CROWDSTRIKE

CrowdStrike Services

Data Sheet

Network Detection Services

Delivering complete network visibility, detection and threat hunting as a service

Network blind spots and silent failure

Blind spots in the network and the silent failure of traditional intrusion detection systems expose organizations to a wide range of potential threats including IP theft, ransomware, malware and other more destructive attacks.

Proprietary devices and the Internet of Things (IoT) — including critical industrial, manufacturing and medical devices, which lack the protection of traditional endpoints — are susceptible to attacks over the network.

To find the latest threats, security operations leaders need to identify potential threat activity occurring within their network so they can respond quickly to a network intrusion and accelerate the investigation of and response to a cyberattack.

Powerful network detection with complete visibility

CrowdStrike Network Detection Services helps correlate high-fidelity security telemetry across endpoints, identities and network devices to gain complete visibility into malicious threat actors operating within your network.

CrowdStrike and CrowdXDR Alliance partner Corelight natively integrate to provide unified technology that delivers network detection and response with complete visibility to network intrusions, lateral movement and cyberattacks across endpoints, identities and unprotected network devices.

Detect threat activity across your network with this CrowdStrike and Corelight integrated solution. Contain and eject adversaries from your network before they disrupt your business operations.

Key benefits

Gain complete visibility across your entire network to learn if attackers have breached your defenses and are moving undetected across your environment

Get next-level analytics to correlate high-fidelity security telemetry across endpoints, identities and network devices

Accelerate the investigation and response to network intrusions

Proactively hunt for threats through network metadata to detect new and unknown attacks

Key service features

Network visibility and analysis

- Gain the network visibility necessary to detect threats and enable threat hunting at the network layer.
- Augment your current security tools that cannot provide the visibility necessary in potential threat vectors like end-of-life operating systems, unmanaged endpoint devices, network devices and IoT devices.
- Go beyond known threats to hunt for unknown threats using next-generation intrusion detection with integrated network metadata analysis and smart packet capture.
- Detect non-malware attacks based on behavioral sequences and the integration of CrowdStrike threat intelligence.

Multi-faceted detection capabilities

- Use indicators of compromise (IOCs) and indicators of attack (IOAs) from CrowdStrike threat intelligence to hunt for threats using network protocol metadata analysis.
- Find command-and-control (C2) activity using advanced analytics to identify attacks hiding in encrypted traffic.
- Streamline network traffic with smart packet capture to extract malware and enable analysis of at-risk data.
- Get all of the benefits of a fully integrated intrusion detection system (IDS).

Flexible deployment options

- Choose your deployment option with hardware, software, cloud or virtual sensors.
- Rapidly deploy to your existing hypervisors via virtual sensors, saving you time, effort and money.
- Opt for physical or virtual sensors that are easy to deploy, install and use and are designed to work effectively within your current IT stack.

About CrowdStrike Services

CrowdStrike Services delivers Incident Response, Advisory Services, Technical Assessments, Product Support and Training that help you prepare to defend against advanced threats, respond to widespread attacks, enhance your cybersecurity practices and controls and operationalize your technology platform.

We help our customers assess and enhance their cybersecurity posture, implement technologies, test defenses against real-world attacks, respond to incidents, accelerate forensic investigations, and recover from a breach with speed and precision. Harnessing the power of the CrowdStrike® Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary-focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike:

We stop breaches.

Why choose CrowdStrike?

CrowdStrike unified XDR platform: CrowdStrike Falcon® Insight XDR delivers a unified view of threat detections across endpoints, identities and network traffic (powered by Corelight).

Corelight Open NDR technology: Corelight Open NDR technology integrates with Falcon Insight XDR to provide smart packet capture to streamline network visibility and close gaps in network intrusions, including IoT and ICS environments.

CrowdStrike expert threat hunting: CrowdStrike expert threat hunters take advantage of correlated high-fidelity security telemetry with CrowdStrike threat intelligence to accelerate the investigation of a cyberattack.

Learn more
www.crowdstrike.com/services/

Email
services@crowdstrike.com