CROWDSTRIKE
Investor Relations

CrowdStrike Bolsters Endpoint Protection Platform with New Capabilities

October 13, 2020

CrowdStrike delivers expanded capabilities and customization for the Falcon Platform to enhance detection, visibility and response across operating systems and support unique business needs

SUNNYVALE, Calif.--(BUSINESS WIRE)--Oct. 13, 2020-- **Fal.Con 2020** -- CrowdStrike, Inc. (Nasdaq: CRWD), a leader in cloud-delivered endpoint and workload protection, today announced enhancements to the CrowdStrike Falcon® platform's visibility, detection and response capabilities across Windows, macOS and Linux operating systems and new customization capabilities enable customers to tailor information views and create dashboards based on unique business needs.

Today's threat actors are expanding their reach beyond Windows operating system targets. The 2019 CrowdStrike Services Cyber Front Lines Report observed threat actors increasingly targeting macOS environments and using relatively unsophisticated methods to gain access. The increasing popularity of macOS systems in organizations, combined with insufficient macOS endpoint management and monitoring, has made macOS devices lucrative targets for adversaries. Additionally, hosts with Linux operating systems are also in threat actors' crosshairs, as the operating system is commonly used to protect high-value assets and servers and is critical to cloud expansion.

"To defend against the expansion of threat activity, businesses need robust threat-centric security capabilities to effectively protect their endpoints. These capabilities are best served within a single platform that provides comprehensive detection, visibility and response capabilities across operating systems," said Amol Kulkarni, chief product officer at CrowdStrike. "The newly expanded capabilities of the cloud-native Falcon Platform bolster endpoint protection, regardless of the operating system of choice. The Falcon Platform also now enables customers to fine tune their security data and dashboards to create custom workload protection specific to their business needs."

The Falcon platform updates provide the following capabilities:

- Detection: CrowdStrike has enhanced its lateral movement detection to encompass cross-operating system attacks, such as when an adversary uses RDP to move from Linux to Windows. CrowdStrike has also expanded detections for Linux based on the MITRE ATT&CK framework. On macOS, Falcon will enhance local protection when these devices are offline with sensor-based machine learning that complements existing cloud-based ML. For Windows, Falcon now detects and prevents attacks that leverage known vulnerable drivers and provides kernel exploit protection.
- Visibility: CrowdStrike is extending Linux visibility by capturing more network events to enhance investigation. CrowdStrike is also extending vulnerability management coverage for Linux with the Spotlight module that offers real-time assessment of vulnerability exposure with zero impact on hosts. Firmware analysis for macOS informs customers if the BIOS is vulnerable or potentially compromised.
- Response: Operating system support for CrowdStrike Real Time Response is expanding to include both macOS and Linux. CrowdStrike Real Time Response gives administrators direct access to investigate and remediate remote hosts, quickly gathering information and returning their environment to a known secure state. Real Time Response gives responders the surgical remediation and investigation capabilities they require including the ability to kill processes, remove files or directories, retrieve data or files, or run custom scripts and executables on multiple systems.
- OS Support: CrowdStrike will fully support Apple's kernel extension software model on macOS Catalina and Big Sur. By leveraging Apple's Endpoint Security Framework, Falcon achieves the same levels of visibility, detection, and protection exclusively via a user space sensor. On Linux, new enhancements now also enable minor Linux kernel version updates to be supported immediately without requiring a Falcon sensor update.
- Customizability: CrowdStrike has completely revamped its dashboard capability with a rich new set of tools, filters, and visualizations. Customers can use new pre-configured dashboards or create custom views to track, measure and prioritize relevant insights based on their own business context. This allows users to choose the information that is relevant to them and then display it on a tailored dashboard. By giving users control over how to display their information, they can move away from "one size fits all" models and choose what is most relevant and best supports their unique business priorities.

To learn more about today's news and CrowdStrike's endpoint and workload protection capabilities, register for CrowdStrike's Cybersecurity Conference Fal.Con 2020, taking place on October 15, 2020!

About CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Qualifying organizations can gain full access to Falcon Prevent™ by starting a free trial.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | Twitter

View source version on businesswire.com: https://www.businesswire.com/news/home/20201013005254/en/

CrowdStrike, Inc.
Ilina Cashiola, 202-340-0517
Ilina.cashiola@crowdstrike.com

Source: CrowdStrike, Inc.