CROWDSTRIKE

CrowdStrike Products
Soultion Brief

Falcon Cloud Security:

Cloud Infrastructure Entitlement Management (CIEM)

Identity-based security, visibility and least-privilege enforcement across hybrid and multi-cloud environments

As organizations are moving to the cloud, they are confronted with the growing complexity of managing access and identities in cloud environments. Although public cloud providers work tirelessly to minimize vulnerabilities and strengthen defenses against cloud threats, it is the customer who ultimately holds the responsibility when it comes to securing identities and data.

With cloud infrastructure evolving and different architectures constantly shifting, trying to figure out what and who is in your environment can seem impossible, let alone establishing a baseline for what normal looks like. This lack of comprehensive visibility can leave organizations vulnerable to insider threats and external attacks exploiting excessive or unnecessary permissions. The rapid deployment of cloud resources, combined with the continuous changes in user roles and permissions, demands a more agile and automated approach to entitlement management. Organizations need robust, efficient and scalable management of cloud identities and entitlements in a fast-paced cloud environment.

CrowdStrike Falcon® Cloud Security provides integrated cloud infrastructure entitlement management (CIEM) capabilities that deliver a single source of truth for monitoring, discovering and securing identities across multi-cloud environments, all in a single, unified platform. Falcon Cloud Security prevents identity-based threats resulting from improperly configured cloud entitlements across AWS, Azure and GCP. It enables you to gain access to the full inventory of permissions, detect overly permissive accounts, continuously monitor activity and ensure least-privilege enforcement.

Key benefits

- Unified multi-cloud visibility and least-privilege enforcement
- Continuous detection and prevention of identity-based threats
- Operational efficiency of security teams

Key features

- IAM entitlement investigation
- Streamlined remediations
- Pre-defined resource-based policies
- Monitoring of AWS identity and access management (IAM) users, roles and permissions across all cloud accounts
- Monitoring of Entra ID users, groups and application registrations

Key capabilities

Complete visibility of cloud identities and entitlements

- Gain complete visibility into cloud resources, and automatically understand the relationships between access and permissions.
- Optimize your security strategy and enhance asset management by performing real-time point queries for incident response and broad analytical queries for security posture optimization.
- Improve security management through a single view of user data across all accounts to quickly spot disabled multifactor authentication (MFA) and excessive permissions.
- Streamline resource access management with resource-based policies that clearly define user access levels and actions on resources, allowing for quick visibility into the resources and permissions associated with each account.
- Enhance your Microsoft Entra ID (formerly Azure Active Directory) security visibility with insightful dashboards, enabling regular audits of privileged user access, application registration permissions and proactive monitoring for potential abuse of secrets or certificates.

Least-privilege implementation across clouds

- Enhance security and minimize risk by implementing the principle of least privilege, efficiently assessing IAM users, roles and permissions across all cloud accounts.
- Ensure robust cloud security by monitoring accounts for excessive or unused permissions, detecting suspicious permission escalations and conducting comprehensive audits of actions allowed per resource, user, group and role in cloud services.
- Identify and mitigate security risks by detecting and eliminating unwanted access and risky permissions, including identity misconfigurations and cloud entitlements, to achieve and maintain least-privilege access in your cloud resources.

Expansive identity threat detection and response

- Get comprehensive identity threat detection and response (ITDR) from the CrowdStrike Falcon® platform spanning a complex environment including identity, cloud, endpoint, data and workloads.
- Detect suspicious lateral movement — including hybrid lateral movement — and anomalous authentication traffic in real time.
- Enforce risk-based, conditional access to stop adversaries in their tracks and empower user productivity.
- Support an identity security posture management (ISPM) framework to proactively prevent identity-based attacks before they start.

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/