Recorded Future®

RISK INSIGHTS SUMMARY | FEB 2026

2025 Cloud Threat Hunting and Defense Landscape

From Insikt Group®

Full Report Link

Threats to the cloud — shared, scalable infrastructure of remote data storage and compute — are becoming easier to carry out. This is driven by an increasingly interconnected environment and the rising trend of credential abuse.

Threat actors use stolen credentials to access your cloud: Threat actors are using stolen usernames and passwords to gain access to one cloud environment, from which they can access other, more sensitive environments.

Third-party tools are the new backdoor: Hackers are taking advantage of security weaknesses in third-party tools to bypass defenses in more secure environments.

Less effort is needed to pull off high-impact attacks: Cloud abuse, exploitation of misconfigured environments, and credential abuse have all gotten easier for even low-level threat actors to achieve.

What's Driving the Trends

92%	**Percent of companies using multi-cloud solutions** *Increased cloud complexity and need for interoperability increases attack surface*
1,295	**Number of cloud services the average company uses** *Increased opportunity for third-party exploits*
60%	**Percent of business data stored in cloud** *Increased motivation for threat actors to target the cloud*

Malicious Tactics in the Cloud

Living-off-the-cloud
Using native tools and functions, not malware, to compromise cloud environments

Logging in, not breaking in
Using of valid credentials provides initial access

Registering their own tools
Using legitimate cloud services to set up malicious infrastructure

Outlook

Third party compromise will become increasingly prevalent and more technically sophisticated.

Ransomware involving **data theft and seizure of cloud processes** will become more common as criminals take advantage of cloud growth.

AI-enabled cloud management tools will provide new avenues for exploitations, such as **malicious prompts.**

Mitigations

- ❏ **Do we have visibility into our third-party integrations?**
- ❏ **Are we monitoring leaked credentials and implementing MFA everywhere?**
- ❏ **Are we implementing zero trust — specifically the principle of least privilege — for managing data access and account configuration?**