CROWDSTRIKE

FALCON NETWORK SECURITY MONITORING

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

POWERFUL NETWORK SECURITY MONITORING FOR COMPLETE VISIBILITY

To find the latest threats, security teams need increased visibility across their networks, including areas not covered by other tools currently in their security stack. Yet they struggle to see the full context of unusual network behavior that's required to adequately monitor and defend their businesses against new, unknown potential attacks.

CrowdStrike Falcon® Network Security Monitoring is a service that utilizes both the expertise of CrowdStrike® Services threat hunters and a network appliance that detects threats present in a customer's environment. It's easy to provision, install and use, and provides the necessary visibility to prevent new attacks. Additionally, it detects traffic to and from unmanaged devices and services in the customer's environment, without the burden of managing yet another agent on the organization's endpoints. This extensive capability for detection, response and threat hunting leverages CrowdStrike's machine-learning capabilities as well as CrowdStrike Intelligence indicators of compromise (IOCs) and indicators of attack (IOAs) to detect both known and unknown malicious activity.

KEY BENEFITS

Provides visibility across your entire network, analyzing network traffic and hunting for threats to detect the next attack on your environment

Integrates the latest IOCs and IOAs from across the globe to detect threats quickly

Utilizes multifaceted detection mechanisms to detect both known and unknown threats and unusual network behavior

Enhances your endpoint protection solution with complete visibility of network traffic and intrusions

Includes an easy-to-use physical or virtual appliance that delivers frictionless deployment with no additional hardware required, reducing your IT costs

FALCON NETWORK SECURITY MONITORING

KEY CAPABILITIES

- **Network visibility and analysis:** Falcon Network Security Monitoring provides your organization with the network visibility necessary to detect threats and enable threat hunting. It augments 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 Internet of Things (IoT) devices. It goes beyond known threats and hunts for unknown threats with powerful threat hunting through network protocol metadata analysis. With CrowdStrike Intelligence integration, IOCs and IOAs identify threats based on behavior. Understanding sequences of behaviors allows Falcon Network Security Monitoring to detect non-malware attacks.
- **Multi-faceted detection capabilities:** Gain complete network visibility to detect threats faster, before they disrupt your business operations. Falcon Network Security Monitoring offers:
  - Powerful threat hunting through network protocol metadata with IOC detection leveraging CrowdStrike Intelligence
  - Automated IOA detection using network metadata with machine-learning-enabled detection of malicious files
  - Full network traffic capture to extract malware and enable analysis of at-risk data
  - A fully integrated intrusion detection system (IDS)
- **Network appliances:** Choose between physical network appliances or virtual network appliances.
  - The Falcon Network Security Monitoring virtual appliance offers rapid deployment to your pre-existing hypervisors, saving you time, effort and money.
  - Both physical and virtual appliances are easy to deploy, install and use. They are designed to work effectively within your organization's current IT stack. Falcon Network Security Monitoring is the fastest and easiest way to get the visibility needed to detect attacks across your network.

ABOUT CROWDSTRIKE SERVICES

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

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations, and recover from a breach with speed and precision. Harnessing the power of our 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.**

Learn more at **www.crowdstrike.com/services/**
Email: **services@crowdstrike.com**

WHY CHOOSE CROWDSTRIKE?

CrowdStrike Falcon Network Security Monitoring provides an extensive network security monitoring capability for detection, response and threat hunting.

Global threat indicators: CrowdStrike uses machine learning combined with CrowdStrike Intelligence IOCs and IOAs to detect malicious activity across security events globally

Efficient threat hunting: Falcon Network Security Monitoring provides the extra visibility necessary to detect new attacks and enable faster, more efficient threat hunting across all of the data traversing your network

Network-level detection: Falcon Network Security Monitoring uses industry-standard signatures for efficient and in-depth intrusion detection and file-level malware detection