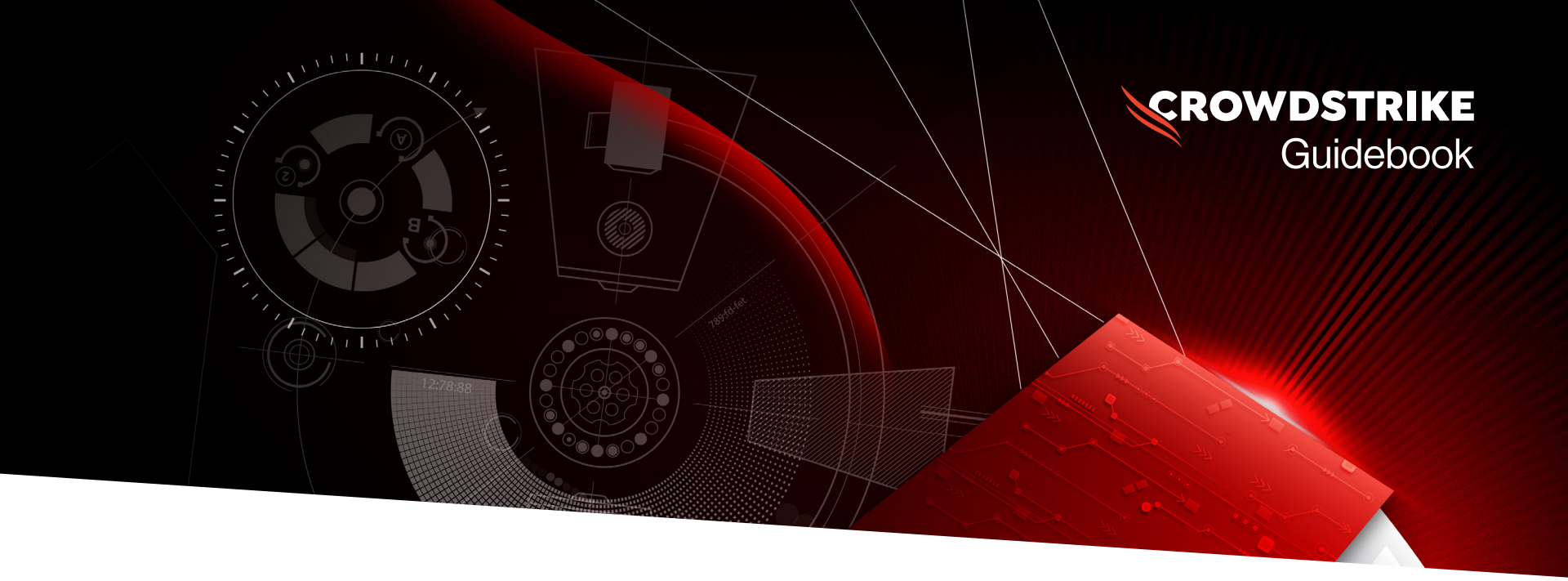
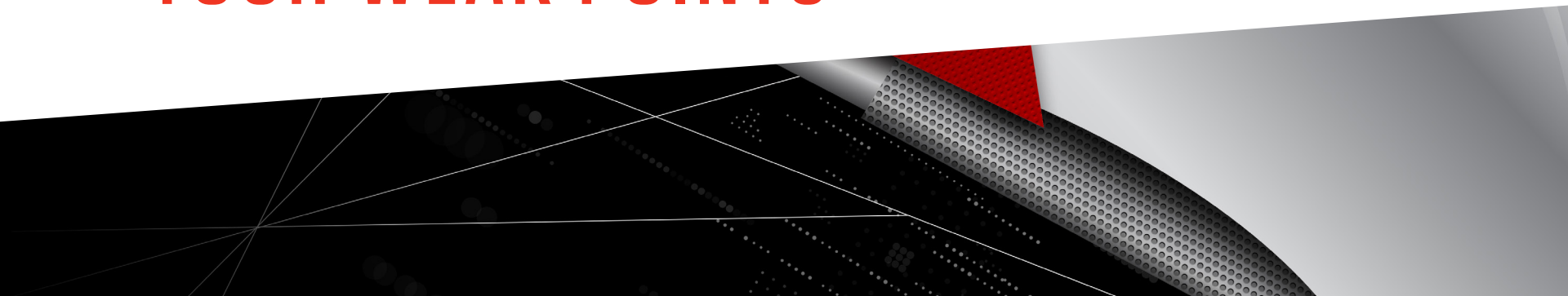


CROWDSTRIKE
Guidebook

ADVERSARIES HAVE THEIR HEADS IN THE CLOUD AND ARE TARGETING YOUR WEAK POINTS



IN ONE INSTANCE INVESTIGATED BY CROWDSTRIKE, THE EXPLOITATION OF THESE VULNERABILITIES BY THREAT ACTORS DISRUPTED THE RELEASE OF A KEY FEATURE LAUNCH. IN ANOTHER, IT DELAYED MERGER AND ACQUISITION ACTIVITIES

Cloud adoption is powering digital transformation, bringing levels of speed and scalability that can unlock new efficiencies and revenue streams. As organizations leverage the cloud's benefits, it is the job of security teams to enable them to do so safely.

