

Falcon for XIoT: Critical Infrastructure Asset Protection for the Utilities Sector

Secure IoT and OT devices for energy and utilities

Rapidly expanding attack surfaces driven by connected, traditionally unmanaged devices are proliferating across critical infrastructure that powers the utilities sector, including electricity, water, gas, and renewables. These institutions and infrastructure power the backbone of society, and ensuring operational resilience is critical.

Utilities environments consist of a wide range of connected assets — such as smart meters, grid automation technologies, and SCADA systems — that require nuanced controls outside of traditional IT security to properly protect them. Many of these assets may lack native security controls, rely on legacy protocols, and have limited tolerance for downtime.

A Modern Platform Approach to XIOT Security

CrowdStrike Falcon® for XIoT is a purpose-built solution that enables energy and utilities organizations to efficiently secure their IoT and OT assets. It addresses the unique security challenges of XIoT infrastructure by providing safe and accurate XIoT asset discovery and visibility. Falcon for XIoT is delivered through the CrowdStrike Falcon® platform — which has ICS vendor validation and FedRAMP High authorization — and combines AI-powered risk analysis and industry-leading threat detection to unify security across IT and OT environments.

Key benefits

- **Complete Asset Visibility:** Gain a real-time, unified view of XIoT assets that power energy and utility infrastructure without introducing operational disruptions.
- **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.

Key capabilities

Robust XIoT Asset Discovery and Visibility

CrowdStrike delivers native XIoT asset discovery with ICS vendor validation and on FedRAMP High architecture, providing the utilities sector with safe, industry-compliant asset visibility into OT and IoT environments while mitigating operational disruption across mission-critical infrastructure.

- Zero-touch XIoT asset discovery with no additional scans, sensors, or hardware required, using the existing Falcon sensor
- Real-time visibility across XIoT assets, such as smart building systems, power grid controls, renewable energy substations, and more
- Operation within a FedRAMP High authorized environment when federal, state, or local security and compliance requirements apply
- Deep protocol support and ICS vendor validation to maintain asset safety and operational integrity

AI-Powered Risk Prioritization for XIoT

CrowdStrike applies AI-powered analysis and XIoT-specific context to help organizations 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
- Operational status monitoring across modern utilities infrastructure to address specific industry risk requirements such as NERC-CIP compliance

Industry-Leading Endpoint 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 within a unified platform
- Add-on managed detection and response (MDR) service that analyzes and correlates XIoT telemetry, providing continuous, expert-led investigation and response for security management operations and support

Unified Security Across IT and OT Environments

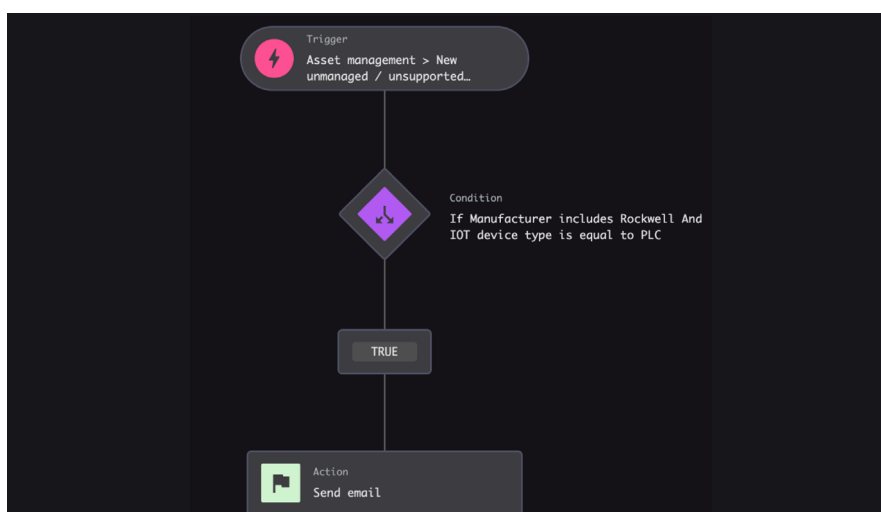
CrowdStrike provides unified visibility and protection across IT and OT through a single lightweight sensor and centralized console.

- 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

The screenshot displays the Falcon console interface with three main summary cards at the top: 'Vulnerabilities' (Total vulnerabilities: 14), 'Remediations' (Total recommended: 7), and 'Installed patches' (Last patch confirmed: Jun. 15, 2024). Below these is a 'Vulnerabilities' section with 3 items, including filters for 'Asset confidence', 'Exploit status', 'ExPRT rating', 'Host groups', 'Product', and 'Vulnerability confidence'. A table of vulnerabilities follows, with columns for Vulnerability ID, ExPRT rating, CVSS severity, Exploit status, Remediation, and Vulnerable product.

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 that may have the biggest impact on critical energy and utilities environments.



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

See Falcon for XIoT in action

Watch the 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/>

