CROWDSTRIKE

FALCON X

Integrating threat intelligence into endpoint protection to automate incident investigations and speed breach response

BRINGING ENDPOINT PROTECTION TO THE NEXT LEVEL

As the threat landscape continues to evolve, security teams need all the help they can get to effectively prevent, detect and respond to threats. The more security teams know about who is attacking them, why they are being targeted and how attacks work, the better prepared they are to defend their organization. Implementing threat intelligence into a security team's workflow significantly enhances the speed and efficiency — not to mention the accuracy — of threat investigations.

Built on the CrowdStrike Falcon® platform, CrowdStrike® Falcon X™ brings endpoint protection to the next level by analyzing high-impact threats taken directly from endpoints that are protected by CrowdStrike. Falcon X automatically investigates incidents to accelerate alert triage and response. Falcon X threat intelligence is presented as part of the incident workflow, providing risk scores to enable prioritization, attribution to identify the attackers' intent and tradecraft, malware analysis to expose the attack behavior, and indicators of compromise (IOCs) to strengthen defenses and implement countermeasures.

By automatically enriching detections with threat intelligence, Falcon X helps smaller teams achieve a level of protection that would normally be out of reach and enables larger teams to operate more effectively.

KEY BENEFITS

Automates investigations into all threats that reach your endpoints

Enriches CrowdStrike Falcon detections with intelligence for faster, better decisions

Built into the Falcon platform, it is operational in seconds

Provides indicators of compromise (IOCs) to proactively guard against future threats and malware infections

Delivers pre-built integrations and application programming interfaces (APIs) to industry-leading security solutions

KEY CAPABILITIES

AUTOMATE AND SIMPLIFY INCIDENT INVESTIGATIONS

Gain seamless endpoint integration: Analyze high-impact threats taken directly from your endpoints that are protected by the CrowdStrike Falcon platform. Falcon X analysis is presented as part of the detection details of a Falcon endpoint protection alert. Security teams, regardless of size or skill level, will never miss an opportunity to learn from an attack in their environment.

Save time, effort and money: Automate each step of a cyber threat investigation and reduce analysis time from days to minutes. Falcon X combines malware analysis, malware search and threat intelligence into a seamless solution.

Visualize threats: The Falcon X Indicator Graph enables you to see and understand the relationships between IOCs, adversaries and the endpoints in your environment. Immediately visualize and explore how the threat has spread and which endpoints have been affected.

KNOW YOUR ADVERSARY

Stop bad actors in their tracks: CrowdStrike threat intelligence provides actor profiles to expose the motives, tools and tradecraft of the attacker. Practical guidance and proactive steps are prescribed so your team can deploy defensive countermeasures and get ahead of future attacks.

Get a weekly threat report: You'll receive a weekly email summarizing recently observed eCrime, cyber espionage and hacktivism activity. Also included are updates to public data exposures, breaches and more.

SHARE IOCs FOR SECURITY ORCHESTRATION

Defend against the most relevant threats: Focus your team on threats you actually encountered. Falcon X delivers IOCs that are generated from the malware analysis of threats taken directly from your endpoints. In addition, IOCs generated from malware from the same campaign, malware family or author are included.

Gain access to CrowdStrike IOCs: The CrowdStrike global IOC feed is a real-time, high-quality set of indicators created and curated by the CrowdStrike Intelligence team. The indicators in the IOC feed are enriched with context, including confidence level, attribution, related vulnerabilities, threat type and more.

Easily integrate countermeasures: Protect against future attacks with IOCs that are easily consumed by your security infrastructure. A rich suite of APIs and pre-built tools enables easy orchestration with existing security solutions.

FALCON X FEATURES

- Built into the CrowdStrike Falcon platform
- Falcon detections enriched with CrowdStrike Intelligence
- Automated malware analysis
- Real-time IOC feed
- Indicator graph
- Actor profiles
- Weekly threat updates
- APIs and pre-built third-party integrations

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint 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 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.