NEWS RELEASE

New CrowdStrike Falcon Platform Innovations Unify End-to-End Security and IT Operations to Remove Complexity and Stop Breaches

2024-09-18

AUSTIN, Texas & LAS VEGAS--(BUSINESS WIRE)-- Fal.Con 2024 -- **CrowdStrike** (NASDAQ: CRWD) today announced new innovations that unify security and IT to stop breaches on the **CrowdStrike Falcon® cybersecurity platform** .

The single-agent, cloud- and AI-native Falcon platform consolidates point products to eliminate complexity and deliver better security outcomes. With these new innovations, CrowdStrike is unifying the security and IT operations lifecycle – from assessing risk and threat detection, to accelerating remediation and response. New and expanded innovations include:

Project Kestrel: A Revolutionary New User Experience : Project Kestrel removes silos and unifies data from across the Falcon platform to provide an all-in-one view of an organization's security environment. With a customizable user experience that ensures the right user gets the right data at the right time, Project Kestrel eliminates complexity, accelerates collaboration and enables rapid threat response. Dynamic access controls and a single view of all assets, vulnerabilities and misconfigurations empower organizations to stay ahead of adversaries.

CrowdStrike Endpoint Security stops breaches with AI-powered protection, detection and response, backed by world-class adversary intelligence. New innovations include:

- CrowdStrike Signal: A new family of AI-powered engines, Signal intelligently groups related events and alerts into actionable, prioritized insights, with a self-learning model tailored to the organization's specific

environment. Signal's AI-generated lead detection improves analyst efficiency and surfaces novel and stealthy adversary tradecraft to reduce the risk of missed detections.
- Legacy OS Support: Falcon introduces anti-malware protection for legacy Windows operating system versions as early as Windows XP SP3/Server 2003.

Falcon Cloud Security delivers comprehensive visibility and protection across the entire cloud estate – infrastructure, applications, data and AI models from a single, unified platform. New innovations include:

- AI Security Posture Management (AI-SPM): A new capability, AI-SPM monitors AI services and large language models (LLM) deployed in the cloud, detects misconfigurations, and identifies and addresses vulnerabilities to enable secure AI innovation.
- Data Security Posture Management (DSPM): Now fully integrated with Falcon Cloud Security, security teams can discover, classify and protect data in all states – at rest or in motion – as it flows through the cloud estate and across endpoints.

Falcon Identity Protection detects and stops identity-driven attacks spanning domains with visibility and protection across and within clouds, identities and endpoints. New innovations include:

- Falcon Privileged Access: Enforces least privilege through risk-based Just-in-Time (JIT) access across hybrid cloud environments to reduce the identity attack surface and combat cross-domain attacks.
- Real-Time Threat Protection for Microsoft Entra ID: Delivers Falcon's AI-powered identity protection against password spraying, phishing and other identity threats targeting Entra ID (cloud-based active directory) environments.

Falcon Next-Gen SIEM unifies Falcon and third-party data, threat intelligence, AI and workflow automation to deliver the AI-native SOC. New innovations include:

- AI-generated Parsers: Easily ingest and process data from any source. Industry-first capabilities include using LLMs to analyze log data and build parsers automatically, accelerating investigations.
- Detection Posture Management: Maps active detection rules across all Falcon platform modules and third party tools to MITRE ATT&CK techniques to instantly identify coverage gaps and provide prescriptive recommendations to strengthen security posture.
- Workflow Automation Enhancements: Accelerate response with a new content library including an expanded set of prebuilt workflows and 300+ response actions.

Falcon Exposure Management proactively reduces intrusion risk with unified, AI-powered vulnerability prioritization and complete attack surface visibility. New innovations include:

- Network Vulnerability Assessment: Built on CrowdStrike's patented ExPRT.AI technology for risk-based

vulnerability prioritization, organizations can replace outdated, complex network scanning infrastructure with sensor-based, continuous scans that minimize network congestion, deliver real-time visibility and assessments, and prioritize the most critical network vulnerabilities.
- Attack Path Analysis: Identifies cross-domain exposures and attack paths leading to business-critical assets and data, enabling teams to predict likely adversary behavior based on real-world activity to harden high-risk areas of exposure.

Charlotte AI delivers the transformative power of conversational AI to organizations, turning hours of work into minutes or seconds. New innovations include:

- GenAI-powered Detection Triage: Analysts can now direct Charlotte AI to triage detections on their behalf, accelerating investigations and incident response. Charlotte AI has been trained leveraging the expertise of the elite Falcon Complete team, CrowdStrike's market-leading MDR, so every organization can leverage industry best practices with the speed, consistency and scale of AI.

Falcon for IT automates complex use cases across security and IT using native GenAI workflows and the single-agent architecture of the Falcon platform. New innovations include:

- Extended Asset Context: Interrogates assets in real-time to gather extended IT context beyond standard security telemetry, such as patch deployment and management data to support investigation and response activities.
- Automated Tasks: Create scheduled queries and define a corresponding set of automated responses to immediately resolve compliance or configuration issues, apply emergency patches, and proactively address issues that might impact end user productivity.

"Today's security challenges are rooted in complexity, which slows down response and increases risk," said George Kurtz, CEO and founder, CrowdStrike. "With our latest innovations, we're simplifying security and IT operations by bringing everything together in a unified platform. With a new user experience that ensures each team has the right data and tools at their fingertips, organizations gain faster decision-making, seamless collaboration and a more proactive approach to stopping breaches. By unifying the entire security and IT lifecycle – from risk assessment to response – we enable organizations to respond faster, work smarter and stay ahead of evolving threats."

CrowdStrike Financial Services was also announced this week at **Fal.Con 2024** , cybersecurity's premier user conference. CrowdStrike Financial Services accelerates Falcon platform consolidation, providing customers with tailored financing solutions to remove procurement complexity. To learn more, **visit here** .

This information about CrowdStrike products is intended for informational purposes. Please do not rely on this information in making your purchasing decisions. The development, release and timing of any products, features or

functionality remain at the sole discretion of CrowdStrike, and are subject to change.

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/**

Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike