Data Sheet

Falcon Insight for IoT

Protect extended Internet of Things (XIoT) assets with the industry's leading XDR platform purpose-built to stop breaches

Challenge

Securing XIoT Assets from Advanced Adversaries

As IT and operational technology (OT) networks converge, threats that were once protected by "air-gapped" industrial control system (ICS) networks are compromising extended Internet of Things (XIoT) assets — which include IoT, OT, Industrial Internet of Things (IIoT), Internet of Medical Things (IoMT) and Industry 4.0 assets — and creating business disruption, financial loss and harm to brand reputation. Security teams have been left with ineffective security controls to prevent, detect and respond to advanced threats like ransomware. As shown in the **CrowdStrike 2023 Global Threat Report**, manufacturing was the fifth most targeted industry in interactive intrusion activities observed in 2022.

Compounding the problem, traditional security tools designed to protect IT assets are not capable of defending XIoT assets due to a lack of interoperability and tailored protection. As a result, organizations are left with downtime, blind spots and ineffective protections that let adversaries compromise and move laterally throughout ICS networks undetected.

To prevent, detect and respond to threats to XIoT assets, organizations need targeted protection that doesn't introduce business disruption and eliminates silos.

Solution

Comprehensive Protection for XIoT assets

CrowdStrike Falcon® Insight for IoT is purpose-built to stop breaches for XIoT, delivering tailored threat prevention, detection and response that won't disrupt operations. Rigorous testing of CrowdStrike's lightweight Falcon agent by leading ICS vendors underscores its benefits: fast and simple deployment, comprehensive interoperability and safety for mission-critical XIoT assets. Falcon Insight for IoT extends world-class protection across the entire enterprise, removes blind spots by breaking down IT/OT silos and delivers best-in-class ROI.

As a global cybersecurity leader, CrowdStrike brings more than a decade of expertise protecting over 76 million critical assets for 23,000+ customers in every industry, including manufacturing, automotive, healthcare, oil and gas, and more. Building on powerful endpoint detection and response (EDR) and extended detection and response (XDR) for IT assets, CrowdStrike delivers holistic security for XIoT assets with Falcon Insight for IoT.

Key Benefits

Stop breaches on mission-critical XIoT assets: Shut down adversaries by extending CrowdStrike's industry-leading EDR/XDR protection to XIoT—without downtime and with negligible system burden.

Enable rapid, proven response for hard-to-patch assets: Instantly contain threats with integrated response actions such as host/process containment and USB device control that won't disrupt operations.

Protect your assets with a tested and validated solution: Get industry-leading protection that won't bring down ICS systems — the lightweight Falcon agent has been validated for interoperability with mission-critical XIoT assets by leading ICS vendors.

Key Capabilities

Stop XIoT Threats at the Source

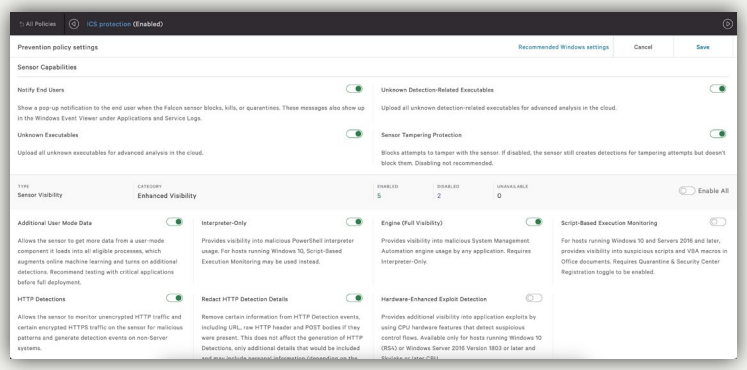
- **Stop threats at the source** with tailored threat prevention policy for XIoT assets.
- **Reduce performance impact** to ensure the effectiveness, interoperability and safety of XIoT assets.
- **Easily manage sensor updates** so you have time to test before deploying.

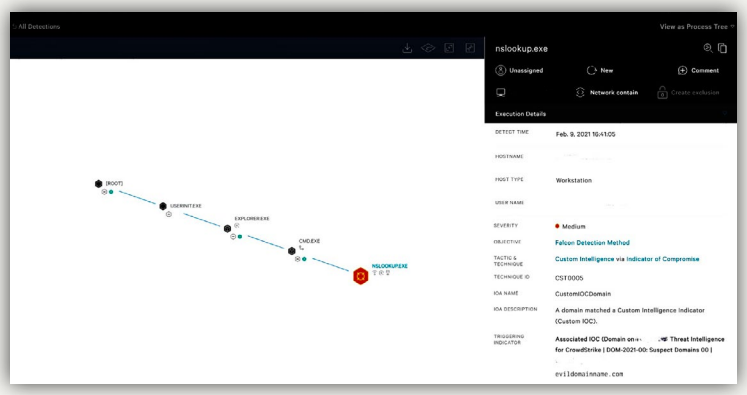
Reduce Risk with Powerful XIoT Detections

- **Reduce risk** by detecting threats to XIoT assets with deep context powered by artificial intelligence (AI), machine learning (ML) and actionable threat intelligence.
- **Ensure business continuity** by identifying threats like ransomware and malicious project file modifications.
- **Build a cohesive picture of threat activity** with telemetry ingested and analyzed across your enterprise.

Enable Rapid, Proven Response for Hard-to-Patch Assets

- **Limit the attack blast radius** by blocking traffic and containing compromised hosts and processes without disrupting operations.
- **Safeguard operations** from ransomware by limiting/revoking access to project files.
- **Streamline operations** with response actions through third-party tools — like Claroty, a CrowdStrike Store partner that helps secure cyber-physical systems — and automate repetitive tasks with CrowdStrike Falcon® Fusion.





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
of Falcon Pro

Learn more at **www.crowdstrike.com**