corelight

The role of network evidence in detecting EDR-evasive threats

EDR evasion is real

EDR Evasion encompasses a range of techniques that threat actors commonly use to evade organizational endpoint defenses. Over-reliance on Endpoint Detection and Response (EDR) systems leaves critical gaps in threat detection.

Edge vulnerability

Breaches at firewalls/VPN gateways surged from

3% ⟶ 22%

exposing weaknesses in perimeter defenses

(Source: Verizon DBIR)

Malware-free intrusions

79%

of attacks are malware-free, **evading EDR** through techniques like credential theft and DLL hijacking

(Source: CrowdStrike GTR)

Rapid attack speed

Fastest breakouts occur in seconds, demanding **real-time detection** beyond EDR capabilities

(Source: CrowdStrike GTR)

Firewall Logs and Netflow are incomplete

Firewall logging involves recording all activities that pass through the firewall into a log file, and Netflow is a protocol from Cisco Systems to capture metadata from routers and switches. Typically, these sources provide only partial data and have limited security value.

Firewall logs are generally very noisy. Firewall logs have a very high volume of records that are unstructured, making it difficult to spot suspicious activity, typically miss both east-west traffic and application/user context.

Netflow and firewall logs are typically incomplete. They are typically made of sampled or limited data due to capacity constraints and configuration needs. Also, attackers are increasingly targeting firewall (and other edge device) vulnerabilities, possibly leaving firewall logs incomplete.

Performance overhead on devices. While it's possible for these devices to be configured to capture all traffic data, doing so can impose significant computational demands on routers, switches, and firewalls, often leading to configurations that sample traffic or limit the scope of the logs and data.

Network evidence provides ground truth

Full packet data provides detailed insights for accurately reconstructing events and diagnosing security or performance issues, but its large volume makes long-term storage impractical.

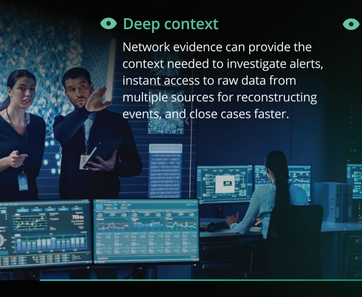
Network evidence involves **enriching data with security context and selectively capturing relevant packets** to extend forensic windows, enabling cost-effective long-term retention and preserving critical evidence.

Complete visibility

Evidence-driven analytics exposes subtle indicators of compromise, including encrypted command-and-control channels and data exfiltration attempts.

Deep context

Network evidence can provide the context needed to investigate alerts, instant access to raw data from multiple sources for reconstructing events, and close cases faster.



High-fidelity

SOCs face excessive alerts, false positives, and incomplete data, but high-fidelity, correlated telemetry powers analytics, machine learning tools, and SOAR playbooks, improving efficiency and unlocking new capabilities for SecOps teams.

Evidence drives accurate threat detection (including EDR-evasive threats)

Corelight enriches detections with deep context and AI-driven automations, providing evidence-backed summaries, guided triage, and analyst-ready workflows to accelerate investigations.

Reduce ingest

Corelight's evidence preserves the fidelity of the data while reducing the SIEM ingest by **over 70%.**

ML-accuracy

Corelight's evidence improves machine learning-based threat detection accuracy to **minimize false positives.**

Expert Hunting

Corelight's evidence enables you to spot vulnerabilities, intruder artifacts, critical misconfigurations, signs of compromise, and undetected attacks, **further mitigating risk.**