CrowdStrike Fal.Con 2024 Announcements

STEVE MCDOWELL, CHIEF ANALYST
9/19/24

CONTEXT

At its 2024 Fal.Con customer event in Las Vegas, CrowdStrike unveiled several major updates to its AI-native Falcon cybersecurity platform that unify, automate, and enhance its customers' security and IT operations.

The announcements cover a range of new features in cloud security, SIEM, AI-driven capabilities, and identity protection, all designed to create a cohesive platform for accelerating threat detection, response, and prevention.

PROJECT KESTREL

CrowdStrike announced **Project Kestrel**, a new capability designed to eliminate data silos within security teams. It does this by unifying security data from across various products within CrowdStrike's Falcon platform to give a cohesive view to security teams.

The platform offers a new streamlined user interface that integrates data on assets, vulnerabilities, misconfigurations, and other critical security metrics, enabling faster and more informed decision-making. One of Project Kestrel's standout features is its customizable user experience, which allows users to tailor the platform's views and workflows to suit their specific needs.

Eliminating the need for manual data merging and reducing reliance on spreadsheets will allow Project Kestrel to enhance visibility, speed up analysis, and enable faster action against critical security threats. This powerful new experience will simplify and accelerate the security process.

EXPANDED CLOUD SECURITY FEATURES

CrowdStrike also expanded its **Falcon Cloud Security** capabilities by integrating several security posture management tools, including **Data Security Posture Management (DSPM)**, **Application Security Posture Management (ASPM)**, and **AI Security Posture Management (AI-SPM)**. These additions provide enhanced visibility into cloud assets, applications, and AI models, allowing organizations to detect vulnerabilities and prevent breaches across all infrastructure layers.

The real-time asset inventory feature, now generally available, offers continuous monitoring of assets in AWS, Azure, Google Cloud, and VMware environments, enabling faster identification and response to misconfigurations and attack paths.

NEXT-GEN SIEM

CrowdStrike announced advancements to its **Falcon Next-Gen SIEM** (Security Information and Event Management) platform, focusing on AI and workflow automation.

The updates include new **Falcon Fusion SOAR** (Security Orchestration, Automation, and Response) capabilities to enable security teams to automate threat responses and integrate third-party tools more effectively.

The company also introduced AI-generated parsers to automate log analysis This reduces the manual effort involved in managing data from disparate sources, allowing CrowdStrike customers to detect and respond to threats with greater speed and accuracy.

AI INNOVATIONS

The Falcon platform also gained several AI-powered features to enhance threat response capabilities. **Attack Path Analysis (APA)** helps security teams visualize how attackers could move through their infrastructure, providing precise remediation recommendations.

CrowdStrike Signal is an AI-powered engine for **Falcon Insight XDR** that streamlines threat detection by generating and prioritizing leads, reducing noise for security analysts. **Charlotte AI** also offers new detection triage capabilities to help analysts differentiate between true and false positives.

IDENTITY PROTECTION

CrowdStrike expanded its **Falcon Identity Protection** with real-time threat prevention for **Microsoft Entra ID** to address identity-based threats. The integration leverages advanced user behavior analytics and risk-based access decisions to block unauthorized access and prevent lateral movement between identity providers.

Additionally, **Falcon Privileged Access** introduces just-in-time access control for privileged roles, reducing the attack surface and improving security for critical administrative functions.

FALCON FOR IT

CrowdStrike introduced new features to **Falcon for IT** to unify security and IT operations. The enhancements allow teams to gather real-time extended asset context and automate remediation workflows. The platform's real-time visibility and query allow users to quickly address configuration and compliance issues.

CROWDSTRIKE FINANCIAL SERVICES

CrowdStrike launched **CrowdStrike Financial Services** to make its solutions more affordable by offering tailored financing options to help customers purchase Falcon platform products and services.

The new initiative includes custom payment plans and competitive loans, which give financial flexibility to businesses seeking to enhance cybersecurity defenses.

ANALYSIS

While all its announcements are compelling, Project Kestrel may be the most impactful as it addresses the long-standing challenge of siloed data in security operations. Unifying disparate data streams into a single, customizable platform allows CrowdStrike to enhance visibility while driving operational efficiency for security teams.

This addresses one of the most persistent issues facing large organizations: the difficulty correlating and responding quickly to threats due to fragmented data across various tools and platforms.

From a competitive standpoint, Project Kestrel differentiates CrowdStrike from legacy security providers and next-gen competitors. Vendors like Splunk and Palo Alto Networks have invested heavily in unified security approaches. Still, CrowdStrike's emphasis on a seamless user experience and the ability to customize workflows for different roles provides an edge in user adoption and flexibility.

The enhancements to Falcon Cloud Security, including expanded DSPM, ASPM, and AI-SPM capabilities, are a forward-thinking approach to securing cloud environments and AI models—an area that many of CrowdStrike's competitors remain under-addressed. The company's ability to provide comprehensive, real-time protection across AWS, Azure, and Google Cloud environments is a powerful set of capabilities that should cement its leadership in cloud security as it competes head-to-head with players like Palo Alto Networks and Microsoft.

Overall, CrowdStrike's updates show the company continuing its path to deliver a unified, AI-powered platform to address the full spectrum of cybersecurity needs. By expanding its capabilities across cloud, identity, AI, and SIEM, CrowdStrike demonstrates why it continually outpaces competitors in functionality and usability. CrowdStrike remains the go-to platform for organizations looking to streamline and fortify their security operations.