CROWDSTRIKE

NEWCOM
Authorized Partner

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 less effective, complicating and slowing threat 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

- Optimize security operations with prioritized, AI-powered 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, 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. All CrowdStrike EDR users get native XDR included at no additional cost to accelerate investigations with comprehensive endpoint, identity, cloud, and data protection telemetry from across the Falcon platform.

» **AI-powered workflows and real-time collaboration:** CrowdStrike® Signal and CrowdStrike® Charlotte AI™ elevate the speed, consistency, and effectiveness of your investigations, automating analyst workflows at the speed of agentic AI.

- **Automated leads powered by CrowdStrike Signal:** Go beyond alert triage with AI-generated leads that surface novel, potentially malicious activity specific to your environment. By intelligently correlating related indicators, CrowdStrike Signal delivers easy starting points for investigations. This helps analysts cut through the noise to quickly zero in on emerging threats and streamline triage from the start.
- **Charlotte AI Agentic Detection Triage and Charlotte AI Agentic Response:** Automate alert evaluation, prioritization, and remediation in one motion. Charlotte AI filters out false positives, highlights high-priority detections, and delivers tailored, step-by-step response actions aligned with managed detection and response (MDR) best practices, accelerating resolution while reducing analyst burden.

With CrowdStrike Signal and Charlotte AI, your SOC can act faster, stay focused, and scale response with confidence.

» **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 often 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, 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.

CrowdStrike: The Endpoint Security Leader

Avoid missed attacks and speed response with unbeatable protection that can accelerate ROI

100%
ransomware protection in the 2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test[1]

96%
more potential threats identified in half the time[2]

70%
reduction in mean time to respond (MTTR)[3]

Native Falcon Platform Data

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

[1] 2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test

[2] Results are from The Business Value of the CrowdStrike Falcon XDR Platform report from IDC. Individual results may vary by customer.

[3] These numbers reflect the median inputs provided by customers during pre- and post-sale motions that compare the value of CrowdStrike with incumbent solutions and are not guaranteed. They are intended to demonstrate potential value compared to incumbent solutions and do not represent promised outcomes. Actual value realized will depend on individual customer module deployment and environment.

- **Streamline triage and investigation:** Security analysts around the world can now collaborate on cases in real time from a unified source of truth via the Workbench view. Together, teams can triage, investigate, and respond as a unit to outpace the adversary. 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 the adversary behind it.
- **Get operational immediately:** The Falcon platform's single lightweight agent deploys in minutes and is immediately operational — no reboots required. With unmatched 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 CrowdStrike Falcon® Complete Next-Gen MDR for a fully managed experience.

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 of all skill levels to respond quickly, 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 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.

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.

NEWCOM

Call **NEWCOM** for more infortmation or a quote!
781.826.7989 | sales@newcomglobal.com
NEWCOMGlobal.com

© 2025 CrowdStrike, Inc. All rights reserved.