CROWDSTRIKE

FALCON ENDPOINT DETECTION AND RESPONSE (EDR)

Streaming the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike® Falcon Insight™ solves this by delivering complete endpoint visibility across your organization.

Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. All endpoint activity is also streamed to the CrowdStrike Falcon® platform so that security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

CROWDSTRIKE IS CONSISTENTLY RECOGNIZED AS A LEADING ENDPOINT PROTECTION SOLUTION

CrowdStrike is positioned as a leader in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms

CrowdStrike is validated against the MITRE ATT&CK™ framework to track and detect advanced attacks in MITRE Nation-State Emulation Tests, 2018

CrowdStrike is the only vendor positioned as a Leader in both the Forrester Wave™: Endpoint Detection and Response, Q3 2018, and the Forrester Wave: Endpoint Security Suites, Q3 2019

CrowdStrike scored highest in the October 2019 Gartner Critical Capabilities for Endpoint Protection Platforms among "Type A" organizations

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore™, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Insight uses IOAs (indicators of attack) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches. The CrowdStrike Threat Graph® database stores event data and answers queries in five seconds or less, even across billions of events.
- **Unravel entire attacks on just one screen:** The CrowdScore Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK™:** Mapping alerts to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) framework allows you to understand even the most complex detections at a glance, shortening the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.
- **Respond decisively :** Act against adversaries in real time to stop attacks before they become breaches. Powerful response actions allow you to contain and investigate compromised systems, and Falcon Insight Real Time Response Capabiltiies provide direct access to endpoints under investigation. This allows security responders to run actions on the system and eradicate threats with surgical precision.

GAIN FULL-SPECTRUM VISIBILITY IN REAL TIME

- **See the big picture in real time:** CrowdScore delivers a simple metric that helps an organization understand its threat level in real time. This makes it easy for security leaders to quickly understand if they are under attack and assess the severity of the threat so they can coordinate the appropriate response.
- **Capture critical details for threat hunting and forensic investigations:** Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.
- **Get answers in seconds:** The CrowdStrike Threat Graph database stores event data and answers queries in five seconds or less, even across billions of events.
- **Recall for up to 90 days:** Falcon Insight provides a complete record of endpoint activity over time, whether your environment consists of fewer than 100 endpoints or more than 500,000.

IMMEDIATE TIME-TO-VALUE

- **Save time, effort and money:** Cloud-enabled Falcon Insight is delivered by the CrowdStrike Falcon platform and does not require any on-premises management infrastructure.
- **Deploy in minutes:** CrowdStrike customers can deploy the cloud-delivered Falcon agent to up to 70,000 endpoints in less than a single day.
- **Immediately operational:** With unmatched detection and visibility from Day One, Falcon Insight hits the ground running, monitoring and recording on installation without requiring reboots, fine-tuning, baselining or complex configuration.
- **Zero impact on the endpoint:** With only a lightweight agent on the endpoint, searches take place in the Threat Graph database without any performance impact on endpoints or the network.

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.

DISCLAIMER:

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**

© 2020 CrowdStrike, Inc. All rights reserved.