Cloud Security

CROWDSTRIKE

White Paper

Insider's Guide to Defending the Cloud

Introduction

Organizations are increasingly moving to the cloud, and their attack surface grows with every bucket, container and service deployed. And as the cloud expands, so does the number of cloud-based attacks.

It's no surprise that attackers go where the data goes. However, the cloud is a uniquely difficult environment to protect. The cloud's complexity, along with its dynamic and ephemeral nature, make it ripe for threat actors to leverage proven and innovative attack techniques. In addition, many cloud environments are largely unsupervised, as organizations lack the visibility and controls required to detect and stop malicious activity.

Addressing cloud risk requires deep knowledge into threat actor activity. To effectively automate prevention and execute accurate, rapid investigation and response, organizations need a complete understanding of adversary tactics, tools and procedures (TTPs) in the cloud.

This paper highlights the top three attack trends in the cloud and offers five best practices for protecting your cloud environment.

CrowdStrike observed a

95%

increase in cloud exploitation from 2021 to 2022. Now is the time to protect your cloud and your business.

Source: CrowdStrike 2023 Cloud Risk Report

The Current State of the Cloud

For many modern businesses, the public cloud has become a mission-critical asset. Having accelerated their digital transformation initiatives during the COVID-19 pandemic, these organizations show no sign of slowing down — and neither does cloud growth. According to the Google Cloud Brand Pulse Survey, Q2 2022, more than 40% of cloud leaders say they are increasing their use of cloud-based services and products (41.4%). In addition, 33.4% are planning to migrate from legacy enterprise software to cloud-based tools, and 32.8% are migrating on-premises workloads to the cloud. As a result, organizations are managing complex multi-cloud environments (some of which were likely deployed during business duress) that today host business-critical applications and data.

Meanwhile, as the cloud grows, so does the attack surface. The CrowdStrike 2023 Global Threat Report predicts cloud exploitation will increase as more businesses move operations to cloud environments and more adversaries become "cloud-conscious" — a term referring to threat actors that are aware of the potential to compromise cloud workloads and seek ways to abuse features unique to the cloud. From 2021 to 2022, cloud exploitation increased as expected and cases involving cloud-conscious actors nearly tripled from 2021.

This increase in cloud exploitations is due to several factors, some related to the nature of the cloud itself. Cloud providers make it easy for developers to experiment with new services and quickly push successful projects to production. However, the desire to move quickly using agile processes and continuous delivery can make cloud-native applications susceptible to vulnerabilities and misconfigurations. Similarly, the ease with which users can get started in the cloud leads to "rogue" and shadow cloud environments. Like shadow IT, these environments are spun up outside of the security team's purview. They lack governance and are deployed with minimal or no security controls, putting these cloud environments at greater risk of exploitation.

The security controls organizations do have in the cloud offer limited protection. Cloud security approaches are built on siloed point products that leave blind spots adversaries can slip through. An agentless solution, for example, uses out-of-band technology that relies on snapshots taken every 24 hours. While it's an effective tool for asset visibility where deploying an agent isn't viable, these solutions lack the critical ability to see between the shadows of their 24-hour cycles.

Meanwhile, threat actors are doing their own research and development in the cloud. They have a deep understanding of cloud infrastructure and continue to refine their tactics to abuse cloud services and exploit cloud vulnerabilities. Some of these threat actors are highly sophisticated, with access to plenty of resources to fund their efforts. In fact, the growth of cloud exploitation indicates a larger trend of eCrime and nation-state actors adopting knowledge and tradecraft to increasingly exploit cloud environments.

Defending against cloud-savvy threat actors requires an understanding of the motivations, strategies and techniques they use to infiltrate the cloud. As technology evolves, adversary tradecraft is becoming more sophisticated, exploiting vulnerabilities and today's fragmented security environment. Here are the top three cloud attack techniques observed by the CrowdStrike Intelligence team in 2022 while tracking 200+ threat actors:

- **Lateral movement across IT infrastructure**
- **Cloud misconfigurations leading to a breach**
- **Cloud identities as the new access point**

71%

of attacks in the cloud observed by CrowdStrike were malware-free.

