CROWDSTRIKE

White Paper

Insider's Playbook: Defending Against Cloud Threats

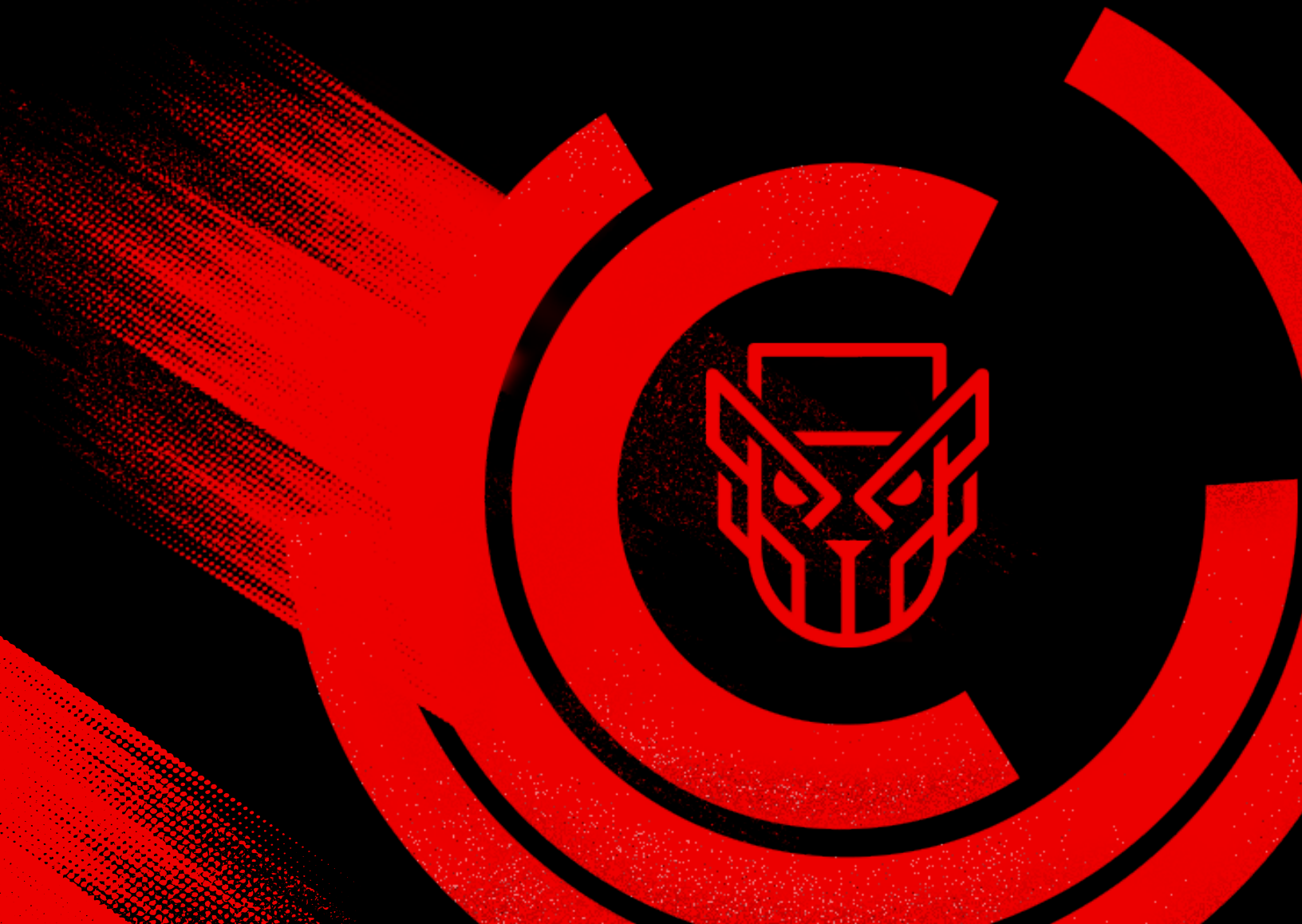


Table of Contents

Introduction 3
The Current State of the Cloud 3
- Cloud Is Becoming a Focus Area for BGH Adversaries 5
- Identity Continues to Be a Key Cloud Access Point 5
- Siloed DevOps and Security Practices Drive Cloud Risk 6

Requirements for a Cloud Security Solution 6
Building a Modern Cloud Security Program: A Playbook 7
CrowdStrike for Cloud Security 8
About CrowdStrike 8

Introduction

The accelerated velocity of development from the increased adoption of cloud technologies is unprecedented — making reactive crisis management more and more expensive. In fact, the Puppet 2024 State of DevOps Report found that a huge indicator for success in cloud environments is when a strong security posture and developer productivity work in harmony.

