

Falcon for XIoT

Comprehensive security for mission-critical
XIoT assets

Challenge: Mission-critical assets lack modern security

From industrial control systems (ICSs) to medical devices, the Extended Internet of Things (XIoT) underpins critical operations in virtually every industry. But these interconnected devices introduce a host of challenges: They lack robust built-in security controls, sprawl across hybrid IT/operational technology (OT) environments, and often operate with outdated or unpatched software. As a result, each newly connected sensor, controller, and endpoint becomes a potential foothold for attackers, threatening not only data but also physical processes and human safety.

Rising cyber threats further complicate this landscape, with adversaries leveraging ransomware and identity-based tactics to damage XIoT ecosystems. Meeting compliance mandates is a constant struggle, as organizations must ensure operational resilience without sacrificing visibility, performance, or reliability. By adopting a unified XIoT security strategy that addresses visibility, threat prevention, and identity protection under one framework, businesses can protect their most critical assets, maintain continuous uptime, and stay ahead of evolving adversarial tactics.

Solution: A modern, platform approach to XIoT security

Securing XIoT environments demands more than patchwork solutions — it requires a unified, platform-driven approach that addresses every phase of the defense lifecycle. From automatically discovering and contextualizing every asset to detecting threats, validating segmentation policies, and stopping identity-based attacks, CrowdStrike Falcon® for XIoT brings together everything security teams need. By unifying asset visibility, threat protection, identity security, and expert-led threat hunting into one integrated platform, organizations can strengthen their defenses without sacrificing uptime, performance, or operational safety. Falcon for XIoT delivers the core capabilities needed to reduce blind spots, respond faster, and maintain consistent protection across IT and XIoT landscapes.

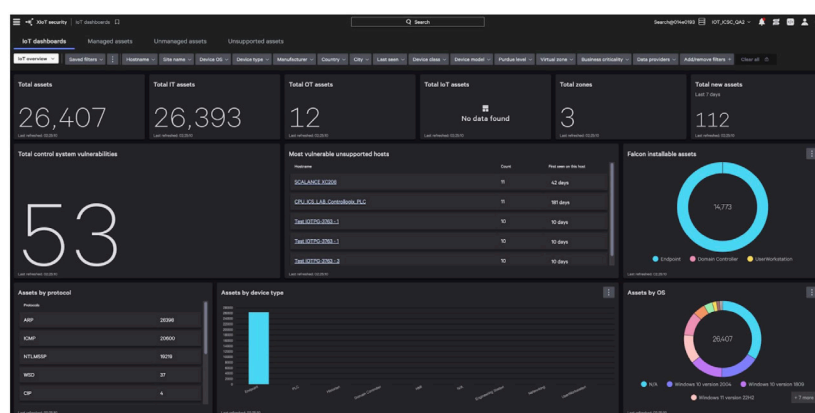
Key benefits

- **Complete visibility:** Gain a real-time, unified view of all XIoT assets — including segmentation insight and asset behavior — without disrupting performance or uptime.
- **Comprehensive threat protection:** Prevent ransomware and advanced threats with a single lightweight sensor validated for 12+ ICS vendors.
- **Actionable insights and managed detection and response (MDR):** Tailor user views, monitor device behavior, and respond faster with expert threat hunting and fully managed detection and response.

Key capabilities

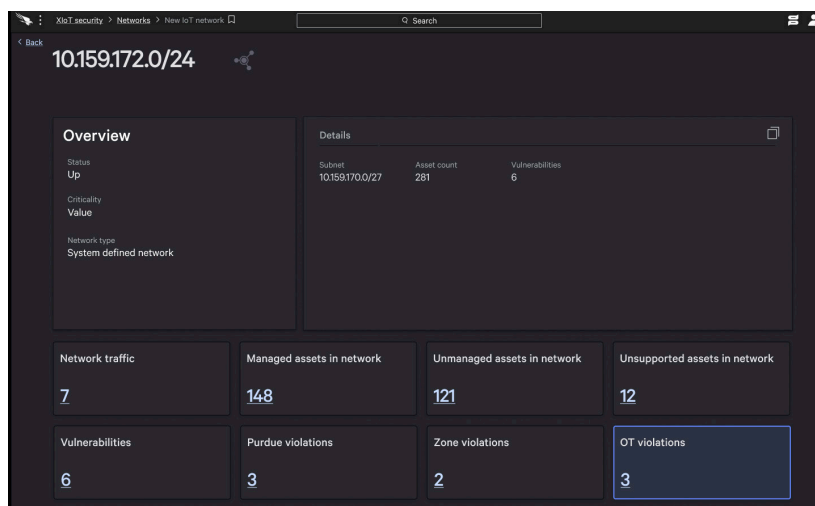
Complete XIoT Asset Visibility

You can't secure what you can't see. Falcon for XIoT delivers comprehensive, real-time visibility across your network — from industrial controllers and IoT systems to standard IT endpoints — without scanning overhead or operational risk. Asset discovery is configuration-free and continuously updated, using passive telemetry and safe identification methods to detect devices across VLANs, subnets, and gateways. Enriched with details like hardware type, Purdue level, and firmware status, each asset is mapped into the CrowdStrike Falcon® platform for full visibility. With integrated, XIoT-specific vulnerability insights from ExPRT.AI, CrowdStrike's predictive risk prioritization AI engine, organizations can take control of their most pressing risks and exposures. Unlike traditional discovery tools that rely on active scans, CrowdStrike's zero-touch approach is non-disruptive, ensuring minimal impact on performance. With unified visibility across both IT and OT environments, security teams can quickly identify and prioritize risks without disrupting uptime.



