CROWDSTRIKE

# FALCON INSIGHT XDR: EXTENDED DETECTION AND RESPONSE

Supercharge cross-domain detection, investigation and response across your extended security ecosystem, all from one command console

## CHALLENGES

Today, many organizations rely on a collection of disparate security tools to identify and mitigate threats. These siloed security implementations are inherently inefficient and ineffective. Detecting, isolating and remediating security incidents is resource-intensive, time-consuming and error-prone, and involves multiple platforms and administrative interfaces. To get to the bottom of an issue, security analysts are often forced to manually sift through and piece together volumes of diverse alert and event data generated by different systems.

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.

For more effective protection, organizations must optimize threat detection, investigation, hunting and response across environments and domains with extended detection and response (XDR).

## 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 endpoint detection and response (EDR) to pioneer a new approach to XDR. As EDR is the foundation of XDR, CrowdStrike customers have been leveraging the CrowdStrike Falcon® platform for cross-domain detection, investigation and response since the platform was built over a decade ago. From endpoint telemetry enriched with threat intelligence and network events to cross-domain visibility, integrated workflows and orchestrated response, organizations have made CrowdStrike the cornerstone of their security operations center (SOC).

With CrowdStrike Falcon Insight XDR™, CrowdStrike extends **industry-leading** outcomes to all key security domains as a foundational capability of the **Falcon** platform to deliver superior cross-domain detection, investigation and response capabilities and an unrivaled experience for security analysts to stop breaches.

## KEY BENEFITS

- Create a cohesive, more effective cybersecurity ecosystem
- Optimize security operations with prioritized, actionable detections and security 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 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 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

- **Create a cohesive, more effective cybersecurity ecosystem:** Surface actionable insights by combining previously siloed data into one single source of security truth — a central repository for cross-domain telemetry.
- **Gather, aggregate and normalize threat data with ease:** Purpose-built XDR integrations and a common data schema combine to funnel security data at massive scale, ensuring security teams have the visibility they need across their entire environment.
  - **Falcon platform data**
    - Endpoint detection and response (EDR)
    - Identity
    - Cloud workload
    - Mobile
    - Threat intelligence
    - Vulnerability management
    - Cloud security posture management (CSPM)
  - **Third-party integrations across key security domains from CrowdXDR Alliance partners and industry-leading vendors**
    - Email security
    - Web security
    - Cloud access security broker (CASB)
    - Network detection and response (NDR)
    - Firewall
    - Identity and access management (IAM)
- **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.

CrowdXDR Alliance

The CrowdXDR Alliance, formed with industry leaders and best-of-breed solutions, is a unified XDR coalition that offers a coordinated approach to true XDR for joint customers to protect their organizations from sophisticated adversaries in an evolving threat landscape.

Learn about the CrowdXDR Alliance:

**https://www.crowdstrike.com/partners/crowdxdr-alliance/**

## OPTIMIZE SECURITY OPERATIONS

- **Surface attacks missed by siloed approaches:** Detect stealthy cross-domain attacks when the world's richest threat intelligence, advanced analytics and artificial intelligence are working across your diverse ecosystem. Out-of-the-box and custom detection capabilities give you the power and flexibility you need.
- **Investigate cross-domain threats like never before:** Pivot from both CrowdStrike-generated and custom detections to a graph explorer, viewing the entire cross-domain attack path with rich context for quick understanding and confident response.
- **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.

## HARMONIZE AND SIMPLIFY RESPONSE ACROSS THE ENTERPRISE

- **Respond decisively:** Detailed detection information — from impacted hosts and root cause to indicators and timelines — guides remediation. Powerful response actions allow you to eradicate threats with surgical precision.
- **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 streamlines tasks, from notifications and repetitive tasks to complex workflows, dramatically improving the efficiency of your SOC teams.

## 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.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**



**Start Free Trial**
**of Next-Gen AV**

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