In this reality, it is vital that IT leaders understand how threat actors are targeting their cloud infrastructure. As one might suspect, attackers first go after low-hanging fruit — the systems and applications that are the easiest to exploit.

In the 2020 CrowdStrike Cyber Front Lines Report, our researchers noted:

- Adversaries target neglected cloud infrastructure slated for retirement that still contains sensitive data.
- Adversaries use a lack of outbound restrictions and workload protection to exfiltrate your data.
- Adversaries leverage common cloud services as a way to obfuscate malicious activity.

Neglected and soon-to-be-retired infrastructure makes for low-hanging fruit for attackers, often because that infrastructure no longer receives security configuration updates and regular maintenance. Security controls such as monitoring, expanded logging, security architecture and planning, and posture management no longer existed for these assets.

Unfortunately, CrowdStrike researchers encountered cases where this neglected cloud infrastructure still contained critical business data. As such, attacks led to sensitive data leaks requiring costly investigation and reporting obligations. In other cases, attacks on abandoned cloud assets caused service disruptions because the impacted infrastructure provided critical services that hadn't been fully transitioned to new infrastructure.

LAUNCHING ATTACKS FROM THE CLOUD

SECURITY MUST ADAPT

Not only did the CrowdStrike team see attackers target cloud infrastructure during 2020, we also observed threat actors leveraging the cloud to make their attacks more effective. Over the past year, threat actors used well-known cloud services, such as Microsoft Azure, and data storage syncing services, such as MEGA, to exfiltrate data and proxy network traffic. A lack of outbound restrictions combined with a lack of workload protection allowed threat actors to interact with local services over proxies to IP addresses in the cloud. This gave attackers additional time to interrogate systems and exfiltrate data from services ranging from partner-operated, web-based APIs to databases — all while appearing to originate from inside victims' networks. These tactics allowed attackers to dodge detection by barely leaving a trace on local file systems.

Securing cloud environments demands a different approach than the strategies organizations traditionally use to protect their on-premises data center. As organizations continue to embrace cloud services to improve their business, there are four key tenets of cloud security they should consider.

1. Enable runtime protection and obtain real-time visibility. The adage that you cannot protect what you cannot see holds true. Central to securing your cloud infrastructure to prevent a breach is runtime protection and visibility provided by solutions such as CrowdStrike Falcon® Cloud Workload Protection (CWP). It remains critical to protect your workloads and containers with next-generation endpoint, workload, and container protection, including servers, workstations and mobile devices. This protection should extend across the entire organization, from the on-premises data center to the cloud.

2. Eliminate configuration errors. Human error continues to be the most common cause of vulnerabilities in cloud environments. These errors are often introduced during common administrative tasks. It's important to set up new infrastructure in ways that make secure operations easy to adopt. One way to do this is to use a cloud account factory to create new sub-accounts and subscriptions. This strategy ensures that new accounts are set up in a predictable manner, eliminating common sources of misconfiguration mistakes. Also, make sure to set up roles and network security groups that keep developers and operators from needing to build their own security profiles and accidentally doing it poorly.

3. Leverage a cloud security posture management (CSPM) solution. Ensure your cloud account factory includes enabling detailed logging and a CSPM solution — such as CrowdStrike Falcon Horizon™ — with alerting to responsible parties including cloud operations and security operations center (SOC) teams. Actively seek out unmanaged cloud subscriptions, and ensure that responsible parties are identified and motivated to either decommission any shadow IT cloud environments or bring them under full management along with your CSPM. Then use your CSPM on all infrastructure up until the day the account or subscription is fully decommissioned to ensure that operations teams have continuous visibility.

CROWDSTRIKE: A CLOUD-NATIVE PARTNER FOR A CLOUD-FIRST WORLD

4. Empower DevSecOps. Enterprises need to enforce security without slowing the speed of application delivery. As developers continue to adopt container technologies to increase velocity, the importance of a shift-left approach to security has only grown. To meet this need, CrowdStrike Container Security was designed to integrate frictionless security into the continuous integration/continuous delivery (CI/CD) pipeline. This integration takes multiple forms, including continuously scanning container images for known vulnerabilities and misconfigurations, detecting malware in base images before container deployment, and integrating with developer toolchains. By automating protection, organizations can empower DevSecOps to deliver secure applications without slowing the build cycle.

Because the cloud is dynamic, so too must be the tools used to secure it. The visibility needed to see the type of attack that traverses from an endpoint to different cloud services is not possible with siloed security products that only focus on a specific niche.

CrowdStrike is the market-leader in cloud-native cybersecurity products and services. We take an adversary-focused approach to protecting our clients and their customers from all cyberattacks, including those that occur within the cloud. The CrowdStrike Falcon® platform leverages sophisticated signatureless artificial intelligence (AI), machine learning (ML), and indicator-of-misconfiguration (IOM)-based and indicator-of-attack (IOA)-based threat prevention to stop known and unknown threats in real time, helping organizations address these four tenets and any others within their cybersecurity strategy and toolset.

Want to learn more about how to minimize risk through a reduced attack surface? Download the latest eBook from CrowdStrike, a market leader in cloud-native cybersecurity:

The CrowdStrike Security Cloud: Transforming Security for Today's Modern Cloud Business

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

Learn more at **www.crowdstrike.com**