Source: CrowdStrike 2023 Global Threat Report

Lateral Movement across IT Infrastructure

While organizations are increasingly moving workloads to the cloud, they aren't eliminating their on-premises infrastructure. These servers and workstations can provide a toehold for threat actors to access the cloud. CrowdStrike has observed adversaries growing more confident leveraging traditional endpoints to pivot to cloud infrastructure. The reverse is also true: Cloud infrastructure is being used as a gateway to access traditional endpoints.

Lateral Movement Enabled by a Vulnerability

CVE-2022-29464 is a critical vulnerability that affects multiple WS02 products. Successful exploitation of the vulnerability enables remote code execution and unrestricted file uploads. Exploit code was made publicly available the day the vulnerability was disclosed. CrowdStrike® Falcon OverWatch™ threat hunters began identifying multiple exploitation incidents in which adversaries used tools, infrastructure and TTPs consistent with China-nexus activity.

To stop lateral movement, organizations need full visibility across the entire IT infrastructure, both on-premises and in the cloud. However, organizations rarely have this visibility, as they have often acquired numerous point solutions to address the on-premises environment, and more recently, cloud environments. When cobbled together, these siloed tools provide a fragmented, point-in-time view of the IT infrastructure.

Cloud Misconfigurations Leading to a Breach

Misconfigurations are the number one vulnerability in cloud environments. A cloud misconfiguration is a poorly chosen, incorrect or absent security setting that exposes the cloud environment to risk. Misconfigured access policies and security settings are often missed during security audits, and it only takes one misconfiguration to increase the likelihood of a breach. CrowdStrike is consistently called in to investigate cloud breaches that could have been detected earlier or prevented if cloud security settings had been correctly configured.

Common Cloud Misconfigurations

Unrestricted outbound access: Unrestricted outbound access to the internet allows bad actors to take advantage of the lack of restrictions and workload protection to exfiltrate data from cloud platforms. Cloud instances should be restricted to specific IP addresses and services to prevent adversaries from accessing and exfiltrating data.

Disabled logging: Effective logging of cloud security events is imperative for the detection of malicious behavior, but logging is often disabled on cloud platforms to reduce maintenance overhead. If logging is disabled, there is no record of events and no means of detecting potentially malicious actions. Logging should be enabled and managed as a best practice.

Misconfigurations not only increase the risk of a breach, they also continue to become more prevalent and problematic as organizations expand their cloud infrastructure. Cloud service providers continually update and roll out new platforms and services that are easy to get started with but not necessarily straightforward when it comes to checking all of the right boxes. And organizations often lack governance over cloud adoption and use, which is needed to establish internal configuration standards. Teams also lack monitoring capabilities, which are necessary to detect malicious activity — a potential indication of a misconfiguration — in a timely manner.

60%

of containers CrowdStrike observed lacked properly configured security protections.

Source: CrowdStrike 2023 Cloud Risk Report

36%

of cloud environments had insecure cloud service provider default settings.

Source: CrowdStrike 2023 Cloud Risk Report

Cloud Identities as the New Access Point

In the cloud, identity is both the perimeter and a key access point — for both cloud users and threat actors. Threat actors are becoming more reliant on legitimate user accounts, which were used to gain initial access in 43% of cloud intrusions CrowdStrike observed from January 2022 to February 2023. As further proof that identity is usurping the firewall as the new perimeter, CrowdStrike observed threat actors focus less on deactivating antivirus and firewall technologies for defense evasion and more on modifying authentication processes and attacking identities. In addition, more threat actors were seen moving toward cloud account discovery as opposed to cloud infrastructure discovery. They were also identified using valid higher-privileged accounts for privilege escalation.

Nearly half (47%)

of critical misconfigurations in the cloud were related to poor identity and entitlement hygiene.

Source: CrowdStrike 2023 Cloud Risk Report

In 67% of cloud security incidents,

CrowdStrike found identity and access management (IAM) roles with elevated privileges beyond what was required — indicating an adversary may have subverted the role to compromise the environment and move laterally.

Source: CrowdStrike 2023 Cloud Risk Report

Identity and access management have long been a challenge for organizations. With the move to the cloud, identity protection must become a priority. As the new perimeter, identities have become the keys to the kingdom. The continued adoption of cloud-based applications and services increases the number of identities an adversary can target and use to their advantage. Threat actors will likely continue to seek opportunities to use valid identities to log in, move laterally and achieve their goals. The identity threat is pervasive, affecting all major cloud providers and many smaller ones across customers of all sizes and industries.

