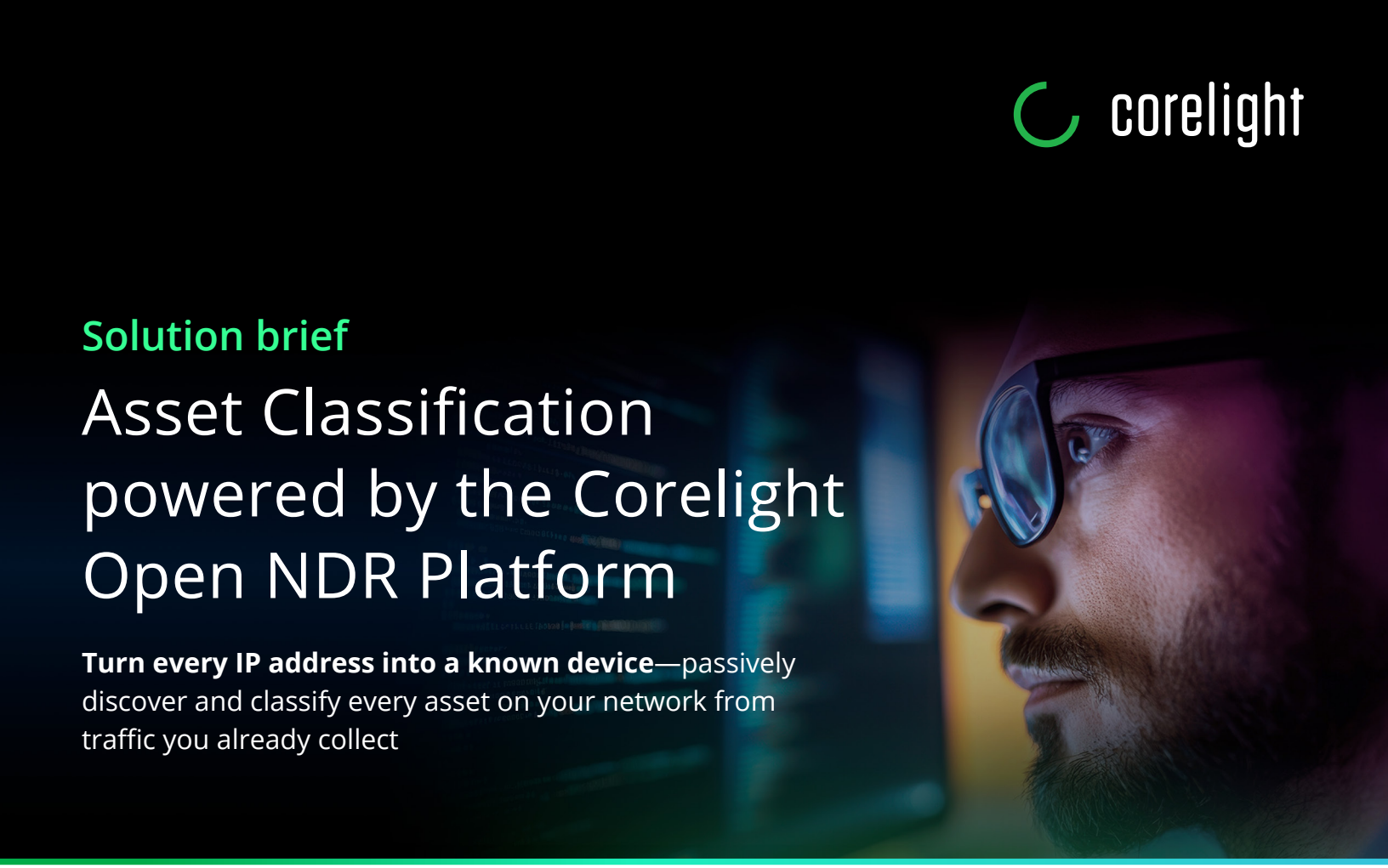
corelight

Solution brief

Asset Classification powered by the Corelight Open NDR Platform



Turn every IP address into a known device—passively discover and classify every asset on your network from traffic you already collect

Security teams investigating alerts shouldn't have to waste time asking "What is this IP?" Corelight Asset Classification uses network evidence to passively fingerprint and classify every device on the network—servers, workstations, IoT, printers, IT, and unmanaged endpoints—the moment they communicate. By deriving asset intelligence directly from observed traffic, Corelight delivers a continuously updated, authoritative inventory that closes the blind spots where agents can't run and CMDBs fall behind.