However, the cloud environment is uniquely difficult to protect. The cloud's complexity, along with its dynamic and ephemeral nature, allows attackers to hide in the blind spots, a problem that continues to grow as organizations increasingly adopt multiple cloud infrastructure providers. And due to the rapid pace of innovation, many impactful security risks are ignored or not fixed in time.

Cloud-based attacks will continue to accelerate, and it's crucial that organizations are aware of what they are up against. Addressing cloud risk requires understanding which cloud risks are the most targeted and developing a strong program to help SecOps and DevOps teams effectively collaborate.

This paper highlights the latest cloud-based attack trends and offers five cloud strategies for hardening and protecting your cloud environment.

The Current State of the Cloud

Organizations are constantly moving to the cloud. Many of them are finding themselves in hybrid or multi-cloud environments, leading to a surge in complexity. For many modern businesses, the public cloud processes customer data and powers all of their revenue-generating applications due to its scalability, simplified management and ability to increase business agility. "By 2028, cloud computing will shift from being a technology disruptor to becoming a necessary component for maintaining business competitiveness," according to Gartner, Inc.[1] Meanwhile, as cloud adoption grows, so does the attack surface — especially in hybrid and multi-cloud environments. The CrowdStrike 2024 Global Threat Report revealed that cloud-conscious cases — those involving threat actors that are aware of the ability to compromise cloud workloads and use this knowledge to abuse features unique to the cloud — increased by 110% from 2022 to 2023. The report also found that the modern threat landscape includes widespread use of "interactive intrusion" techniques, which involve adversaries actively executing actions on a host instead of leveraging malicious tooling and scripts. Since cloud environments are dynamic and difficult to centrally monitor, it becomes even harder to know the difference between expected behavior and a hands-on attack.

CrowdStrike observed a

75%

increase in cloud environment intrusions from 2022 to 2023.[2] Now is the time to protect your cloud and business.

1 Gartner® Press Release, "Gartner Says Cloud Will Become a Business Necessity by 2028," November 29, 2023

2 CrowdStrike 2024 Global Threat Report

The 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 projects to production. However, the desire to move quickly using agile processes and continuous delivery leads to more vulnerabilities and misconfigurations getting deployed to production. Additionally, the need for organizations to stay competitive and innovate at an unprecedented pace means that new features are often prioritized over vulnerability patches. 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 and lack any sort of governance or security controls.

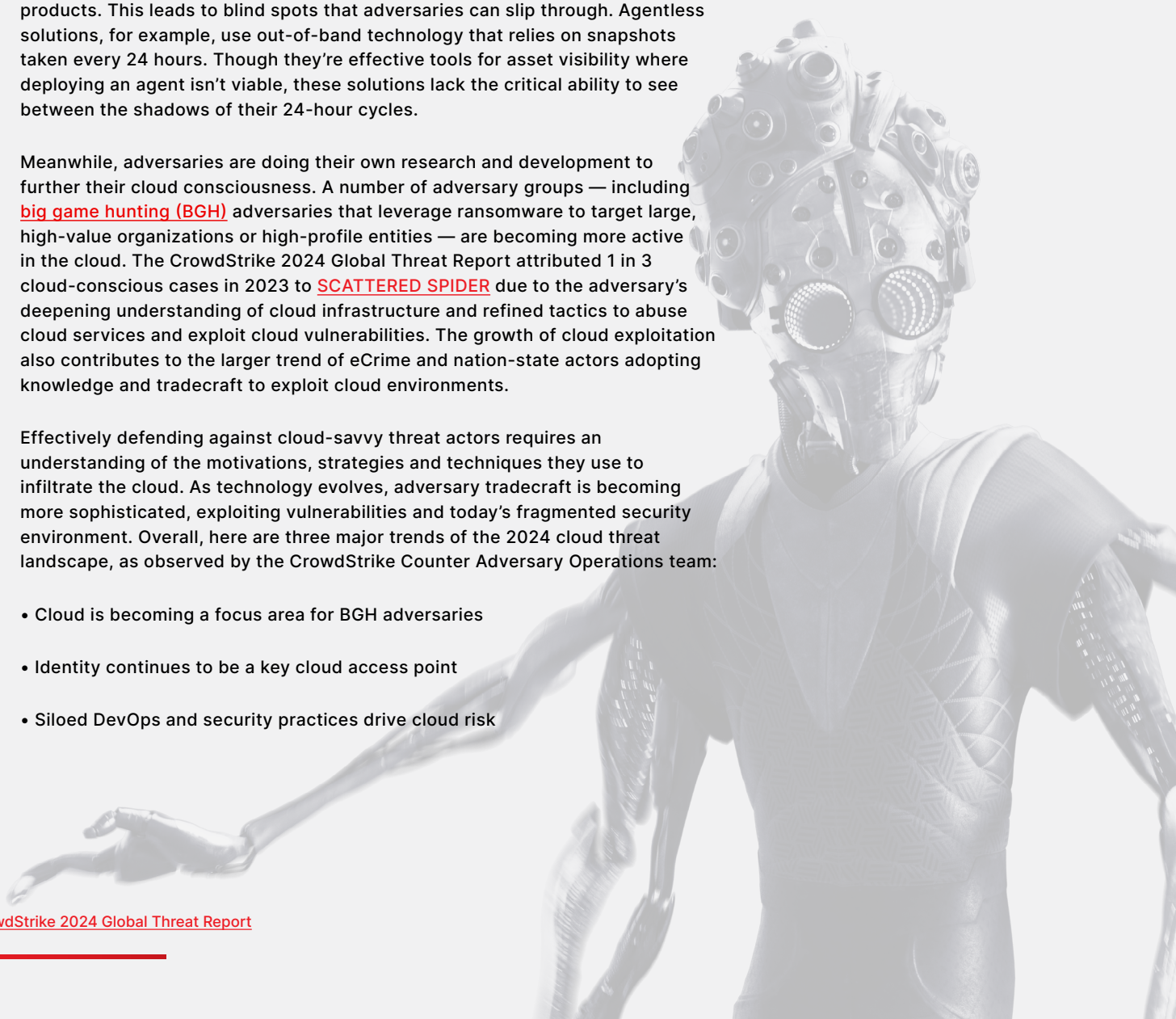
The most intriguing part of the dramatic increase in cloud exploitation is that there is no shortage of cloud security tooling in the market — cloud security emerged as a concept over 15 years ago. So why is cloud security still a growing challenge for many organizations? Today's cloud security tools are very bespoke, forcing organizations to build their cloud security programs on siloed point products. This leads to blind spots that adversaries can slip through. Agentless solutions, for example, use out-of-band technology that relies on snapshots taken every 24 hours. Though they're effective tools 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, adversaries are doing their own research and development to further their cloud consciousness. A number of adversary groups — including big game hunting (BGH) adversaries that leverage ransomware to target large, high-value organizations or high-profile entities — are becoming more active in the cloud. The CrowdStrike 2024 Global Threat Report attributed 1 in 3 cloud-conscious cases in 2023 to SCATTERED SPIDER due to the adversary's deepening understanding of cloud infrastructure and refined tactics to abuse cloud services and exploit cloud vulnerabilities. The growth of cloud exploitation also contributes to the larger trend of eCrime and nation-state actors adopting knowledge and tradecraft to exploit cloud environments.

