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 use XDR to extend visibility and control across all 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 industry's dominant EDR offering to pioneer a new approach: unified EDR and XDR. The CrowdStrike Falcon® platform combines the world's best 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 and third-party cross-domain telemetry to deliver high-confidence detections, unprecedented investigative efficiency and rapid, confident response. Gain unparalleled visibility across your endpoints and extended security ecosystem with third-party connectors for all key security domains, and enable your security team with one unified, threat-centric command console.

Gain more effective security outcomes

Tap into industry-leading EDR and XDR in a single platform: Start with the endpoint and easily activate extended capabilities to unlock cross-domain detections, investigations and response across your entire enterprise.

Create a cohesive, more effective cybersecurity ecosystem: Gain actionable insights by combining previously siloed data into one single source of security truth — a central repository for endpoint and cross-domain telemetry.

Gather, aggregate and normalize with ease: Falcon Insight XDR strikes the balance between EDR, native XDR and open XDR with a combined approach for the most holistic view of your environment. Native first-party data, such as EDR telemetry, from modules across the Falcon platform can be combined with normalized data from third-party sources to provide an easy-to-understand view of an attack from start to finish.

- Native XDR: Falcon Insight XDR correlates native data from across the entire Falcon platform at no additional cost* to truly unify security operations and paint the complete picture of advanced attacks beyond the endpoint.
- Open XDR: Also known as Hybrid XDR, purpose-built XDR integrations and a common data schema together enable third-party security data ingestion at massive scale. This open approach ensures security teams have the visibility they need in one unified XDR command console.

Best of both worlds

Falcon Insight XDR correlates both native and third-party cross-domain telemetry to supercharge your SOC.

Native Falcon platform data

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

Open ecosystem integrations

- Email
- Network detection and response (NDR)
- Identity and access management (IAM) and single sign-on (SSO)
- Security service edge (SSE)
  - Secure web gateway (SWG)
  - Cloud access security broker (CASB)

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.

Be immediately operational: 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. 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 XDR 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 the ecosystem: Trigger response actions across Falcon-protected hosts and through third-party solutions. One unified command console empowers analysts, from containing a host under attack to automatically enforcing more restrictive user access policies based on detection criticality through third-party solutions.

Orchestrate and automate workflows: CrowdStrike Falcon® Fusion security orchestration automation and response (SOAR) automates and streamlines tasks, from notifications and repetitive tasks to complex workflows, dramatically improving the efficiency of your SOC teams.

Newly announced Falcon Insight XDR capabilities*

Charlotte AI Investigator: Radically transform the speed and efficiency of investigations with Charlotte AI Investigator. Focus on incidents instead of alerts and engage AI to accelerate incident triage and investigation for analysts of all skill levels.

XDR Incident Workbench: Accelerate response times with this all-new lightning-fast user experience designed around incidents, not standalone alerts. Analysts can optimize workflows with intelligent entity linking, added cross-domain context, annotations, incident history tracking and more.

Collaborative Command Center: Security analysts around the world can now collaborate on incidents in real time from a unified source of truth. Together, teams can triage, investigate and respond as a unit to outpace the adversary.

XDR for All: Falcon Insight XDR 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.

*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.

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.

Free Trial →