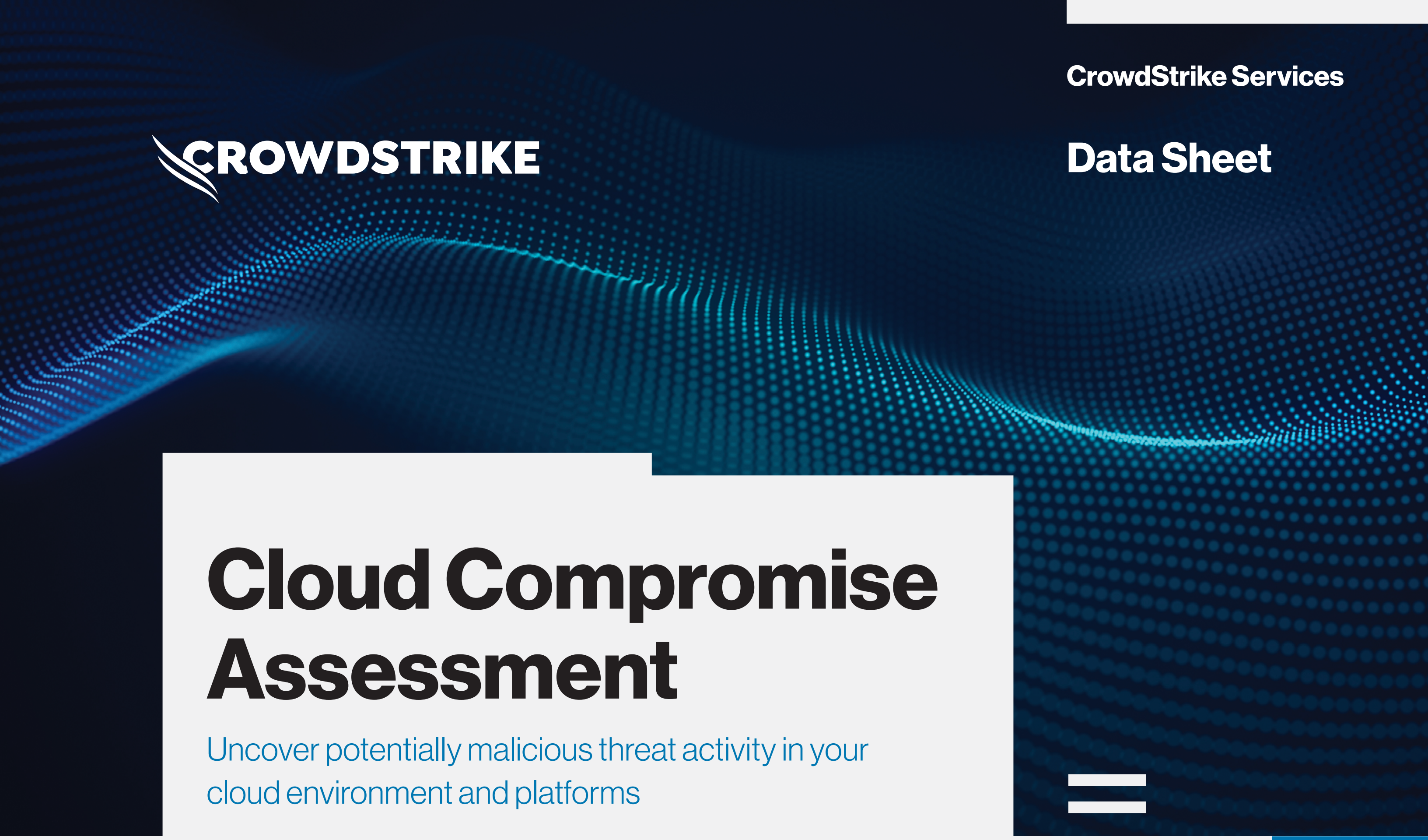

CROWDSTRIKE

CrowdStrike Services

Data Sheet

Cloud Compromise Assessment

Uncover potentially malicious threat activity in your cloud environment and platforms

Adversaries have their heads in your cloud

Ineffective and misconfigured cloud security settings enable threat actors to gain access to your cloud platforms and operate undetected as they search for data and systems of value in your cloud environment. This "silent failure" to detect malicious activity and allow adversaries to move laterally across your cloud environment is often caused by:

- **Improper public access configured and exposed access keys**
- **Excessive account permissions and ineffective identity architecture**
- **Disabled logging, missing alerts and inadequate network segmentation**
- **Public snapshots and images, and open databases and caches**

CrowdStrike Services consultants provide expert advice and best practices for the successful deployment, configuration and operationalization of the Falcon cloud security modules to better protect your cloud workloads and platforms.

Identifying compromise activity in a cloud environment

A CrowdStrike Cloud Compromise Assessment identifies current (and past) threat activity in your cloud environment. This cloud threat hunting engagement collects configuration and log information across your cloud service plane to determine if your cloud environment has been compromised.

The investigation analyzes the information collected to identify and explore evidence of access or configuration changes consistent with unauthorized activity by a threat actor.

Key benefits

Determine if there is current (or past) adversary activity within your cloud environment

Investigate evidence of a cloud data breach

Receive prioritized findings and recommendations to help prevent future attacks

Key service features

The CrowdStrike Cloud Compromise Assessment collects configuration and log information from the cloud service plane using the CrowdStrike Falcon® platform and proprietary Cloud Collectors toolset. The compromise assessment is available for leading cloud vendors including Amazon AWS, Microsoft Azure/O365 and Google Cloud Platform (GCP). This one-time threat hunt determines if the cloud environment has been compromised, and includes:

- **Collection of cloud configuration information** using the CrowdStrike Falcon® Horizon cloud security posture management (CSPM) module
- **Collection of cloud log information** using proprietary CrowdStrike Cloud Collectors
- **Detailed analysis** of cloud telemetry information
- **Investigation findings** of potential compromise activity and evidence
- **Review of the active configuration** for critical cloud security settings
- **Recommendations for remediation** to prevent future cloud breaches

CrowdStrike consultants deliver their findings related to cloud compromise activity, along with associated recommendations organized by criticality and impact.

About CrowdStrike Services

CrowdStrike Services delivers Incident Response, Advisory Services, Technical Assessments, Product Support and Training that help you prepare to defend against advanced threats, respond to widespread attacks, enhance your cybersecurity practices and controls and operationalize your technology platform.

We help our customers assess and enhance their cybersecurity posture, implement technologies, test defenses against real-world attacks, respond to incidents, accelerate forensic investigations, and recover from a breach with speed and precision. Harnessing the power of the CrowdStrike® Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary-focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike:

We stop breaches.

Why choose CrowdStrike?

Cloud threat intel: CrowdStrike investigators leverage the extensive threat intelligence and indicators of attack (IOAs) gained from protecting millions of cloud workloads and containers across the globe.

Superior technology: CrowdStrike consultants leverage the full power of the CrowdStrike Falcon platform and Cloud Collectors tools to gain visibility into threat actor activity in your cloud environment.

Comprehensive IOMs: CrowdStrike consultants leverage the Falcon Horizon module with indicators of misconfiguration (IOMs) to detect ineffective cloud security settings and misconfigurations.

Learn more
www.crowdstrike.com/services/

Email
services@crowdstrike.com