

Powering the Modern SOC: CrowdStrike Falcon Next-Gen SIEM with Endace Always-on Packet Capture



The Problem

Modern enterprises use complex hybrid environments with cloud, virtual, and on-premises infrastructure that delivers SaaS, email, OT, identity, and other business functions. Modern cyber-attacks are driven by highly evasive live-off-the-land and AI-augmented attacks that move at machine speed..

Traditional SIEM and security tools typically rely on slow, index-based logging and use pre-defined static assumptions, which are no longer sufficient to secure highly distributed environments spanning cloud, virtual, and on-prem infrastructure. This creates critical challenges for security teams, including:

- **Novel threats** – Unknown and subtle attacks such as sophisticated ransomware, insider threats, and compromised credentials are missed by legacy tools that cannot correlate vast datasets in real time.
- **Alert fatigue** – Security operations centers are overwhelmed by thousands of siloed, low-fidelity alerts, resulting in slow and incomplete triage and investigation due to ingestion bottlenecks.
- **Forensic blind spots** – When incidents occur, the lack of complete, historical network data makes root-cause analysis slow, laborious, and inconclusive.
- **Security teams cannot fully understand the attack scope** or ensure complete remediation without definitive network recording.

Organizations need a solution that:

- **Delivers advanced Next-Gen SIEM capabilities** powered by petabyte-scale logging and AI-driven analytics.
- **Provides continuous full packet (not triggered) capture** for reliable incident recording.
- **Supports deployment** across on-prem, private, and public cloud infrastructure.
- **Delivers the required functionality** while being easy to use and fast to implement.

Benefits

- **Complete threat interruption.** The CrowdStrike Falcon® platform neutralizes attacks in real time using automated workflows, while Endace ensures the underlying network evidence is captured.
- **Accelerated investigations.** Investigation time is reduced from days to minutes with CrowdStrike Charlotte Agentic SOAR to automate initial triage and Endace Pivot-to-Vision capability to give packet-level evidence required for root cause analysis.
- **Operational efficiency.** Consolidate and maximize security investments by hosting CrowdStrike Falcon Log Collectors on EndaceProbes in Application Dock™, eliminating the need to acquire and deploy additional hardware for log forwarding.
- **Definitive evidence.** With Endace's always-on network recording, teams gain the packet-level evidence needed to conclusively prove whether a breach occurred, understand the scope, and meet legal regulatory requirements.
- **Cost Effective and Highly Scalable.** Scale to petabytes of fast search sufficient to retain months of history with fast search for instant access to packet evidence.
- **Support mandatory and best practice requirements** including HIPAA, M-22-09, NERC CIP, PCI-DSS, SAMA, and more.
- **Zero-day threat risk validation.** Vulnerability management and incident response teams can use recorded network playback and threat analysis to prove risk mitigation.
- **FIPS and Common Criteria/NIAP Certified** for deployment in high security environments.

SOLUTION BRIEF: CROWDSTRIKE

Powering the Modern SOC: CrowdStrike Falcon Next-Gen SIEM with Endace Always-on Packet Capture

The Solution

By integrating **CrowdStrike Falcon® Next-Gen SIEM** with Endace Always-on packet capture, organizations gain the confidence to detect and respond accurately to threats across their on-prem and cloud environments.

CrowdStrike Falcon Next-Gen SIEM uses a cloud-native, index-free architecture to unify data, security, and IT operations, providing comprehensive visibility across the organization's infrastructure.

CrowdStrike real-time, cross-domain detection detects subtle indicators that signal threats, including novel and zero-day threats and stealthy internal activity across the entire attack surface: Network, Email, Cloud, OT, Identity, and Endpoint.

Telemetry from the entire CrowdStrike Falcon® platform is visible in Falcon Next-Gen SIEM, leveraging AI-native detection to continuously analyze every connection, device, identity, and attack path to cut through the noise and improve detection accuracy.

The **EndaceProbe™ Platform** continuously records days, weeks or months of full packet capture data, forming a unified, hybrid cloud recording fabric. This delivers the

comprehensive network history required for in-depth drill down to the ultimate network forensic evidence.

Pivot-to-Vision™ integration links alerts from the CrowdStrike Falcon platform directly to the relevant packet data in EndaceVision™.

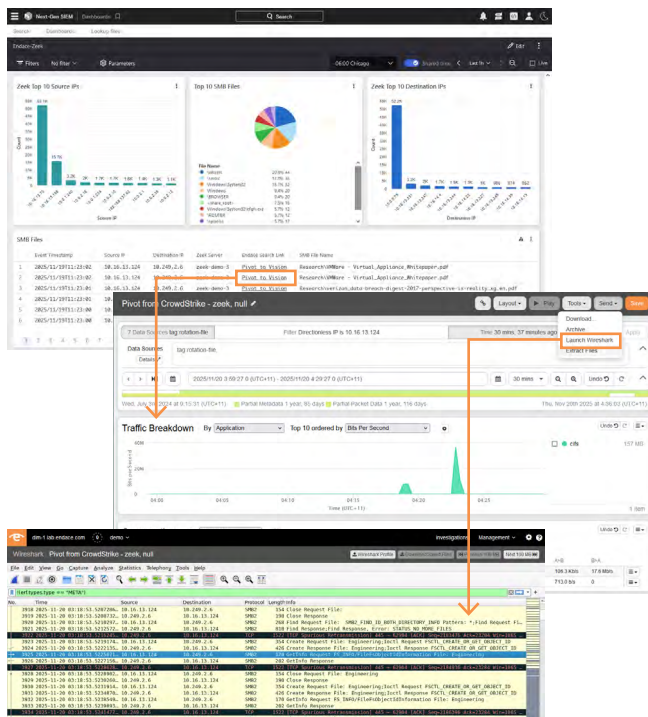
This enables streamlined workflows resulting in faster, more efficient investigation and resolution of network security issues by putting definitive evidence at the analysts' fingertips.

Conclusion

Combining CrowdStrike and Endace provides two essential components of a modern security strategy, including predictive, autonomous defense and ultimate network forensic evidence.

CrowdStrike Falcon Next-Gen SIEM ensures an organization is defended autonomously across its entire hybrid environment, while Endace provides the definitive always-on network history needed for fast, accurate, and conclusive incident response and threat hunting. Together, they enable security teams to stay ahead of adversaries by transitioning from reactive incident response to proactive cyber resilience.

How it works



1. CrowdStrike detects a threat through Falcon platform telemetry and Falcon Next-Gen SIEM analytics.
2. Analysts can select that event in the Falcon Next-Gen SIEM console.
3. The Pivot-to-Vision link allows direct drilldown to the EndaceProbe Always-on Packet Capture to display Network History related to the detection.
4. Using the Endace Vision GUI, analysts can zoom in to look at specific packets or zoom out to look for precursor or post-event activity.
5. Analysts can also launch embedded WireShark® hosted on the EndaceProbes, avoiding the need to download large PCAP files.
6. File extraction can export associated file data for attachment to CrowdStrike case investigations.
7. REST API endpoints enable automation of SOC investigation workflows.

Solution Components

- » CrowdStrike Falcon Next-Gen SIEM
- » EndaceProbe and EndaceProbe Cloud appliances
- » EndaceProbe Application Dock for on-prem deployment of Falcon Log connectors.

© 2026 Endace Technology Limited. All rights reserved. Information in this data sheet may be subject to change.

Endace™, the Endace logo, Provenance™ and DAG™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).