Publishing Access Key Credentials to GitHub

In November 2022, a victim organization in a CrowdStrike Services case accidentally published its cloud provider root account's access key credentials to GitHub. Within seconds, automated scanners and multiple actors attempted to use the compromised credentials. CrowdStrike Services observed an actor establish persistence to the victim by enabling single sign-on (SSO) for the cloud service provider, then adding an identity provider for SSO. Had the activity gone undetected, such persistence via an identity provider would continue to grant access to the organization's accounts — even after credentials and access keys of the IAM users in these accounts have been rotated or revoked.

Requirements for a Cloud Security Solution

To reduce cloud security risk, organizations need a security solution that can stop active cloud breaches and shut down misconfigurations, accidental exposure, and human error. This requires a **unified platform** that spans both the on-premises and cloud computing environments to provide continuous visibility, protection and response across runtime and agentless capabilities. To stop threats in real time, the platform must leverage both **agent-based and agentless** technologies as well as **high-fidelity threat intelligence** about cloud adversaries to inform and accelerate security operations with the right content, at the right time, natively within the security platform. Finally, **managed detection and response (MDR) and threat hunting services** round out a comprehensive solution to help ensure **better outcomes.**

Compare
CrowdStrike vs. the competition

Top 5 Best Practices for Protecting Cloud

Prioritize cloud identity protection
Why: Adversaries use cloud identities as their front door into cloud environments.

Recommendation: Consider leveraging identity security tools built into cloud-native application protection platform (CNAPP) products, and audit and remove old users/old credentials with account access.

Gain visibility into security gaps
Why: Cloud misconfigurations put organizations at risk of data loss.

Recommendation: Leverage visibility and real-time insights to spot misconfigurations before they become a problem. Internal and external application security testing can also provide insight into potentially dangerous vulnerabilities and misconfigurations.

Employ real-time monitoring and visibility
Why: Without continuous detection, threats can slip under the radar.

Recommendation: Deploy continuous monitoring across cloud and endpoint systems to identify and address potential threats in real time. Ensure your monitoring profile aligns with organizational and technical constraints, ensure the most important metrics and events are included in the monitoring scope, and choose the most effective monitoring software.

Ensure timely patching
Why: Cloud assets must be updated and configured to create the strongest defense against adversaries.

Recommendation: Regularly update software in the cloud environment to ensure vulnerabilities are patched in a timely manner, and conduct regular assessments of hosted applications to identify flaws in application design and implementation. Special care should be taken to patch known remote code execution and server-side request forgery (SSRF) vulnerabilities in public-facing applications running in the cloud.

Watch for unusual behavior in real time
Why: Visibility into cloud workloads and container events is critical to reduce the mean time to detect and respond to an attacker.

Recommendation: Monitor for suspicious activity, including newly created cloud instances and cloud accounts, newly added credentials or multifactor authentication (MFA) factors, changed firewall rules, access to cloud resources by new or unexpected entities, and the disabling of MFA through configuration changes. Any of these behaviors may indicate an intruder in the cloud.

CrowdStrike for Cloud Security

IT environments are growing increasingly larger and more complex, providing threat actors with a vast attack surface. It's impossible to catch every cloud vulnerability, misconfiguration and user error, let alone understand the evolving TTPs used by threat actors. Organizations may struggle doing it alone. They may need a partner who is deeply knowledgeable on threat actor behavior and cloud.

As a cybersecurity leader recognized by multiple independent testing organizations and third-party analyst firms, 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 entire IT infrastructure with seamless and unified agentless and agent-based protection. Falcon Cloud Security brings together cloud security posture management, cloud workload protection and cloud identity entitlement management as a fully integrated CNAPP offering.

Understand how to protect your cloud environment, and receive customized insights to operationalize best practices for cloud security.

Learn more

Follow us:

- **Blog ›**
- **Twitter ›**
- **LinkedIn ›**
- **Facebook ›**
- **Instagram ›**

Start a free trial today

Get a CrowdStrike Cloud Security Risk Review →

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.