JOINT SOLUTION BRIEF

Forescout eyeExtend for Crowdstrike Falcon Next-Gen SIEM



FORESCOUT + CROWDSTRIKE

FORESCOUT + CROWDSTRIKE

Extending Falcon Next-Gen SIEM with Comprehensive Cyber-Physical Asset Intelligence

Joint Solution Overview

As organizations modernize security operations centers (SOCs), they are increasingly consolidating event monitoring, analytics, and incident response into next-generation SIEM platforms. While these platforms deliver powerful detection and correlation capabilities, cyber-physical environments often contain unmanaged and agentless devices that create visibility gaps for security teams.

The Forescout and CrowdStrike integration bridges this gap by streaming Forescout asset intelligence, device classification, and policy events directly into CrowdStrike Falcon Next-Gen SIEM. This enables security analysts to correlate endpoint, identity, cloud, and network telemetry with rich device context from managed and unmanaged assets across IT, OT, IoT, and IoMT environments.

The Challenge

Security analysts are frequently tasked with investigating alerts that lack sufficient context about the affected device.

Common challenges include:

- Limited visibility into unmanaged or agentless devices
- Difficulty prioritizing incidents without device identity and posture information
- Separate workflows for endpoint telemetry and network asset intelligence
- Blind spots across operational technology (OT), IoT, and IoMT environments
- Increased investigation time due to multiple security consoles

As organizations adopt Zero Trust and Exposure Management initiatives, these visibility gaps create operational risk and slow threat response.

The Joint Solution

The Forescout eyeExtend plugin for CrowdStrike Falcon Next-Gen SIEM forwards Forescout security, device, classification, and policy events directly into Falcon LogScale for centralized analysis and correlation. Security teams gain a unified view of cyber assets and security telemetry within the CrowdStrike Falcon platform.

Key Capabilities

- Stream device, classification, and policy events from Forescout into Falcon Next-Gen SIEM
- Correlate Forescout asset intelligence with Falcon security telemetry
- Search, visualize, and alert on Forescout-generated events within Falcon
- Enrich investigations with device identity, posture, and compliance status

© 2026 Forescout. All rights reserved.

- Extend Falcon visibility to unmanaged and agentless assets
- Support large-scale event ingestion through automated forwarding mechanisms

Key Use Cases

Unified SOC Visibility

Security analysts can investigate managed and unmanaged devices from a single console rather than pivoting between multiple tools and data sources. Forescout provides visibility into devices that may not have endpoint agents installed, including OT, IoT, and IoMT devices, while Falcon delivers centralized security analytics.

Enriched Detection and Incident Triage

Analysts can correlate Falcon detections with Forescout device identity, classification, compliance state, and network context to determine which incidents represent the highest operational risk.

Zero Trust Validation

Organizations can leverage historical and real-time Forescout events within Falcon to validate segmentation policies, identify unauthorized devices, and support Zero Trust initiatives across cyber-physical environments.

Threat Hunting Across Cyber-Physical Assets

Security teams can proactively search for risky, rogue, or non-compliant devices alongside endpoint detections to uncover attack paths and hidden exposure.

Customer Benefits

Organizations deploying the joint solution can achieve:

Increased Visibility

Discover and monitor managed and unmanaged assets across IT, OT, IoT, and IoMT environments within Falcon Next-Gen SIEM.

Faster Investigations

Provide analysts with device context directly inside existing investigation workflows, reducing manual lookups and tool switching.

Better Incident Prioritization

Understand device identity, compliance status, and risk profile when evaluating alerts and security incidents.

Enhanced Zero Trust Initiatives

Support exposure management and Zero Trust strategies through continuous visibility into cyber-physical assets.

Greater Security Operations Efficiency

Maximize the value of both Falcon Next-Gen SIEM and Forescout by consolidating visibility and accelerating incident response.

© 2026 Forescout. All rights reserved.

Joint Value Proposition

CrowdStrike provides world-class security analytics, detection, and response.

Forescout provides comprehensive visibility and contextual intelligence for managed and unmanaged cyber-physical assets.

Together, the two platforms help organizations eliminate visibility gaps, accelerate investigations, strengthen Zero Trust initiatives, and improve security outcomes across modern enterprise environments.

FORESCOUT

Experience the Forescout Vistaro™ platform today.

GET STARTED »

About Forescout

As AI-driven vulnerability discovery and exploitation accelerate attack velocity to machine speed, Forescout is a foundational cyber defense layer that allows organizations to segment and isolate compromised systems, block lateral movement, and automate response across IT, OT, IoT, and IoMT environments. The Forescout Vistaro™ platform, powered by agentic AI and enhanced with Vedere Labs threat intelligence, delivers a Universal Zero Trust Network Access (UZTNA) architecture that integrates seamlessly with 180+ security and IT products. With Forescout Vistaro, organizations get comprehensive inventory and classification of both managed and unmanaged assets, continuous exposure management, and real-time protection including dynamic network segmentation and automated threat response.

FORESCOUT

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com

©2026 Forescout Technologies, Inc. All rights reserved.
Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal. Other brands, products, or service names may be trademarks or service marks of their respective owners.
09_26_V01