

Falcon for XIoT: Critical Infrastructure Asset Protection for Government Institutions

Unified XIoT security for mission-critical environments

Rapidly expanding attack surfaces driven by connected, traditionally unmanaged devices are proliferating across critical infrastructure that supports government institutions and agencies. These organizations play an essential role in serving the public, so ensuring operational resilience is critical.

Government agencies and institutions must implement cybersecurity processes and controls while balancing the rigorous federal, state, or local regulations required to effectively deploy security tools and controls across critical infrastructure. This has driven demand for solutions that can deliver comprehensive extended internet of things (XIoT) visibility, risk prioritization, and platform deployment within a FedRAMP High authorized architecture.

A modern platform approach to XIoT security

CrowdStrike's FedRAMP High authorized offering, Falcon Platform for Government, now includes CrowdStrike Falcon® for XIoT, providing asset visibility and protection across mission-critical government infrastructure. The Falcon platform enables automated asset discovery and profiling for systems such as power grid controls, smart building sensors, and connected medical devices. Using XIoT-specific asset and adversary context, Falcon identifies and prioritizes the exposures most likely to be exploited, analyzes unique operational technology (OT) device context and automation, and provides actionable remediation recommendations.

Key capabilities

Native XIoT Asset Discovery on FedRAMP High Authorized Architecture

CrowdStrike delivers native XIoT asset discovery on the Falcon platform's FedRAMP High authorized architecture, providing government agencies with visibility into OT and IoT environments without introducing operational disruption.

- Zero-touch XIoT asset discovery using the existing Falcon sensor with no additional scans, sensors, or hardware required
- Real-time visibility across XIoT assets, such as smart building systems, industrial control systems (ICS), power grid controls, connected medical devices, and more
- Operation within a FedRAMP High authorized environment to support strict federal security and compliance requirements
- Deep protocol support and ICS vendor validation to maintain asset safety and operational integrity

Key benefits

- **Complete Asset Visibility:** Gain a real-time, unified view of all XIoT assets to help mitigate operational disruptions and support strict federal security and compliance requirements.
- **AI-Driven Risk and Threat Detection:** Identify, prioritize, and address vulnerabilities and exposures across XIoT assets with industry-leading threat protection and services.
- **Unified IT and OT Convergence:** Close blind spots, reduce operational complexity, and detect lateral movement across converged attack surfaces with Falcon's unified protection through a single lightweight sensor and centralized console.

AI-powered Risk Prioritization for XIoT

CrowdStrike applies AI-powered analysis and XIoT-specific context to help agencies identify, prioritize, and address risk across converged IT and OT environments, focusing attention on the exposures most likely to be exploited.

- Risk analysis through [ExPRT.AI](#), CrowdStrike's AI-powered risk scoring that goes beyond traditional CVSS scoring by evaluating exploitability, asset criticality, network exposure, and adversary context
- Insights that surface additional high-risk conditions, including legacy assets, unsupported devices, and vulnerable hosts
- Automated remediation workflows and accelerated risk reduction across IT and OT environments using CrowdStrike Falcon® Fusion SOAR orchestration

Real-Time Detection and Response for XIoT

CrowdStrike delivers industry-leading threat protection and services for XIoT assets, extending real-time visibility, threat detection, and response across unmanaged and hard-to-secure devices without disrupting critical operations.

- Comprehensive, contextual detection of XIoT assets with the Falcon platform's AI-native detection and response
- Detection of lateral movement and support for IT/OT boundary protection across converged attack surfaces
- Add-on managed detection and response (MDR) service with CrowdStrike Falcon® Complete Next-Gen MDR that correlates XIoT telemetry to provide continuous, expert-led investigation and response

Unified Security Across IT and OT Environments

CrowdStrike provides unified visibility and protection across IT and OT through a single lightweight sensor and centralized console.

- Closes blind spots between traditional IT systems and operational technology
- Reduces complexity by consolidating IT and OT security within the Falcon platform
- Detects lateral movement and supports continuous detection and response across converged attack surfaces

CrowdStrike Products

Falcon for XIoT: Critical Infrastructure Asset Protection for Government Institutions

Vulnerabilities

Total vulnerabilities

14

Remediations

Total recommended

7

Installed patches

Last patch confirmed

Jun. 15, 2024

Vulnerabilities

3 items

Go to full table

Asset confidence : 1 excluded

Exploit status

ExPRT rating

Host groups

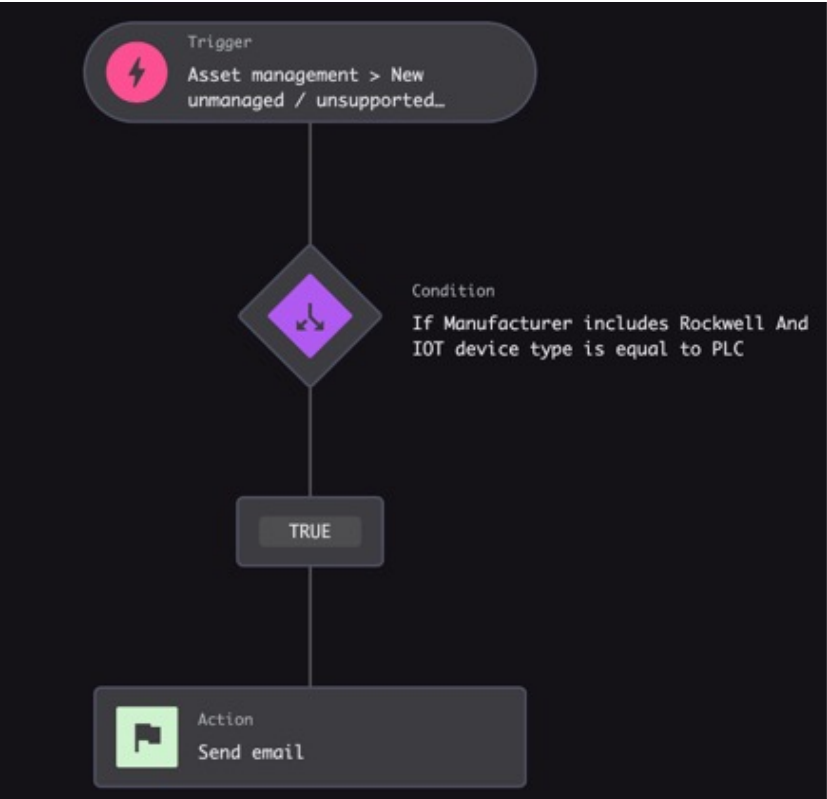
Product : 2 applied

Vulnerability confidence : 1 excluded

Vulnerability ID

Vulnerabil...	ExPRT rat...	CVSS sev...	Exploit st...	Remediation	Vulnerable pr...
CVE-2024-46...	Medium	High	Unproven	Update Rock...	FactoryTalk V...
CVE-2022-38...	Low	High	Unproven	Update Rock...	FactoryTalk A...
CVE-2023-46...	Low	High	Unproven	Update Rock...	FactoryTalk V...

Falcon for XIoT identifies vulnerabilities and exposures on FedRAMP High authorized architecture.



Unique high-risk asset conditions surrounding OT devices can be identified in the Falcon platform.

See Falcon for XIoT in action in this demo

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.

Learn more: <https://www.crowdstrike.com/>

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

