Joint solution brief

Corelight and Palo Alto Firewall Integration for Rapid Response

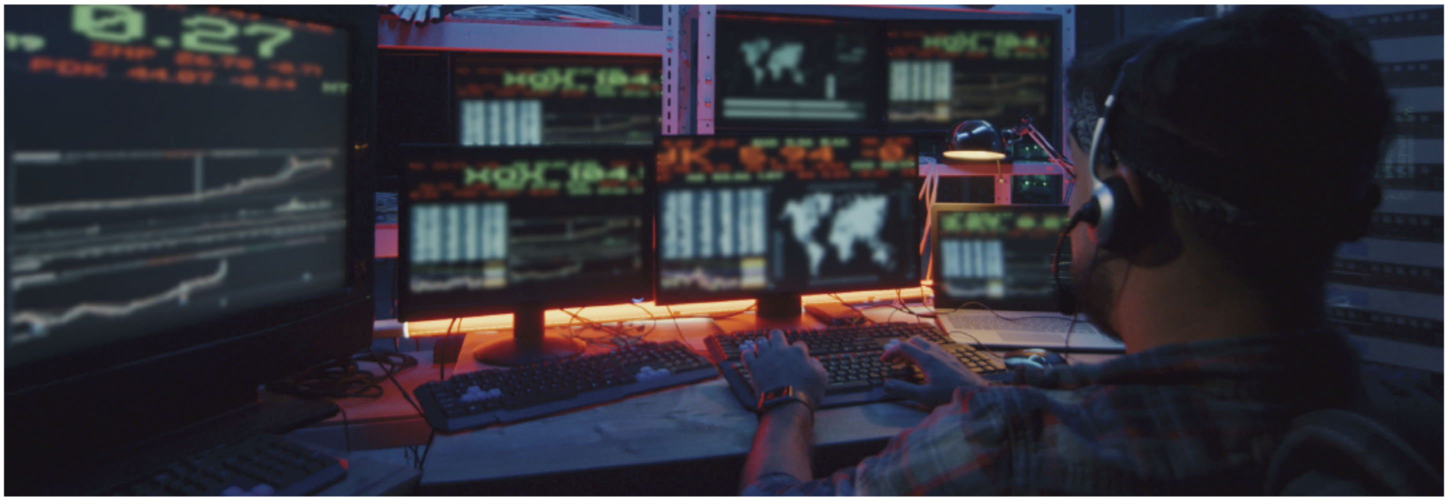
Accelerate Incident Response and Block Threats in Corelight Investigator

Security teams know that when an attack is in progress, rapid containment is critical. Yet in high-pressure situations, responders are often forced to jump between disconnected security tools—identifying a threat in one platform, then manually locating the same device or user in another just to take action. In some cases, they must even submit a ticket to the network team to block a malicious IP at the firewall. These fragmented workflows slow response times and increase risk. Many security solutions lack the integrated threat detection and response needed to act swiftly from a single interface. In fast-moving attacks, every second counts—the difference between stopping ransomware in its tracks or losing sensitive data to exfiltration.

SOLUTION HIGHLIGHTS

- Extensive visibility into network traffic and firewall blocking of malicious traffic
- Faster threat containment with 1-click firewall blocking directly within Corelight Investigator
- Higher analyst productivity through integrated UI workflows

Integrated Corelight and Palo Alto Networks for accelerated response capabilites



Accelerate your incident response capabilities by integrating Corelight with Palo Alto Networks Firewall.

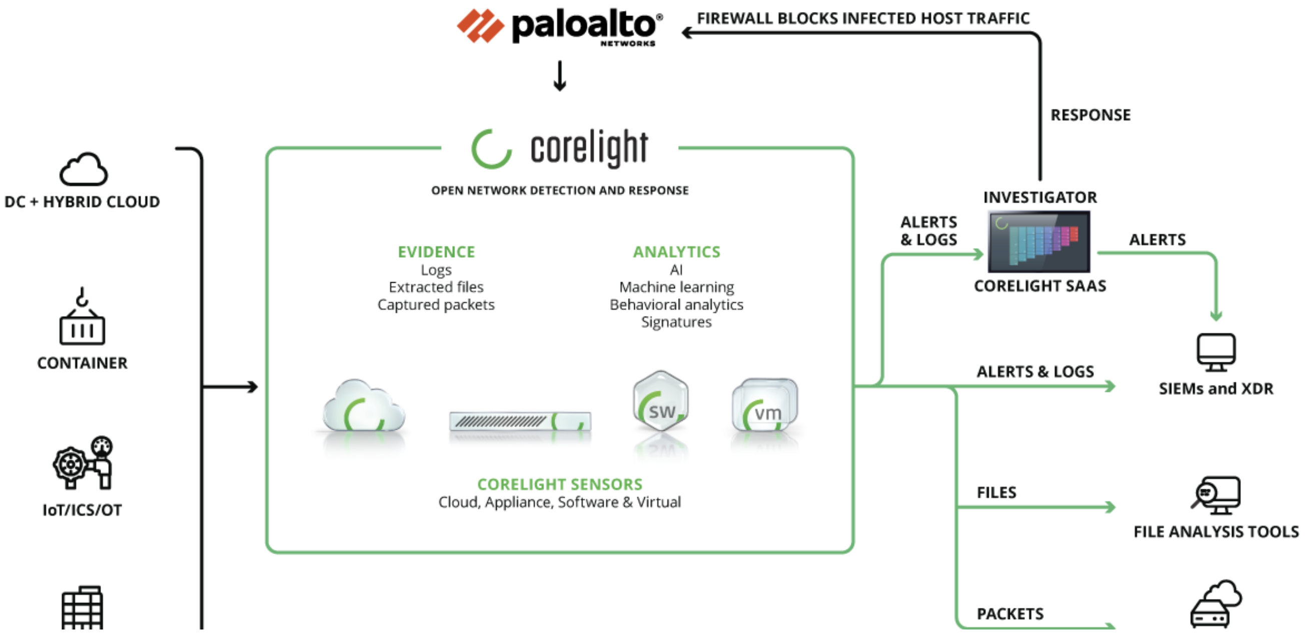
BLOCK MALICIOUS IPS IN REAL-TIME

Corelight's integration with Palo Alto Networks Firewalls empowers analysts to block malicious IPs directly from a detection within Corelight Investigator. With a single click of the "Block" action button, Corelight updates the organization's Palo Alto External Dynamic List (EDL). The firewall then pulls this updated list into its Access Control List (ACL), enabling near real-time enforcement. This indirect push-pull architecture ensures secure, scalable blocking—without requiring direct API access to the firewall. The result: Security analysts can quickly and confidently disrupt attacker communications, all from within a unified interface.

STREAMLINED INCIDENT RESPONSE

Corelight's native integration with Palo Alto Networks Firewalls empowers SOC teams to accelerate incident response by pivoting from threat detection to enabling blocking capabilities—all within Corelight Investigator. This tight integration allows security analysts to take immediate remediation actions, reducing the time between detection and response and ensuring a more coordinated approach to high-risk security incidents.

Native Integration for faster threat containment



Simplify investigations and prioritize alerts based on actual risk to the enterprise by integrating network, firewall, and endpoint data.

SOLUTION BENEFITS

GET COMPLETE VISIBILITY

Detect early, mid, and late-stage indicators of network compromise with comprehensive visibility into all network traffic across the enterprise. This includes support for unmanaged and unknown devices, as well as those that cannot accommodate endpoint agents.

ACCELERATE INCIDENT RESPONSE

Corelight enhances incident response by leveraging Palo Alto Firewall capabilities to block malicious IPs in real time. Analysts can quickly pivot from threat detection to remediation within Corelight Investigator, using 1-click actions to enforce firewall policies and contain compromised devices. This streamlined approach minimizes response time and reduces the risk of lateral movement.

QUICK THREAT ANALYSIS AND BLOCKING

Corelight's integration with Palo Alto Firewalls enables rapid remediation through firewall enforcement based on verified threat data. Security analysts can quickly analyze threats within Investigator and block traffic to malicious IP addresses, ensuring a swift response to critical threats.

INCREASE OPERATIONAL EFFICIENCY

Corelight consolidates multiple security functions—including network monitoring, IDS, and intelligent packet capture—into a unified NDR platform. By leveraging Palo Alto Firewall response capabilities, Corelight reduces SOC complexity across on-premise, hybrid, and multi-cloud environments. Analysts can enforce firewall policies and block malicious IPs directly through Corelight Investigator, streamlining remediation processes and enhancing security outcomes.

corelight

To learn more about Corelight for Palo Alto Networks, request a demo at:

https://corelight.com/contact

info@corelight.com | 888-547-9497