CROWDSTRIKE

CROWDSTRIKE FALCON XDR™

Supercharge detection and response across your security stack, 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 need to optimize real-time threat detection, investigation and hunting across environments and domains. They need extended detection and response (XDR).

SOLUTION

Falcon XDR™ extends CrowdStrike's industry-leading endpoint detection and response (EDR) capabilities and delivers real-time multi-domain detection and orchestrated response to improve threat visibility across the enterprise, accelerate security operations and reduce risk. The CrowdStrike Security Cloud correlates trillions of security events per day with indicators of attack, the industry's leading threat intelligence, and enterprise telemetry from across customer endpoints, workloads, identities, DevOps, IT assets and configurations. Falcon XDR seamlessly adds third-party telemetry from a wide range of security solutions to this threat-centric data fabric, powering the next generation of detection, protection and elite threat hunting to stop breaches faster.

KEY BENEFITS

- Create a cohesive, more effective cybersecurity stack
- Optimize security operations with prioritized, actionable detections and security insights
- Accelerate multi-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 XDR unifies detection and response across your security stack to take CrowdStrike's EDR technologies to the next level. Falcon and non-Falcon telemetry are integrated into one single command console for unified detection and response. Falcon XDR turns cryptic signals trapped in siloed solutions into high-efficacy, real-time detections and deep investigation context. Equipped with Falcon XDR, security professionals can more quickly and intuitively investigate, threat hunt and respond.

EMPOWER YOUR TEAM

- **Gather, aggregate and normalize threat data with ease:** Purpose-built XDR integrations and an open data schema combine to funnel security data at massive scale, ensuring security teams have the visibility they need across their environment.
  - CrowdStrike Falcon® platform data
    - Endpoint detection and response (EDR)
    - Identity
    - Cloud workload
    - Threat intelligence
  - Third-party supported domains
    - Email security
    - Web security/CASB
    - Network detection and response (NDR)
    - Firewall
    - Cloud security
    - Identity and access management (IAM)
    - And more
- **Focus on what matters:** Unveil actionable insights from previously siloed security data left in disparate, disconnected systems across your IT stack. Distill weak signals into high-fidelity, prioritized XDR detections.
- **Reduce the burden of finding threats:** Advanced Falcon XDR analytics and correlation across security telemetry automatically detect stealthy threats, eliminating the need for you or several people on your team to write, tune and maintain detection rules.

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/

GET THE RIGHT ANSWERS — FAST

- **Understand complex attacks at a glance:** Speed up triage and investigation with prioritized alerts, context and detailed detection information that is mapped to the MITRE ATT&CK® framework. View the entire multi-domain attack with the interactive graph explorer visualizing each step. The intuitive Falcon console lets you quickly tailor views, filter and pivot across data sets with ease.
- **Schedule searches and create custom detections:** Build custom scheduled queries and detections for behaviors and activity unique to your organization.
- **Search at blazing speed and scale:** Search index-free across structured and unstructured data from any XDR source to accelerate cross-domain threat hunting and investigation.

TURN XDR INSIGHT INTO ORCHESTRATED ACTION

- **Stop attacks before they become breaches:** Contain hosts associated with suspicious activity instantly — right from the detection.
- **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.
- **Orchestrate and automate workflows:** Falcon Fusion streamlines tasks from notifications and repetitive tasks to complex workflows, dramatically improving the efficiency of your security operations center (SOC) teams.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms 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**