SOLUTION BRIEF

Advanced Zero Trust Security & Next-Gen SIEM Intelligence

Real-Time Threat Correlation Meets Secure NaaS

The Context and Data Quality Challenge

Traditionally, network infrastructure and related solutions stream unstructured event data to Security Information and Event Management (SIEM) systems without local context or filtering. This overwhelms today's cloud-based SIEM solutions, floods security analysts with false positives, and triggers adding a dedicated pre-ingestion layer that adds unnecessary overhead.

An Intelligent Alternative

The integration between CrowdStrike Falcon® Next-Gen SIEM and Nile's Network-as-a-Service (NaaS) bridges the gap, eliminating traditional telemetry bottlenecks through a unified, contextual data flow. Nile automatically correlates network events, policy alerts, and audit logs at a **service-level**, directly delivering clean data.

This empowers network and security IT teams to detect and contain issues and potential threats faster without digging through extensive noise generated by today's traditional network architectures.

Key Capabilities & Benefits

1

Unified Context and Visibility

Endpoint telemetry merged with network context in a single view - no blind spots across managed and unmanaged devices.

2

Accelerated Threat Response

Simplified investigative workflows link active endpoint data with real-time network access containment controls.

3

Optimized Ingestion and Costs

No redundant, raw syslog overhead - Nile sends pre-correlated, contextual network data directly to Falcon Next-Gen SIEM.

Copyright © 2026 Nile. All Rights Reserved

Unified Context & Visibility across Managed and Unmanaged Assets

Using CrowdStrike with Nile's native network access visibility, ensures IT can more easily see network events, security alerts, and audit logs in greater detail within the Falcon Next-Gen SIEM. This gives IT teams network, endpoint telemetry, and context without additional sensors or manual log collection, reducing investigation times from hours to minutes.

Enhanced Detection and Investigation Data

Nile natively streams pre-filtered, structured network telemetry, including physical layer location, micro-segmentation status, continuous device fingerprinting, and user identity directly into CrowdStrike Falcon Next-Gen SIEM. Correlating network data with SIEM event logs gives security analysts instant, cross-domain visibility to scope threats faster, dramatically reducing business impact across managed and unmanaged assets.

Optimized SIEM Economics and IT Resources

Legacy networks flood SIEMs with raw, redundant syslog data, driving up licensing expenses. Nile eliminates this bloat by pre-filtering and sending only correlated, high-value network context directly to CrowdStrike Falcon Next-Gen SIEM. This simple step dramatically reduces ingestion costs and prevents wasted hours stitching together raw syslog data.

Smarter Signals, Complete Context

01

Every device, fully identified:

Nile sends events with user info, MAC, IP, SSID or switch port, and timestamp for all onboarded devices, even those that can't run agents. Analysts see when devices join, owner, and where connected - wired or Wi-Fi.

02

No spoofing

Nile detects/blocks unapproved static IPs, IP and MAC spoofing right where the device connects. Built-in IDS flags rogue and evil-twin APs that copy SSIDs. CrowdStrike receives one unified alert, not raw ARP and DHCP logs to piece together.

03

Every access decision recorded

Trust Service sends policy logs to CrowdStrike SIEM, ensuring allow and deny decisions for all requests. Data includes source and destination, user and device group, IPs, MACs, port, matched rule and action.



1 Every device, fully identified

User, MAC, IP, port or SSID, and onboard time

2 Threats stopped at the access edge

Spoofing blocked at the port, rogue APs flagged

3 Every access decision on record

Trust Service policy logs: who, what, which rule

Wired *Wireless* *Threat* *Blocked by Nile*

IT Needs a Next-Gen SIEM and Network Architecture

Can you really afford not to eliminate coverage blind spots, reduce ingestion costs, and enable instant, cross-domain troubleshooting? CrowdStrike Falcon® Next-Gen SIEM with Nile's secure NaaS, allows organizations to easily replace raw noise with pre-filtered, contextual telemetry across managed, unmanaged, and IoT devices.

About Nile

Nile is a pioneer and leader in secure networking-as-a-service (NaaS). With AI-powered service delivery and autonomous operations, Nile solutions cut through complexity and cost versus legacy networking solutions, while delivering radical operational simplicity and user experiences.

About CrowdStrike

CrowdStrike Holdings, Inc. (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.

Ready to Get Started?

Request a Demo

Copyright © 2026 Nile. All Rights Reserved