CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Insight XDR

The world's leading AI-powered platform for unified endpoint detection and response (EDR) and extended detection and response (XDR)

Challenges

Today's adversaries are moving faster than ever. To keep pace, organizations continue to rely on a collection of disparate security tools to identify and mitigate threats. These siloed security tools are inherently ineffective, complicating and slowing incident detection and remediation.

To make matters worse, today's sophisticated threat actors know where to look for gaps in security silos. They can slip between defenses and move laterally across the network, flying under the radar for extended periods of time, lying in wait and gathering reconnaissance data for future attacks.

To outpace the adversaries, organizations must use EDR to optimize threat detection, investigation, hunting and response enterprise-wide, and employ native XDR to extend visibility and control across key attack surfaces.

Solution

As a global cybersecurity leader, CrowdStrike brings over a decade of expertise building the world's most advanced cloud-native platform and the industry's dominant EDR to pioneer a new approach: unified EDR and native XDR. The AI-native CrowdStrike Falcon® platform combines industry-leading threat intelligence with innovative detection and response technology to better understand and stay ahead of adversaries. CrowdStrike Falcon® Insight XDR extends enterprise-wide visibility, detects advanced threats and responds automatically across endpoints and beyond.

Key benefits

- Create a cohesive, more effective cybersecurity ecosystem
- Optimize security operations with prioritized, incident-driven insights
- Accelerate cross-domain threat analysis, investigation and hunting from a single console
- Speed response times and orchestrate action against sophisticated attacks
- Improve threat visibility and situational awareness across the enterprise
- Stop breaches that siloed tools and legacy approaches often miss

Key capabilities

Falcon Insight XDR correlates native cross-domain telemetry to deliver high-confidence detections, unprecedented investigative efficiency and rapid, confident response. Gain unparalleled visibility across your endpoints and enable your security team to detect and respond faster with one unified, threat-centric command console.

Gain more effective security outcomes

- **Tap into industry-leading EDR with native XDR in a single platform:** Start with the endpoint and easily activate extended capabilities to unlock native cross-domain detections, investigations and response across your entire enterprise.
- **Use AI-powered workflows with real-time collaboration:** Radically transform the speed and efficiency of investigations with the help of CrowdStrike® Charlotte AI™. Focus on incidents instead of alerts and engage AI to accelerate triage and investigation.* Accelerate response times with the lightning-fast Incident Workbench designed around incidents, not standalone alerts. Analysts can optimize workflows with intelligent entity linking, added cross-domain context, annotations, incident history tracking and more.
- **Gather, aggregate and normalize with ease:** Falcon Insight XDR unifies market-leading EDR with the power of native XDR for a more holistic view of your environment. Native first-party data, such as EDR telemetry, from modules across the Falcon platform provides an easy-to-understand view of an attack from start to finish.

Optimize security operations

- **Find attacks missed by siloed approaches:** Detect stealthy cross-domain attacks with industry-leading threat intelligence and world-class AI, providing a tight human feedback loop from CrowdStrike threat hunters, managed detection and response (MDR) experts and incident response (IR) specialists. Out-of-the-box and custom detection capabilities give you the power and flexibility you need to outpace the adversary.
- **Streamline triage and investigation:** Prioritized alerts, rich context and detailed detection information mapped to the MITRE ATT&CK® framework help analysts quickly understand and act on threats. The intuitive Falcon console lets you quickly tailor views, filter and pivot across data sets with ease. Automatic sandbox submissions and in-depth threat actor profiles allow for complete understanding of the threat and adversary behind it.
- **Rapid enterprise-wide deployment:** The Falcon platform's lightweight agent deploys across your organization in minutes for immediate protection. With comprehensive detection and visibility from Day One, the easy-to-use Falcon Insight XDR interface delivers an unrivaled analyst experience with seamless workflows across endpoint protection (EPP), EDR, XDR and threat intelligence for maximum efficiency.
- **Benefit from experts at the ready:** Strike the right balance of technology and expertise with pioneering 24/7 proactive threat hunting and the world's #1 MDR service with full-cycle remediation via a seamless optional upgrade. Falcon Insight XDR users benefit from the tight feedback loop between CrowdStrike's products and industry-leading experts, whether you manage the Falcon platform yourself or upgrade to Falcon Complete Next-Gen MDR for a fully managed experience.

Native Falcon Platform Data

- Endpoint detection and response (EDR)
- Identity
- Mobile
- Threat intelligence
- Vulnerability management
- Cloud security
- Data protection*

Free Third-Party Data Ingest

Uncover sophisticated threats across all key security domains — Falcon Insight XDR customers receive 10GB per day of free third-party data ingestion via CrowdStrike Falcon® Next-Gen SIEM with over 100 one-click connectors with parsers to enable seamless cross-domain detection and response.

* The above indicated section(s) include(s) forward-looking statements including, but not limited to, statements concerning the expected timing of product and feature availability, the benefits and capabilities of our current and future products and services, and our strategic plans and objectives. Such statements are subject to numerous risks and uncertainties and actual results could differ from those statements. Any future products, functionality and services may be abandoned or delayed, and customers should make decisions to purchase products and services based on features that are currently available.

Harmonize and simplify response across the enterprise

- **Rapidly respond with surgical precision:** Detailed detection information — from impacted hosts and root cause to indicators and timelines — helps to rapidly remediate threats. Powerful response capabilities such as Falcon Real Time Response (RTR) allow you to eradicate threats with surgical precision from anywhere in the world.
- **Take action across Falcon modules:** Trigger response actions across Falcon-protected hosts. One unified command console empowers analysts, from containing a host under attack to automatically enforcing more restrictive user access policies based on detection criticality.
- **Orchestrate and automate workflows:** CrowdStrike Falcon® Fusion SOAR security orchestration, automation and response automates and streamlines tasks, from notifications and repetitive tasks to complex workflows, dramatically improving the efficiency of your SOC teams.

Free Trial →

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/

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

The Endpoint Security Leader

Go from missed attacks and slow response to unbeatable protection with immediate ROI

100%
protection, visibility and analytic detection in the 2023 MITRE ATT&CK® Evaluations[1]

95%
reduction in mean time to respond, speeding triage from 4 hours to <10 min[2]

100%
ransomware protection in 2023 SE Labs test[3]

[1] MITRE Engenuity ATT&CK® Evaluations: Enterprise, Round 5

[2] These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on the individual customer's module deployment and environment.

[3] 2023 SE Labs Enterprise Advanced Security (EDR) Ransomware test