corelight

DATASHEET

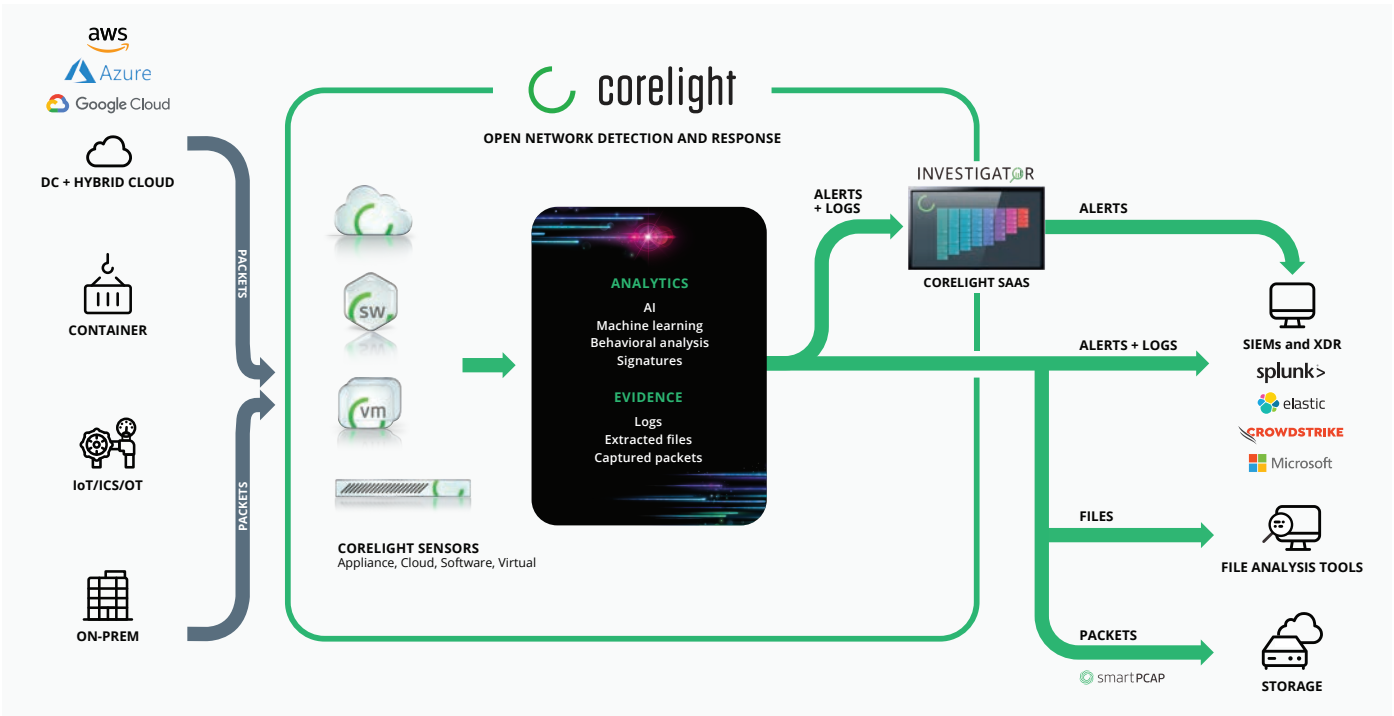
Open Network Detection & Response (NDR) Platform

Corelight's Open NDR Platform combines the power of open source and proprietary technologies and provides complete network visibility across on-prem, cloud, and distributed environments to deliver a complete solution elite defenders use to drive SOC efficiency and disrupt future attacks.

PLATFORM HIGHLIGHTS

- Single solution for NSM, IDS, and PCAP functionality
- Broad range of detection coverage
- AI-powered workflows
- Seamless integration with SIEM and XDR solutions
- Powered by open source Zeek® and Suricata® technologies
- Highly customizable

INTEGRATES SEAMLESSLY WITH YOUR EXISTING ARCHITECTURE



CORELIGHT OPEN NDR PLATFORM

APPLIANCE SENSORS		Nominal capacity*
AP 5000 SERIES	• 2 QSFP28 interface modules • Support for optical modules at 8 x 10G, 2 x 40G, or 2 x 100G	100 Gbps
AP 3000 SERIES	• Up to 8 SFP/SFP+ or 2 QSFP+ interface modules • Support for copper and/or optical modules at 1G, 10G, or 40G	35 Gbps
AP 1000 SERIES	• 4 1G/10G SFP/SFP+ interface modules • Support for copper and/or optical modules at 1G, or 10G	20 Gbps
AP 200 SERIES	• 4 SFP interface modules • Support for copper and/or optical modules at 100M and 1G	2 Gbps

* Capacity for Zeek-based traffic analysis. Enabling additional analysis workloads like Suricata reduces capacity and performance will vary depending on traffic.

VIRTUAL SENSORS	vCPUs	RAM (Gb)	Disk (Gb)	System requirements	Nominal capacity
VMware	4–64	16–256	500–4000	ESXi 6.5 or above	500 Mbps–8 Gbps
Hyper-V	4–64	16–256	500–4000	Windows Server 2016	500 Mbps–8 Gbps

SOFTWARE SENSORS	CPUs	RAM (Gb)	Disk (Gb)	System requirements	Nominal capacity
	2–64	8–256	100–4000	Any 64-bit Linux distribution	250 Mbps–8 Gbps

FLEET MANAGER

- Manage hundreds of sensors
- See overall fleet health in one pane of glass; drill into individual sensor metrics with one click
- Deploy custom sensor policy templates
- Define custom sensor groups, assign individual user roles and access levels
- Demonstrate compliance using audit logs

corelight

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497