

CrowdStrike Expands Cloud Detection and Response Leadership to Stop Cloud Breaches

May 6, 2024

Unveils new 24/7 cross-domain threat hunting for Microsoft Azure environments with industry-first visibility across clouds, identities and endpoints—powered by elite adversary intelligence

AUSTIN, Texas--(BUSINESS WIRE)--May 6, 2024-- **RSA Conference 2024** -- [CrowdStrike](#) (Nasdaq: CRWD) today announced new Cloud Detection and Response (CDR) innovations to unify industry-leading managed threat hunting with deep visibility across cloud, identity and endpoints to speed detection and response across every stage of a cloud attack. Beginning with Microsoft Azure, new CDR innovations expand visibility into cloud control plane activity, strengthening existing threat hunting for cloud runtime environments.

With [cloud intrusions growing 75% in the past year](#), cloud is the new battleground as adversaries increasingly leverage identity-based attacks to exploit visibility gaps created by fragmented platforms and cloud security point products. At the same time, Cloud SecOps teams face an emerging [skills gap](#) in cloud security expertise that can significantly delay detection and response times to threats. With this release, the powerful combination of CrowdStrike's proven expertise in 24/7 managed threat hunting and its industry-defining Cloud Native Application Protection Platform (CNAPP) sets a new standard for CDR by delivering the visibility across and within clouds, identities and endpoints needed to stop cloud breaches, even as threats move laterally from cloud to endpoint.

"CrowdStrike pioneered EDR, we established MDR before it was a category and now we're setting the standard for what CDR delivers and can do for customers. Stopping cloud breaches requires rapid detection and response, but too often, Cloud SecOps teams are forced to manage multiple platforms and point products to get the visibility they need across their cloud infrastructure," said Michael Sentonas, president at CrowdStrike. "The combination of CrowdStrike's industry-leading cloud threat hunting services and comprehensive CNAPP provides a powerful force multiplier for Cloud SecOps teams to consolidate tools, close gaps in visibility and deliver the security outcome that matters most – stopping the breach."

Stopping Identity-Based Attacks in the Cloud

As noted in the DHS Cyber Safety Review Board (CSRB), the Summer 2023 [breach of Microsoft Exchange Online](#) was "preventable and should never have occurred." Adversaries commonly use identity-based attacks to breach customer cloud environments, and the security lapse noted in the CSRB report highlights the critical need to proactively detect and respond to cloud attacks, especially for Microsoft Azure environments.

With this release, CrowdStrike delivers the world's most comprehensive cloud detection and response service by:

- **Protecting Cloud Control Planes:** Beginning with Microsoft Azure, CrowdStrike expands visibility into cloud control plane activity, complimenting existing threat hunting for cloud runtime environments.
- **Stopping Cloud Identity Threats:** CrowdStrike's unified platform approach enables cloud threat hunters to proactively monitor and prevent compromised users and credentials from being exploited in cloud attacks.
- **Preventing Adversary Lateral Movement:** The unified AI-native CrowdStrike Falcon platform empowers CrowdStrike cloud threat hunters to track lateral movement from cloud to endpoint, enabling rapid response and actionable insights for decisive remediation from indicators to root cause.

For more information, please visit [our website](#).

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](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

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

©2024 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

View source version on [businesswire.com](https://www.businesswire.com/news/home/20240506232248/en/): <https://www.businesswire.com/news/home/20240506232248/en/>

Media Contact

Jake Schuster

CrowdStrike Corporate Communications

press@crowdstrike.com

Source: CrowdStrike