CROWDSTRIKE

Top Cloud Attack Techniques

And how to defend against them

The cloud is an ever-growing, ever-evolving attack surface. Defending this environment against increasing cloud attacks requires deep knowledge of threat actor activity. Here are the top three attack trends in the cloud as observed by CrowdStrike and how to defend against them.

Threat actors are increasingly targeting the cloud

Cloud environments continue to grow:

41.4% of cloud leaders say they are increasing their use of cloud-based services and products[1]

33.4% are planning to migrate from legacy enterprise software to cloud-based tools[1]

32.8% are migrating on-premises workloads to the cloud[1]

And threat actors have taken notice.

In 2022, CrowdStrike observed:

95% increase in cloud exploitation cases

3x the number of cases involving cloud-conscious actors

71% of attacks were malware-free

Why target cloud environments?

Multi-cloud environments are complex and therefore more difficult to protect

Rapid software delivery processes make cloud-native apps susceptible to vulnerabilities and misconfigurations

Rogue and shadow cloud environments lack security controls and oversight

Siloed security point products leave blind spots adversaries can slip through unnoticed

Threat actors are cloud-savvy and refine their tactics to abuse cloud services and exploit cloud vulnerabilities. Here are the top three cloud attack techniques observed by the CrowdStrike Threat Intelligence team over the past year while tracking 200+ threat actors.

Lateral movement across IT infrastructure

Threat actors are increasingly leveraging traditional endpoints to pivot to cloud infrastructure — and vice versa: Cloud infrastructure is being used as a gateway to access endpoints. Organizations rarely have the visibility they need to stop this activity, having acquired numerous point solutions to address the on-premises environment, and more recently to address cloud environments.

To stop lateral movement, organizations need full visibility across the entire IT infrastructure, both on-premises and in the cloud.

Cloud misconfigurations leading to breaches

CrowdStrike consistently investigates cloud breaches that could have been detected earlier or prevented if cloud security settings had been correctly configured. Misconfigurations not only increase the risk of a breach, they also continue to become more prevalent and problematic as organizations expand their cloud infrastructure.

#1 vulnerability in cloud environments

60% of containers CrowdStrike observed lacked properly configured security protections

36% of cloud environments had insecure cloud service provider default settings

Cloud identities as the new perimeter

As the new perimeter, identity has become the keys to the kingdom. Threat actors focus less on deactivating antivirus and firewall technologies and more on modifying authentication processes and attacking identities. The continued adoption of cloud-based applications and services increases the number of identities an adversary can target and use to their advantage.

Legitimate user accounts were used to gain initial access in **43%** of cloud intrusions

47% of critical misconfigurations in the cloud **are related to poor identity and entitlement hygiene**

In **67%** of cloud security incidents, **CrowdStrike found identity and access management roles with elevated privileges beyond what was required — indicating an adversary may have subverted the role to compromise the environment and move laterally**

CrowdStrike for Cloud Security

As cloud environments continue to grow, so will the attacks against them. It's impossible to catch every cloud vulnerability, misconfiguration and user error — let alone understand all of the evolving tactics, tools and procedures used by threat actors. Organizations cannot do it alone — they need a partner who is deeply knowledgeable on threat actor behavior and cloud.

As the #1 agent-based endpoint detection and response provider in the world, CrowdStrike has taken a visionary approach to designing scalable and effective cloud security that can be deployed and managed easily in a single platform. CrowdStrike Falcon® Cloud Security was built from the ground up to deliver both agentless and agent-based protection. Organizations can simply turn it on and extend protection from their endpoints to their cloud, covering their whole IT infrastructure with seamless, unified protection. Falcon Cloud Security brings together cloud security posture management, cloud workload protection and cloud identity entitlement management as a fully integrated cloud-native application protection platform (CNAPP) offering.

Download the white paper, Insider's Guide to Defending the Cloud. Learn More →

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Follow us:

CROWDSTRIKE

[1] https://cloud.google.com/blog/transform/top-cloud-computing-trends-facts-statistics-2023