SOLUTION BRIEF

End-to-end visibility and faster response across managed endpoints and every network path

Executive Summary

Security teams lose time and context when endpoint intelligence and network data live in separate tools. The Cato Networks + CrowdStrike integration closes that gap. By pairing the CrowdStrike Falcon® platform with Cato SASE Platform, security teams can unify endpoint and network context in one workflow. Together, they deliver richer context, faster investigations, and flexible analyst workflows.

Common Use Cases

Remote Workforce Containment

The Falcon platform flags a phished remote managed endpoint; Cato XOps correlates egress and related flows into a guided story. The operator blocks destinations and tightens access in Cato, and Falcon Next-Gen SIEM confirms no spread.

Endpoint-Network Correlation

The Falcon platform flags a suspicious process; Cato correlates rare DNS beacons and lateral SMB into one guided XOps story so the analyst confirms with network evidence and contains in Cato.

Trusted Device Context

The Falcon platform shows an outdated OS on a managed laptop; the Falcon-enriched Cato device inventory reflects the device details. The admin publishes an attribute-based policy in Cato to restrict the device until remediation.

Network-Aware Hunting In Falcon

In Falcon Next-Gen SIEM, the analyst investigates DNS spikes using correlated Cato network evidence, identifies an exfiltration pattern, and updates Cato policy to block the domains and restrict the behavior.

Challenges

Many solutions share the same core issues: Endpoint-only views miss lateral movement. Point products rarely align network activity with user, device, and host details in one view. Device lists are incomplete or out of date and posture is not consistently used to set network access. Analysts pivot between consoles, delaying containment and raising costs. A fragmented stack and tool sprawl create noise and hide context. The result: frequent alerts, WAN and East-West blind spots, and slow decisions.

Investigations suffer from partial visibility. Analysts need a single place to see the full story. Endpoint-only telemetry can miss lateral movement and traffic between systems.

Policy suffers from a posture-to-policy gap; managed endpoint posture and attributes are not consistently used to set network access. Teams default to IP-based rules and overprivileged access. Segmentation becomes hard to maintain as conditions change.

Hunting often becomes host-only. Many teams hunt in SIEM tools but lack full network evidence, which forces tool switching, slows queries, and leaves uncertainty about spread and scope.

Cato Networks + CrowdStrike Joint Solution

Cato SASE Cloud delivers converged, cloud-native SASE with single-pass inspection and a single policy across Internet and WAN. When integrating with Cato, the CrowdStrike Falcon platform provides endpoint detections and analytics. Together, the integration spans three complementary motions that work in concert:

- **Correlated Detection and Investigation in Cato**
  (Cato XOps and CrowdStrike Falcon Exposure Management licenses):

  Falcon endpoint detections are ingested into Cato and correlated with Cato networking, DNS, security, remote user and device context, and flow telemetry. Cato XOps assembles guided incident stories that map the affected user or device, impacted sessions, destinations, and any lateral movement over time, so analysts confirm impact quickly and take decisive action across the Cato SASE Cloud. This improves detection fidelity and accelerates investigations without switching between multiple consoles.

- **Device Inventory Enrichment for Policy Readiness**
  (Cato IoT/OT Security and CrowdStrike Falcon Exposure Management licenses):

  Cato builds a device inventory from observed traffic and enriches profiles for managed endpoints with device details from the Falcon platform. Operators then author attribute-based policies in Cato using device characteristics instead of IPs, hostnames, or vLANs. Access follows device identity and posture. Segmentation stays clean and aligned to Zero Trust.

- **Network-Aware Hunting in Falcon**
  (CrowdStrike Falcon® Next-Gen SIEM license):

  Cato streams normalized networking, DNS, security, remote user, and device events into Falcon Next-Gen SIEM. Analysts hunt for threats and build detections in the Falcon platform with fullnetwork evidence, then use findings to drive operator-authored policy updates in Cato.

Better Together Benefits

Unified visibility reduces risk. Falcon detections and device insights for managed endpoints correlate with Cato network evidence. Teams see which endpoints were affected, which connections and data flows occurred, and where to act. This data enrichment improves detection fidelity and cuts false positives.

Investigations move faster and scale smoothly. Cato XOps presents guided stories with endpoint and network context in one view. This allows analysts to confirm scope and apply controls in Cato. One global policy propagates across WAN and Internet without device-by-device updates. Hunts in the Falcon platform use the same shared network evidence.

Coverage spans the full attack path. Cato inspects Internet and WAN traffic across all ports and protocols, combining that network evidence with Falcon Insight XDR endpoint detections and device insights. Together, analysts expose lateral movement sooner, limit spread, and minimize disruption.

Segmentation becomes device-aware. Falcon-enriched profiles for managed endpoints raise confidence in identity and attributes. Attribute-based rules in Cato enforce least privilege access and adapt as conditions change, reducing maintenance.

Conclusion

Cato SASE Cloud and the CrowdStrike Falcon platform turn siloed signals from managed endpoints and networks into shared evidence and guided investigations. Cato's single-pass inspection and unified policies provide consistent visibility and control. Teams decide faster and act confidently through data enrichment and flexible workflows. When action is required, operators apply consistent, attribute-based controls in Cato without additional tools.

The result is faster investigation, tighter containment, and device-aware policies that align with Zero Trust. To see the integration in action, schedule a demo, review the Cato Knowledge Base for XOps and Device Management configurations, or visit the CrowdStrike Marketplace listing.

About Cato Networks

Cato Networks, a leader in SASE and AI security, delivers secure, zero-trust access everywhere to thousands of customers worldwide. Built for organizations operating across all cloud and hybrid environments, the Cato Platform unifies networking, security, and access, providing them as elastic, modular capabilities that organizations can easily adopt and grow over time. Cato combines the Cato Cloud, a purpose-built global network, with simplified operational experience, all delivered across a robust, AI-driven platform. With Cato, organizations modernize confidently, operate with greater resilience, and innovate faster, without added complexity or risk.