THE CHALLENGE

Accurate asset visibility is foundational to security operations, yet most organizations struggle to maintain a reliable, real-time inventory. Today's approaches have significant gaps:

- **Stale and incomplete CMDBs**—Configuration management databases rely on manual updates and scheduled scans. Assets are frequently missing, outdated, or miscategorized—leaving security teams with an inventory they can't trust during an investigation.
- **EDR blind spots**—Agent-based tools only cover managed endpoints. Cloud resources, printers, IoT devices, IT systems, medical equipment, contractor laptops, and BYOD devices are invisible to EDR—yet they represent a growing attack surface.
- **"What is this IP?" slows every investigation**—When an alert fires on an unknown IP address, analysts must pivot between SIEM, EDR, and CMDB tools just to understand what the device is, wasting critical triage time and increasing mean time to resolution.

THE SOLUTION

Corelight Asset Classification analyzes protocol fingerprints captured in network traffic to continuously identify and categorize every device on the network. Built on Zeek®-based network evidence, it passively classifies assets using DHCP and HTTP user-agents—emitting a dedicated asset_classification.log that enriches existing Zeek logs with device context. No additional hardware, agents, or active polling is required.

Key capabilities:

- **Passive, continuous discovery**—assets are identified and classified the moment they communicate, with no scanning windows, no agents, and no network impact
- **Role-aware classification**—asset context is understood not just by what it is, but by what it does—client, server, gateway, DNS resolver—giving teams context, not just a list

- **Software inventory in real time**—OS versions, application banners, and client fingerprints are updated continuously as traffic is observed, not on a scheduled poll
- **Hybrid environment coverage**—the same asset intelligence is derived from physical sensors, cloud software sensors, and VPC traffic mirroring, providing a consistent inventory across on-prem and cloud

Asset intelligence: What is on the network?

- Discover IT, IoT, Shadow and BYOD devices that bypass agent-based tools
- Continuously classify device type, OS, manufacturer, model, and network role from observed traffic
- Surface assets across every network segment with a confidence score (0-100) for each classification
- Enrich a CMDB with real time context and intelligence

Faster investigations: Instant device context

- Turn abstract IP addresses into recognizable, real-world devices directly in Zeek logs
- Prioritize alerts by asset type and criticality (e.g., domain controllers vs. guest Wi-Fi clients)
- Conduct asset-centric threat hunting (e.g., "show me all cameras communicating externally")
- Reduce mean time to resolution by eliminating manual asset lookups during triage

Tool consolidation: Do more with fewer tools

- Replace or reduce reliance on standalone asset discovery and inventory products
- Consolidate asset visibility into the same platform already delivering NDR, eliminating redundant data sources and licensing costs
- Feed asset context into Investigator, existing SIEM dashboards, detection logic, and SOAR playbooks—without adding another tool to the stack
- Extend value of your Corelight sensor investment to asset management and IT operations stakeholders

Operational value: Validate and enrich existing tools

- Use network-derived "ground truth" to validate and supplement CMDB and EDR inventories
- Feed asset context into Investigator, existing SIEM dashboards, detection logic, and SOAR playbooks
- Provide compliance teams with auditable, always-current evidence of asset visibility across IT and IoT
- Extend value of your Corelight sensor investment to asset management and IT operations stakeholders

The solution architecture

1. Passive traffic observation
2. Fingerprint & classify every device
3. Enriched logs with device type & role

HOW IT WORKS

1. Corelight sensors (physical, virtual, or cloud) passively observe mirrored network traffic. Zeek parses protocol data from every connection—no active scanning or agents required.
2. Asset Classification analyzes protocol fingerprints to identify device type, OS, manufacturer, model, and network role.
3. A dedicated asset_classification.log is emitted with each classification event, including a confidence score and the data sources that contributed to the result.
4. Asset context flows directly into Corelight Investigator, SIEMs, and SOAR platforms—enriching alerts, enabling asset-centric hunting, and validating existing CMDB data.

corelight

To learn more about Corelight Asset Classification, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497