

Data Sheet

EDR AND NDR

Stop breaches faster with powerful unified endpoint detection and response (EDR) and network detection and response (NDR) for defense in depth

CHALLENGES

With cloud adoption surging and workforces becoming increasingly remote, it is more critical than ever for organizations to maintain comprehensive real-time visibility of their digital assets, regardless of location, to avoid any blind or weak spots that can be harnessed by bad actors and result in compromised or breached environments. Uncoordinated responses across the network edge and devices could result in two problems: 1) a waste of costly time and resources on alerts across multiple, siloed systems that do not talk to each other, and 2) even worse, threats that may go unattended for days and be weaponized for malicious intent.

SOLUTION

Network detection and response (NDR) and endpoint detection and response (EDR) solutions form two pillars of the security operations center (SOC) visibility triad — SIEM is the third — to bring network and endpoint telemetry together for faster incident investigation and response, without negatively impacting productivity.

The CrowdStrike Falcon® platform supports a rich, pre-built and validated series of integrations with leading NDR and network threat analytics (NTA) partners. These integrations help organizations build a cohesive platform to create end-to-end visibility, and defend against any threats wherever those threats are encountered — from network edge to the cloud, and across endpoints and workloads. These integrations facilitate the sharing of contextual information and indicators of compromise (IOCs) across ecosystem vendors to help security teams become effective and efficient by providing early detection of complex attacks focused on endpoints or networks. The result is a well-coordinated response and remediation strategy.

KEY BENEFITS

Provides actionable and contextual insights across CrowdStrike Falcon and leading NDR solutions

Speeds threat investigation and response with integrated data feeds and workflows

Delivers enriched threat intelligence to identify threats across any attack surface

Allows for operational simplicity with cloud-delivered extensibility and flexibility



BUSINESS VALUE

Stop breaches faster with EDR and NDR that provides:

- Concise and actionable insights based on coordination of alerts and telemetry across CrowdStrike Falcon and leading NDR solutions
- Integrated data feeds that enable enhanced response capabilities, allowing customers to identify and isolate risks faster by leveraging cloud-scale artificial intelligence
- Better threat intelligence for novel attacks — EDR and NDR work together to identify new attack signatures
- Sharing of CrowdStrike IOCs to allow NDR technologies to terminate network communications with a malicious host at the network level, providing a secure perimeter and an extra layer of defense
- Customizable response actions that are available for partners to execute leveraging Real Time Response (RTR) capabilities on the Falcon platform, based on early attack behaviors observed on the network
- Open ecosystem of purpose-built integrations for cloud-delivered extensibility and flexibility

KEY CAPABILITIES

- **Enhanced visibility:** Combining visibility in network communication with device telemetry gives customers broad visibility into and oversight of their networks and its devices and users, thus removing blind spots.
- **Extended threat lifecycle management:** Customized policies and real-time, behavior-based discovery — using machine learning with aggregation of contextual network and endpoint telemetry — results in faster detection of anomalous behaviors and threats between devices and the network edge, and within internal network traffic.
- **Streamlined investigations and response:** Break down silos across NDR and Falcon products with seamless integrations and data aggregation that provide security analysts with a full range of incident information to use in their triaging and investigations — speeding up incident response and mitigating risk.
- **Frictionless automation:** Create easy data schemes with contextual insights across endpoints and networks without manual rules, API changes or professional services engagements, and execute automated response scripts, achieving scale and efficiency in responding to cyber threats.

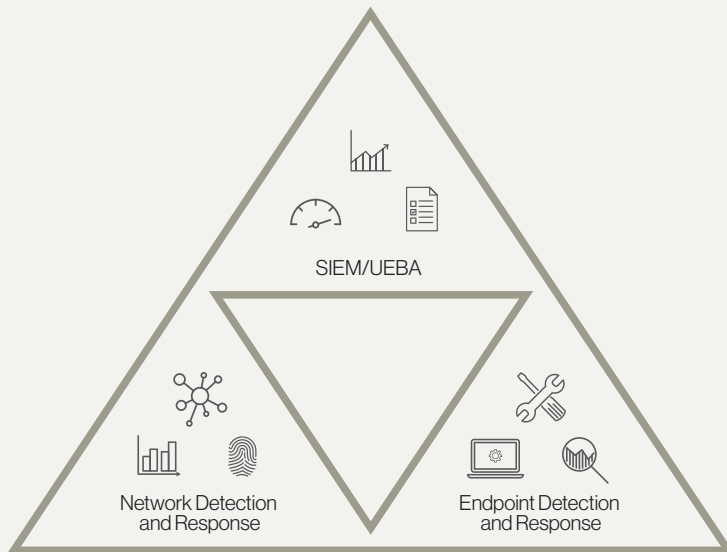
“CrowdStrike’s seamless integration with NDR partners provides mutual customers a comprehensive, holistic cybersecurity solution with enhanced visibility, streamlined detection and response and frictionless automation to address protection and operational challenges, while helping drive total cost of ownership down.”

Amol Kulkarni

Chief Product Officer, CrowdStrike

INTEGRATION DETAILS

CrowdStrike has joined with NDR partners to help provide users with enhanced information for detecting advanced threats and speeding remediation decisions, strengthening the organization's security posture from network edge to cloud.



With dynamic asset discovery, joint customers will be able to get real-time information about every device connected to their network, including whether that device was instrumented with the Falcon agent and what the status of the device's hygiene is. Customers can quickly identify any IOT devices, unmanaged devices or shadow IT devices and deploy CrowdStrike for detection and response on the endpoint. Leveraging the Falcon RTR framework, the integration offers fine-grained controls over which types of network threats result in auto-containment, delivering precise results based on high-fidelity data that minimizes both business disruption and risk exposure.

As cyberattacks escalate in speed and sophistication, defenders need tools that help them stay ahead. Seamless security integrations between NDR and the Falcon platform ensure the right data is available at the right time to the right people, and by automating security tasks that once took manual intervention, security teams maximize their productivity and efficiency.

Learn more at www.crowdstrike.com

NDR PARTNERS SUPPORTED

ExtraHop

Vectra

Arista Awake Security

Corelight

Darktrace

IronNet

ThreatWarrior

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