Asset Context and Operational Insight

Visibility means more than just a list of devices. Falcon for XIoT delivers deep asset context — mapping communication behavior, Purdue level, and device roles — so security teams can understand how assets interact across networks and validate segmentation policies. This enriched telemetry is visualized in the Falcon platform, where teams can explore their environments, track changes, and respond in real time. With this level of insight, teams can reduce lateral movement risk, detect policy violations, and make faster, more informed decisions — without switching tools or adding infrastructure.

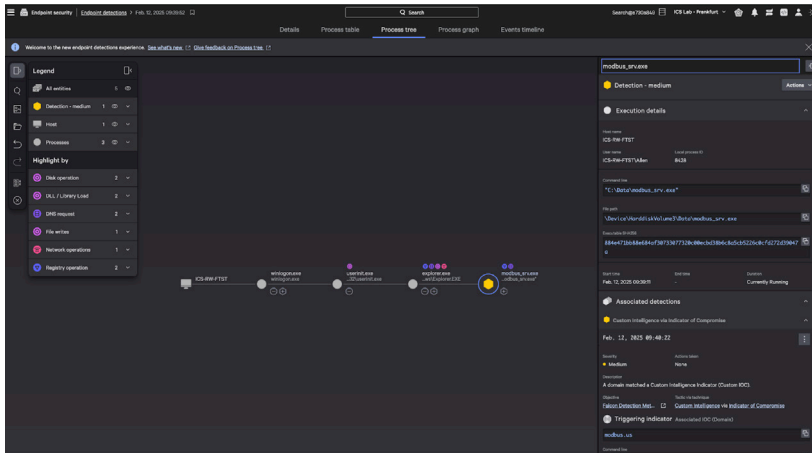


CrowdStrike Products

Falcon for XIoT

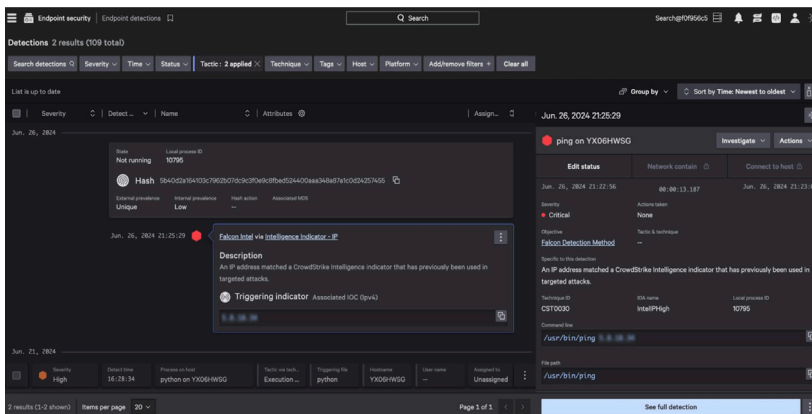
Comprehensive XIoT Threat Protection

CrowdStrike's single lightweight Falcon sensor leverages threat intelligence and AI-driven analytics to detect, prevent, and respond to ransomware, malware, and zero-day attacks specifically targeting XIoT devices. Validated for top ICS vendors, Falcon for XIoT delivers robust endpoint detection and response (EDR) into OT and industrial environments, mitigating risks such as production downtime, operational failure, data loss, and physical disruption. Combined with real-time telemetry and actionable alerts, security teams can stay ahead of adversaries targeting weak points in mission-critical infrastructure.



Protection Against Identity-Based Attacks

XIoT environments often rely on shared or weak credentials, exposing them to identity-based attacks and lateral movement. Beyond proactive and active defenses delivered by Falcon for XIoT, CrowdStrike Falcon® Next-Gen Identity Security enforces strong, risk-based authentication for these assets, blocking unauthorized access and reducing the risk of privilege escalation. By continuously analyzing user behavior, device posture, and contextual signals, security teams can prevent credential misuse, even if login credentials are compromised. Integrated with Falcon for XIoT, this approach helps protect physical processes, maintain compliance, and reduce identity-related attack paths.



Expert MDR and Threat Hunting

Even well-resourced security teams can struggle to monitor and respond to threats around the clock, especially in complex OT and XIoT environments. CrowdStrike Falcon® Complete Next-Gen MDR and CrowdStrike Falcon® Adversary OverWatch™ provide 24/7 protection with expert-led detection, response, and threat hunting. With full access to enriched telemetry and asset context, MDR experts investigate, contain, and remediate threats faster, ensuring minimal disruption to critical systems while extending your team's reach and resilience.

[Get a 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.

Free Trial