Effectively 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. Overall, here are three major trends of the 2024 cloud threat landscape, as observed by the CrowdStrike Counter Adversary Operations team:

- Cloud is becoming a focus area for BGH adversaries
- Identity continues to be a key cloud access point
- Siloed DevOps and security practices drive cloud risk

84% of adversary-attributed cloud-conscious intrusions were focused on eCrime[3]



3 CrowdStrike 2024 Global Threat Report

Cloud Is Becoming a Focus Area for BGH Adversaries

Traditional BGH adversaries, such as INDRIK SPIDER, are becoming more cloud-conscious — a concerning trend since these adversaries tend to be the most sophisticated types of attackers. The cloud has proven to be ripe with attack vectors. Various adversaries have leveraged its vulnerabilities to advance their attacks, from gaining initial access to moving laterally and exfiltrating data.

To ensure BGH adversaries aren't able to execute on a successful breach, organizations need full visibility across their entire IT infrastructure with a unified solution that includes runtime cloud attack defense and proactive threat disruption. Since organizations typically have to rely on disjointed point solutions (especially those that don't have access to live threat intelligence feeds), there are many blind spots where attackers can hide.

Identity Continues to Be a Key Cloud Access Point

Since the cloud has done away with physical perimeters, identity has become the key to accessing cloud resources. Attackers typically can't do too much damage without obtaining privileged access to a system, so many of their tactics have an end goal of exploiting identity risk. CrowdStrike has observed adversaries relying heavily on valid credentials to achieve initial access into cloud environments — as well as identity providers — to establish persistence. For example, FANCY BEAR and SCATTERED SPIDER commonly targeted Microsoft 365 credentials via credential-phishing attacks.

Since cloud identities are of extremely high risk, organizations must have visibility into identity-related risks and exposure across their entire software development life cycle (SDLC). It's crucial to review configurations ahead of deployment to ensure accounts and resources are given the least amount of privileges necessary. Additionally, since the cloud is highly dynamic and various resources can spin up or down instantaneously, combining continuous analysis of permissions and entitlements across environments with runtime identity protection can drastically reduce the risk of successful attack.

