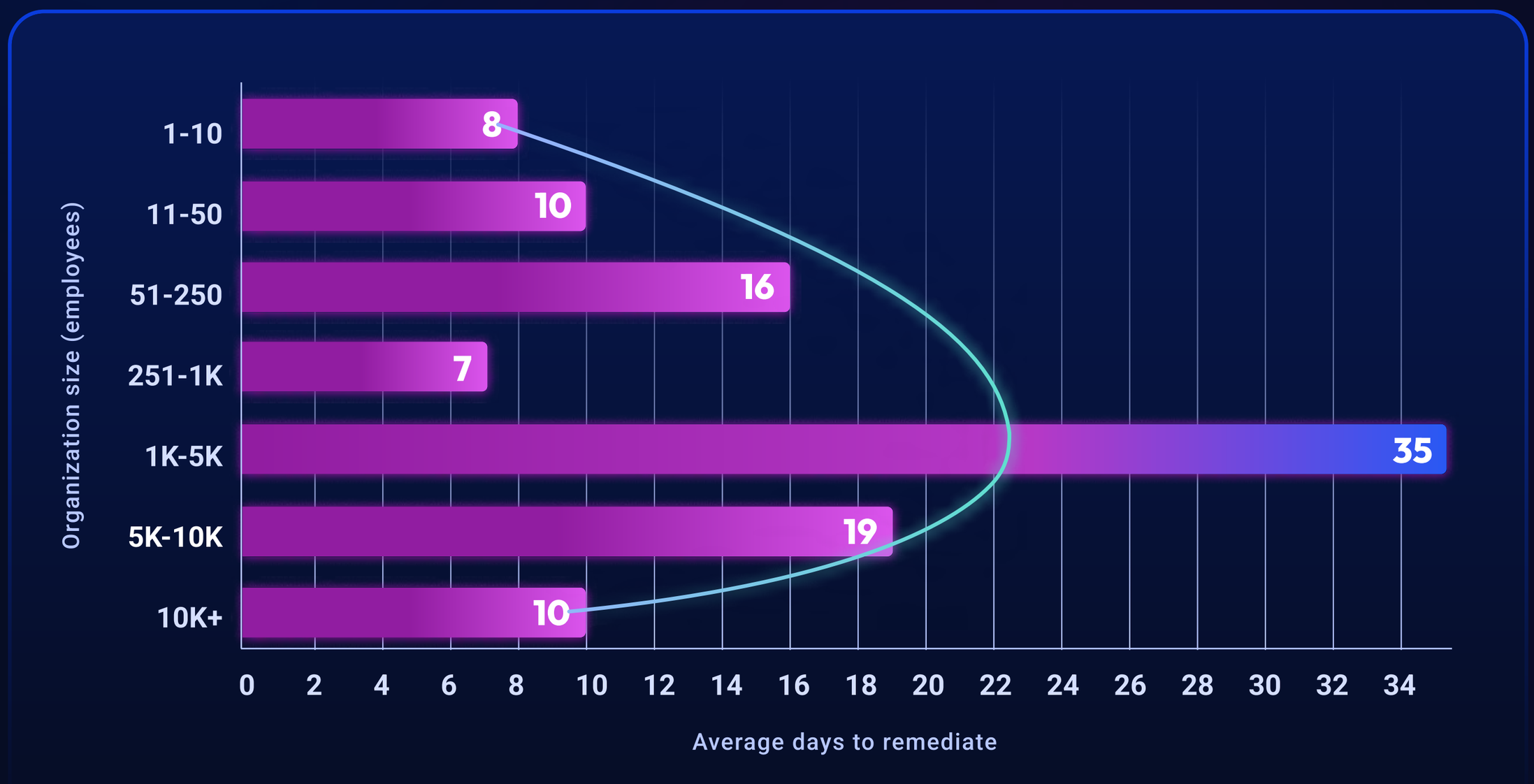
Weak encryption



As organizations grow, cloud security posture generally improves. Larger enterprises are less likely to have permissive firewalls, exposed services, or weak encryption than their smaller counterparts, which points to increasing security maturity, investment, and operational discipline.

The exception is IAM, which weakens as organizations scale: 87% among SMEs, 95% among midmarket, and 98% among large enterprises. More people means more roles, more permissions, and more complexity—and a single overprivileged identity is often all it takes to bypass the controls that have been hardened elsewhere.

Average days to remediate cloud issues by organization size



Smaller organizations remediate cloud issues fastest, averaging 8–16 days. As organizations grow into the 1,000–5,000 employee range, remediation slows significantly, peaking at 35 days. Remediation times improve again at the largest sizes, with 10K+ organizations back down to 10 days.

