CrowdStrike Products

CROWDSTRIKE

FALCON DISCOVER FOR IoT

Comprehensive visibility across IT and OT environments to secure against industry-targeted cyberattacks

LIMITED VISIBILITY OF ASSETS LEAVES ORGANIZATIONS VULNERABLE TO CYBERATTACKS

Critical infrastructure systems remain vulnerable to cyberattacks, and organizations realize the need to secure their industrial control system (ICS) in conjunction with the assets contained in their information technology (IT) and operational technology (OT) systems. Yet according to a 2021 SANS Institute **report**, "asset inventories continue to challenge most organizations, with only 58.2% having a formal process."

Part of the challenge is that industrial control and OT systems have typically been less rigorously secured than IT systems because of limitations in legacy security controls. Organizations' IT and OT systems have therefore traditionally been kept separate, with their networking and security requirements managed by two different teams. But over time, the lines between IT and OT have increasingly blurred as systems — including the Internet of Medical Things (IoMT) and Internet of Things (IoT) — have become more interconnected with the aim of enhancing business processes and improving efficiency.

While interconnected systems have led to business improvements, they have also increased security risks as traditional IT security tools cannot be extended to OT environments because of differences between the two systems' protocols, operating systems, and performance requirements and constraints. As a result, adversaries that attack an industrial organization's ICS and IoT/IoMT devices have been able to take advantage of interconnected networks by entering an organization's IT network or exposed cloud-to-edge services and then pivoting to the OT environment to achieve their goal of disrupting critical infrastructure or exfiltrating data.

Further, because security as a non-functional requirement has frequently taken a back seat to the functional requirements of IoT and smart devices, cyberattacks resulting from a compromised identity or service account or a vulnerable ICS asset can remain undetected for months. Ransomware is the most common threat to organizations with large industrial control, IoT and OT systems, with new ransomware families springing up and old favorites persisting due to inconsistent patching and insufficient security hygiene.

KEY BENEFITS

- **Minimize risk associated with asset inventory**: Accelerate converging your IT/OT security stack for an up-to-date inventory of IT, OT and IoT assets to mitigate risk exposure.
- **Gain comprehensive deep visibility**: Eliminate blind spots associated with unmanaged or unsupported legacy systems and quickly uncover hidden threats with deep, contextual visibility and analysis.
- **Enable continuous real-time asset monitoring**: Leverage CrowdStrike Asset Graph to provide contextual endpoint and network asset visibility, identify application context, monitor critical assets and secure unmanaged assets.
- **Get powerful context enrichment through third-party integrations**: Seamlessly integrate with third-party IoT security vendors to enrich asset and network visibility and achieve comprehensive understanding across ICS/OT environments.

FALCON DISCOVER FOR IoT PROVIDES ASSET VISIBILITY FOR IT, OT AND IoT IN ICS ENVIRONMENTS

CrowdStrike is extending security hygiene across ICS, IT and OT environments with Falcon Discover for IoT™ to address the challenges facing securty teams.

Customers can bridge the gap between IT and OT environments using CrowdStrike's device- and identity-centric approach to secure their IT and OT infrastructure with cloud-scale architecture and a lightweight unified agent. With the CrowdStrike Falcon® platform integrated into ICS/IoT ecosystem partners to secure the organization's OT footprint, security teams can expand beyond traditional network defense to see, monitor and defend their full environment. Comprehensive monitoring and visibility across entire IT and OT environments, spanning managed and unmanaged devices and legacy systems, helps identify sophisticated adversaries targeting ICS/IoT-based systems.

KEY CAPABILITIES

CENTRALIZED DASHBOARD PROVIDING ASSET INVENTORY, MANAGEMENT AND RELATIONSHIP

Gain full visibility of all assets regardless of managed, unmanaged or unsupported status, and organize them in a customizable dashboard that centralizes data from the Falcon platform and third-party vendors. Utilizing CrowdStrike Asset Graph, the dashboard collects CrowdStrike data that's been integrated with third-party data to provide contextual visibility of assets and their relationships. Because the dashboard consolidates multiple data providers, you can easily view a holistic representation of all of your assets in a single pane.

CONTEXTUAL AND ENRICHED ASSET AND NETWORK VISIBILITY

With Falcon Discover for IoT, you get in-depth ICS context including data such as component type, protocols in your environment, the security zones the assets belong to, IP or MAC addresses within the asset, and what the devices are communicating to. With customizable views and filters, you can quickly navigate to the information you need for comprehensive visibility to minimize risks.

REAL-TIME ASSET MONITORING

Proactively reduce your attack surface with real-time mapping of asset relationships and contextual information including risk factor, device identities, which devices are talking to each other and what applications are associated with each asset. Benefit from true real-time monitoring as the lightweight CrowdStrike Falcon agent is continuously running on the device, and third-party solutions provide visibility the moment any device hits the network. This asset recognition data is housed securely into a data layer within the platform and can be exported to a third-party workflow provider to streamline your security program.

COMPREHENSIVE VISIBILITY ALL IN ONE PLACE

Eliminate blind spots with visibility into what applications are running, and which ICS applications are in your environment, as the Falcon platform is positioned for an ICS supervisory layer. With the integration of network vendors across the technology stack, you can get a valuable vantage point of asset dependencies as well as a network-based detection to help proactively prevent breaches and minimize risk of exposure.

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 a free trial today: **https://www.crowdstrike.com/free-trial-guide/**