5 out of the **top 10** MITRE tactics observed by CrowdStrike are **identity-based** (categorized by MITRE ATT&CK® as "Discovery")[4]

4 CrowdStrike 2024 Threat Hunting Report

Siloed DevOps and Security Practices Drive Cloud Risk

Misconfigurations are the number one vulnerability in cloud environments, something that increased collaboration between DevOps and security teams can address. A cloud misconfiguration is a poorly chosen, incorrect or absent security setting that exposes the cloud environment to risk. There are two major challenges when it comes to detecting and fixing these misconfigurations. Since cloud architectures are so complex, it's difficult to get a real-time picture of which misconfigurations are posing an active risk in production at any given time. Additionally, DevOps and security teams need to align on which misconfigurations need to be prioritized and how to fix them.

To effectively reduce cloud risk, DevOps and security teams need a shared, real-time view into every deployed resource, as well as how it's connected to the rest of the infrastructure and its misconfigurations. This context can help security teams effectively triage misconfigurations, and it can help DevOps teams understand the true risk of certain misconfigurations in production.

Requirements for a Cloud Security Solution

To effectively reduce cloud security risk, organizations need a security solution that can provide deep visibility into asset inventory and real-time risk exposure alongside cloud threat detection and prevention. This requires a unified platform that spans across development, operations and runtime to provide continuous visibility, protection and response. To stop threats in real time, the platform must leverage both agent-based and agentless technologies. The security platform also needs native high-fidelity threat intelligence about cloud adversaries to inform and accelerate SecOps and DevOps teams with the right content at the right time. Finally, managed detection and response (MDR) and threat hunting services round out a comprehensive solution to help ensure better outcomes.

Building a Modern Cloud Security Program: A Playbook

1. Gain Real-Time Visibility, from Code to Cloud, into Your Cloud Environment

Why? Cloud environments are highly dynamic and contain ephemeral components, and you cannot secure resources and identities that slip under the radar.

Recommendation: Center security processes around a strong foundation of visibility and correlated real-time insights across all cloud dependencies, threats and attack surfaces (infrastructure, identity, configuration, workloads, containers, applications, APIs and data). Additionally, ensure there are dedicated resources for threat hunting. Proactive threat hunting in cloud environments is essential due to the cloud's dynamic nature and the complexity of interconnected services, which require continuous visibility and rapid detection of advanced threats. This approach not only ensures compliance and cost efficiency but protects against sophisticated attacks that traditional security measures might miss.

2. Build a Risk Prioritization Strategy

Why? Security teams lack the context to effectively triage the deluge of security alerts that come from various security tooling. This is a crucial issue, as DevOps and engineering teams rely on cloud technologies to achieve faster development velocity, and they will prioritize tight development deadlines over security issues that they don't deem important or that may end up wasting their time and resources remediating vulnerabilities that seem impactful but don't present an active risk in production.

Recommendation: Consider leveraging a tool that correlates threat intelligence, business impact and data sensitivity to provide an accurate representation of active risk, enabling alignment between DevOps and security teams on which security issues to prioritize and when.

3. Incorporate Runtime Protection to Stop Breaches

Why? Although it is recommended to focus efforts on risk reduction of applications and cloud resources before they are deployed to production, it would be detrimental to not employ security protection in production environments as well. This provides not only a fail-safe mechanism for any security risks that may end up in production, but also protection against new and emerging threats.

Recommendation: Practice defense-in-depth by employing mechanisms to block threats in real time, improving response times dramatically and eliminating the need to hunt through logs.

4. Harness Elite Expertise Combined with Cloud-native Detection and Response

Why? To maximize the value of your investments in a security solution, teams must have the expertise to leverage it fully.

Recommendation: Look for a solution provider that can function as a partner you can rely on to guard your cloud assets 24/7. Especially in the age of cloud, where all of your teams' efforts should be focused on innovation, it is crucial to leverage a team that can manage every stage of cloud detection and response for you, from detection to remediation, and can quickly neutralize threats with precision and efficiency.

5. Centralize Security Processes into One Workstream Between DevOps, Engineering and Security Teams

Why? Silos between security, DevOps and engineering teams heighten the risk of a successful breach, since engineers are the ones responsible for applying security fixes or patches.

Recommendation: Ensure cloud security tooling integrates both live threat intelligence and your business context to help DevOps and security teams best align on cloud security priorities.

CrowdStrike for Cloud Security

IT environments are growing larger and more complex, providing threat actors with a vast attack surface. Organizations should look to partner with a team that is deeply knowledgeable on threat actor behavior and the cloud so that they can focus on innovating and staying competitive.

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 provides multi-cloud visibility, security and compliance in a single, unified platform. CrowdStrike Falcon® Cloud Security was built from the ground up as a fully integrated CNAPP offering and is simple to turn on, extending protection from customer endpoints to the cloud with agentless and agent-based protection.

Kick-start your cloud security journey today by requesting a Cloud Security Health Check to assess the security of your cloud environment.

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.**

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/