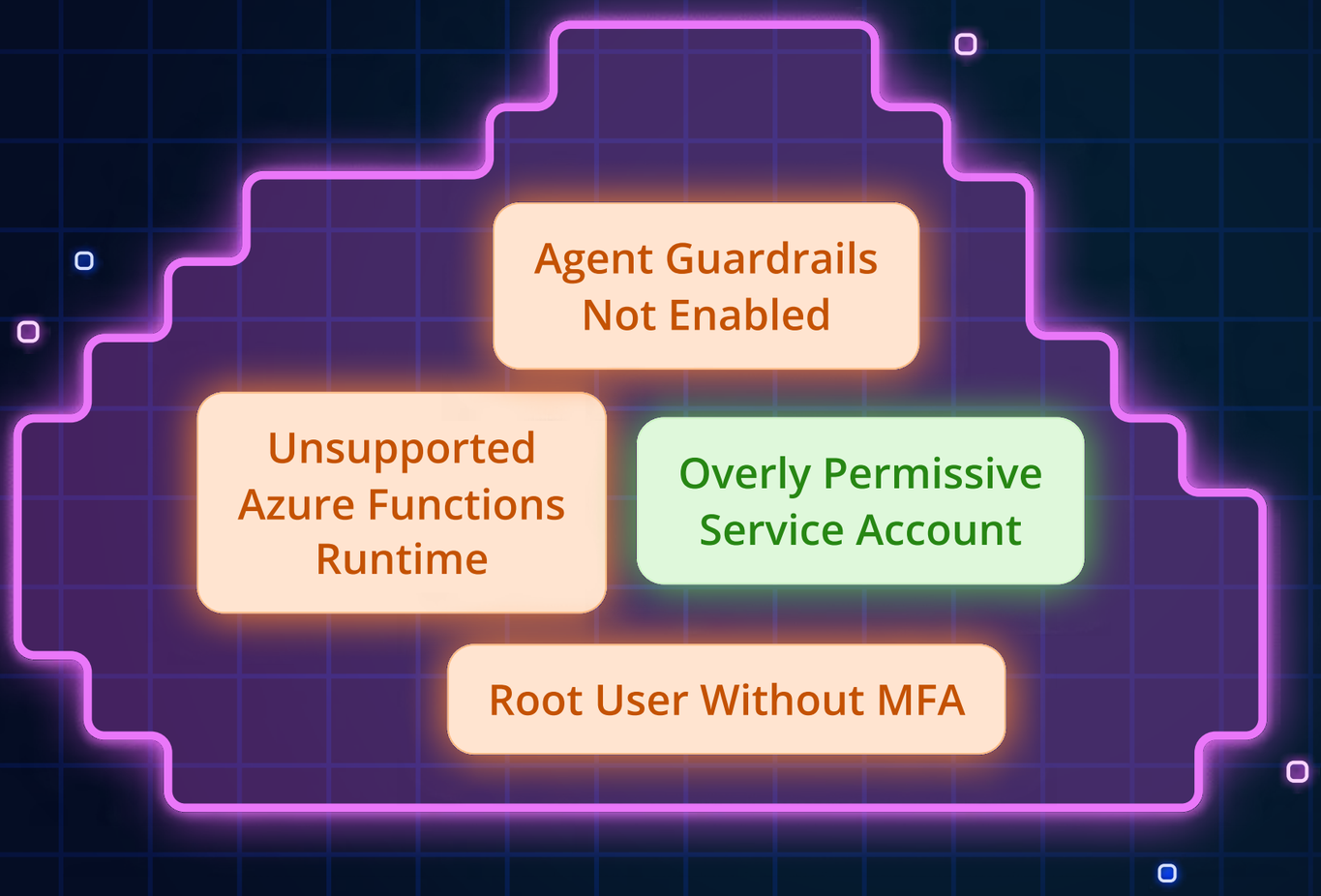
This mirrors the pattern seen in our 2026 Attack Surface Management Index: midmarket organizations face the longest remediation times, likely managing enterprise-level cloud complexity without the dedicated resources to match.

What this means for security teams

The top misconfigurations on AWS, Azure, and Google Cloud have very little overlap. AWS shows the broadest spread of issues, Azure is dominated by storage and key management issues, and Google Cloud's primary challenge is IAM. For teams managing multiple providers, the hard part is not just fixing different issues across different platforms. It's understanding which risks matter most across the whole estate, so limited time and resources go to the right places first.

Risk also changes as organizations grow. Smaller organizations tend to remediate faster, while midmarket teams face some of the longest remediation times and highest rates of misconfigured services. This suggests that many organizations are scaling their cloud usage before they have the dedicated resources, processes, or visibility to secure it efficiently.

Security teams need a consistent way to assess posture across providers, while preserving the platform-specific detail needed to remediate effectively. Otherwise, they are left with too much complexity, too little visibility, and not enough context to prioritize what matters most.



About Intruder

Intruder's continuous exposure management platform helps security, IT, and engineering teams stop breaches before they start. By unifying AI penetration testing, attack surface monitoring, cloud security, and vulnerability management in one intuitive platform, Intruder gives stretched teams an always-on security source of truth. Our approach focuses on continuous automated scanning using expertise and agentic solutions to ensure that the findings we deliver are accurate, prioritized by real-world risk, and ready to act on.

Founded in 2015 by Chris Wallis, a former ethical hacker turned corporate blue teamer, Intruder is now protecting over 3,000 companies worldwide. Intruder has been awarded multiple accolades, was selected for GCHQ's Cyber Accelerator, included on Deloitte's Tech Fast 50 2023 list as the fastest-growing cybersecurity company in the UK and was named in G2's 2026 Best Software Awards.

Get started for free or book a call with one of our experts at intruder.io

Read our reviews on G2.com