CrowdStrike Expands CNAPP Capabilities with Introduction of CIEM to Monitor, Discover and Secure Identities Across Multi-Cloud Environments

CrowdStrike Cloud Security is also now integrated with CrowdStrike Asset Graph to provide rich cloud asset visualizations and unprecedented visibility of cloud resources

AUSTIN, Texas & LAS VEGAS--(BUSINESS WIRE)--Sep. 20, 2022--

Fal.Con 2022--CrowdStrike (Nasdaq: CRWD), a leader in cloud-delivered protection of endpoints, cloud workloads, identity and data, today announced new Cloud Native Application Protection Platform (CNAPP) capabilities for CrowdStrike Cloud Security, which includes new Cloud Infrastructure Entitlement Management (CIEM) features and the integration of CrowdStrike Asset Graph. CIEM enables organizations to prevent identity-based threats resulting from improperly configured cloud entitlements across cloud service providers, like Amazon Web Services (AWS), while Asset Graph provides unprecedented visibility into the attack surface in the cloud across hosts, configurations, identities and applications to stop breaches. AWS is a strategic partner of CrowdStrike, which is available on the AWS Marketplace. CIEM capabilities also extend to Microsoft Azure.

According to a Gartner® report, "75% of security failures will result from inadequate management of identities, access, and privileges [by 2023]." In order to maintain Zero Trust best practices and least-privilege principles in the cloud, compliance and security teams need tools that can help continuously enforce policies across cloud accounts and resources.

"Existing cloud security tools address specific aspects of cloud infrastructure security, but they generally lack identity and access controls. Manual methods to ensure a least-privilege approach to security just don't scale in an environment with so many identities and entitlements. By extending our CNAPP capabilities to include CIEM, we are enabling organizations to gain access to their full inventory of permissions, detect overly permissive accounts, continuously monitor activity and ensure least-privilege enforcement. Organizations can also visually understand the relationships between access and permissions with CrowdStrike Asset Graph, which is a powerful tool that we're making available to CrowdStrike Cloud Security customers," said Amol Kulkarni, chief product and engineering officer at CrowdStrike.

With CrowdStrike Cloud Security, organizations can:

- **Unify visibility and least-privilege enforcement in public and multi-cloud environments.**
  - **Access a single source of truth:** Get up and running in minutes and access a single dashboard for all cloud assets, identities and security configurations.
  - **Simplify privileged access management and policy enforcement:** Manage and enforce identities and permissions across AWS and Azure.
  - **Identify and investigate cloud entitlements:** Detect risky permissions, and remove unwanted access to cloud resources including identity misconfigurations and cloud entitlements to achieve least-privilege.
- **Continuously detect and remediate identity-based threats in public and multi-cloud environments.**
  - **Prevent identity-based threats at scale:** Secure cloud identities and permissions**,** detect account compromises, prevent identity misconfigurations, stolen access keys, insider threats and malicious activity.
  - **Secure Azure Active Directory:** Ensure Azure AD groups, users and apps have the correct permissions using new Identity Analyzer reports.
  - **One-click remediation testing:** Simulate remediation tactics to understand outcomes and ensure confidence by performing a dry run prior to deployment.
- **Gain access to CrowdStrike's Breach Prevention Engine.**
  - **Predict and prevent modern threats:** Ensure real-time protection via CrowdStrike Threat Graph, which provides full visibility of attacks and automatically prevents threats in real-time across CrowdStrike's global customer base.
  - **Access enriched threat intelligence:** Get deeper context for faster more effective response with a visual representation of relationships across account roles, workloads and APIs.
  - **Accelerate response:** Arm your responders in real time via Threat Graph, empowering incident responders to understand threats immediately and act decisively.
- **Get rich cloud asset visualization powered by CrowdStrike Asset Graph.**
  - **See and secure cloud identities and entitlements:** Gain complete visibility into cloud resources, and understand the relationships between access and permissions automatically.
  - **Optimize cloud implementations:** Perform real-time point queries for rapid response, as well as broader analytical queries for asset management and security posture optimization.
  - **Mitigate risks across the attack surface:** Get 360-degree visibility into your organization's assets and their interdependencies across hosts, configurations, identities and applications.

"The one-click remediation testing feature stands out amongst the new CIEM capabilities for CrowdStrike Cloud Security. Ransomware continues to plague cloud environments. Defending against this cyber plague is much more than stopping malware execution. It is stopping the attacker that compromises credentials, moves across cloud environments, escalates privileges and exfiltrates data. One-click remediation testing is a powerful tool

that can enable SOC analysts to quickly detect and remediate identity-based threats for faster, more effective response," said Frank Dickson, group vice president, security & trust at IDC.

"With CrowdStrike Cloud Security, understanding our cloud posture and catching misconfigurations has been key to our risk mitigation strategy," said Anthony Cunha, CISO at Mercury Financial. "We think CrowdStrike extending its CNAPP capabilities to CIEM can further enable us to prevent identity-based threats resulting from improperly configured cloud entitlements."

CIEM capabilities and integration of CrowdStrike Asset Graph are generally available for CrowdStrike Cloud Security customers.

Additional Resources

- CrowdStrike was named a Strong Performer in The Forrester Wave™: Cloud Workload Security, Q1 2022 report.[1]

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms 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 | Twitter | LinkedIn | Facebook | Instagram
Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

---

[1] The Forrester Wave™: Cloud Workload Security, Q1 2022

View source version on businesswire.com: https://www.businesswire.com/news/home/20220920005561/en/

Kevin Benacci
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike