DEEP NETWORK OBSERVABILITY

CORELIGHT and PROFITAP

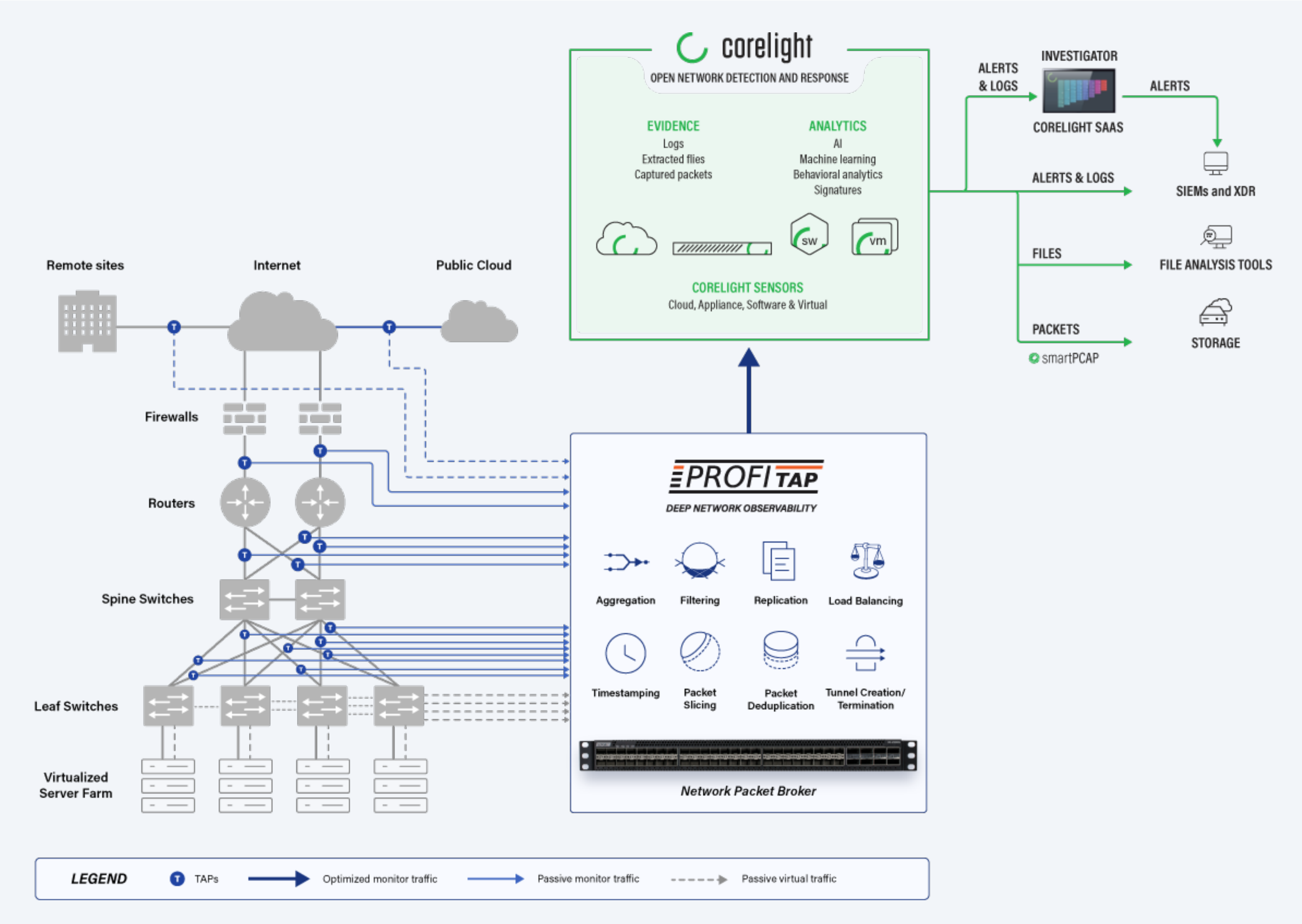
JOINT SOLUTION FOR NETWORK OBSERVABILITY

VISIT WWW.PROFITAP.COM

Corelight and Profitap: A joint solution for network observability

As networks grow in complexity and cyber threats increase in scale and sophistication, security teams need more than fragmented tools. They need full-spectrum visibility and actionable intelligence.

Through their technology alliance, Corelight and Profitap offer a high-performance, scalable monitoring stack for deep, end-to-end threat detection.



Integrated Visibility and Detection

The joint solution of Profitap and Corelight delivers a seamless, high-performance monitoring stack that ensures complete visibility and deep threat detection in complex environments.

Profitap specializes in non-intrusive access to network traffic and efficient data optimization. As a best practice, it ensures reliable, lossless access to network traffic via passive Test Access Points (TAPs).

Network Packet Brokers (NPBs) further enhance the visibility stack by aggregating, filtering, and optimizing traffic streams from multiple monitoring points. These optimized traffic flows are then delivered to Corelight's NDR sensors for deep analysis.

Corelight provides the comprehensive network evidence that traditional network security monitoring tools miss. While signature-based tools fail to detect novel attacks and full packet capture creates overwhelming data volumes, Corelight's Zeek-powered approach is different. It combines rich, structured data derived from all network traffic with multi-layered detections—including behavioral and machine-learning analytics.

This "evidence-first" approach is crucial, enabling customers to move beyond just chasing alerts. With Corelight, security teams can proactively hunt for advanced threats and accelerate incident response from days to minutes by having the definitive data and AI-powered workflows to stop an attack.

PROFITAP

Comprehensive network visibility • Full access to East-West and North-South traffic.	***Real-time traffic processing*** • Immediate delivery to detection tools.	***Non-intrusive operations*** • No network disruption during operation.
Data Diodes • Security-focused design with unidirectional communication, preventing data leakage or unauthorized access.	***Performance integrity*** • Monitor without degrading network performance or weakening security posture.	

corelight

Expanded Detection Coverage • Cover EDR detection gaps for the fastest detection and response to adversaries targeting the network edge.	***High-fidelity threat detection*** • Targeted detections for high-value threat behaviors like lateral movement, C2 communication, ICS protocol anomalies, encrypted traffic misuse, and exfiltration	***Flexibility and scalability*** • Deploy across cloud, on-prem, or hybrid environments with ease.

Proactive Threat Hunting	*Accelerated investigations*	*Open NDR platform*
• Create custom searches to find advanced attacks and identify potential vulnerabilities and misconfigurations before the attacker does.	• Correlated logs, rich network metadata, and multi-layered detections expedite root cause analysis and incident response.	• Seamlessly integrates with any SIEM, XDR, or data lake.

Unified Stack for Critical Environments

Ideal for industries like manufacturing, energy, and critical infrastructure, this joint solution enables:

- End-to-end visibility from packet to protocol to detection.
- Safe, passive monitoring across IT and OT/ICS.
- Scalable, simplified, and open NDR architecture.
- Improved detection coverage and response time.
- Compliance-ready network evidence.

Profitap Network TAPs	Profitap Network Packet Brokers	Corelight platform
• Non-intrusive in-line network access • A permanent network link is guaranteed • Passive, unpowered (Fiber) • Protect network link availability for in-line security tools • Deliver lossless traffic aggregation from multiple in-line links or out-of-band connections (Booster) • Secure traffic access	• High throughput • Traffic optimization (Aggregation, Load Balancing, Filtering, Timestamping, Deduplication, SSL/TLS Decryption, etc) • Flow-aware load balancing • Centralized control	• Real-time threat detection and response • AI-powered workflows, analysis, and data unification • Advanced cyber-physical AI with real-time visibility • Superior evidence and detections with full context to speed investigations • Comprehensive yet lightweight network telemetry and threat intelligence simplifies threat hunting

corelight

Corelight transforms network and cloud activity into evidence so that data-first defenders can stay ahead of ever-changing attacks. Delivered by our Open NDR Platform, Corelight's comprehensive, correlated evidence gives you unparalleled visibility into your network. This evidence allows you to unlock new analytics, investigate faster, hunt like an expert, and even disrupt future attacks.
info@corelight.com | 888-547-9497

PROFITAP

Profitap provides packet-based network intelligence to enhance network monitoring and bolster cybersecurity.

Its unified network observability platform offers reliable data access, traffic optimization, and robust traffic capture and analysis capabilities. These solutions minimize network troubleshooting MTTR, eliminate downtime, support lawful interception, simplify network complexity, and strengthen security for both existing and new networks.

Serving over 1,100 clients across more than 70 countries, Profitap's network monitoring solutions deliver comprehensive visibility and analytics across all traffic, ensuring comprehensive insight into both physical and virtual infrastructures globally.

https://www.profitap.com

Profitap HQ B.V.
High Tech Campus 84
5656 AG Eindhoven
The Netherlands

sales@profitap.com
www.profitap.com

Profitap
@Profitap
Profitap-international