

## Data sheet

# Fleet Manager

Streamlined administration  
for multi-sensor traffic analysis



The creators of Zeek® designed Fleet Manager to accelerate the deployment, configuration, and ongoing administration of Corelight Sensors across the enterprise. Fleet Manager serves as the centralized command center for your entire sensor environment—streamlining configuration, health monitoring, policy enforcement, third-party integrations, and threat intelligence management across global deployments.

### Role-based administration

Assign user roles and individual access levels across your team. Fleet Admins define roles and grant rights to groups of sensors. Monitor-only access roles allow individuals to track sensor metrics for reporting purposes without modifying configurations.

### Rapid sensor configuration

Customizable policy templates allow you to define and deploy sensor settings across your entire fleet from a single interface. Configurable capabilities include:

- Zeek packages and custom scripts
- Suricata IDS rulesets and rule management
- Smart PCAP capture policies and SPCAP Suricata Levers
- YARA rules for file and payload analysis
- Input filters and traffic selection
- Export targets and export filters (SIEM, SOAR, XDR, cloud analytics)
- Net-perf thresholds and asset classification settings
- Threat intelligence feeds and enrichment sources

Deploy new configurations or policy templates in minutes to individual sensors or across your entire fleet.

### Centralized software management

Deploy software upgrades and new Zeek packages across your fleet from a single interface. Fleet Manager tracks sensor versions, flags sensors that need upgrades, and supports coordinated rollouts to minimize operational disruption.

### Third-party integrations

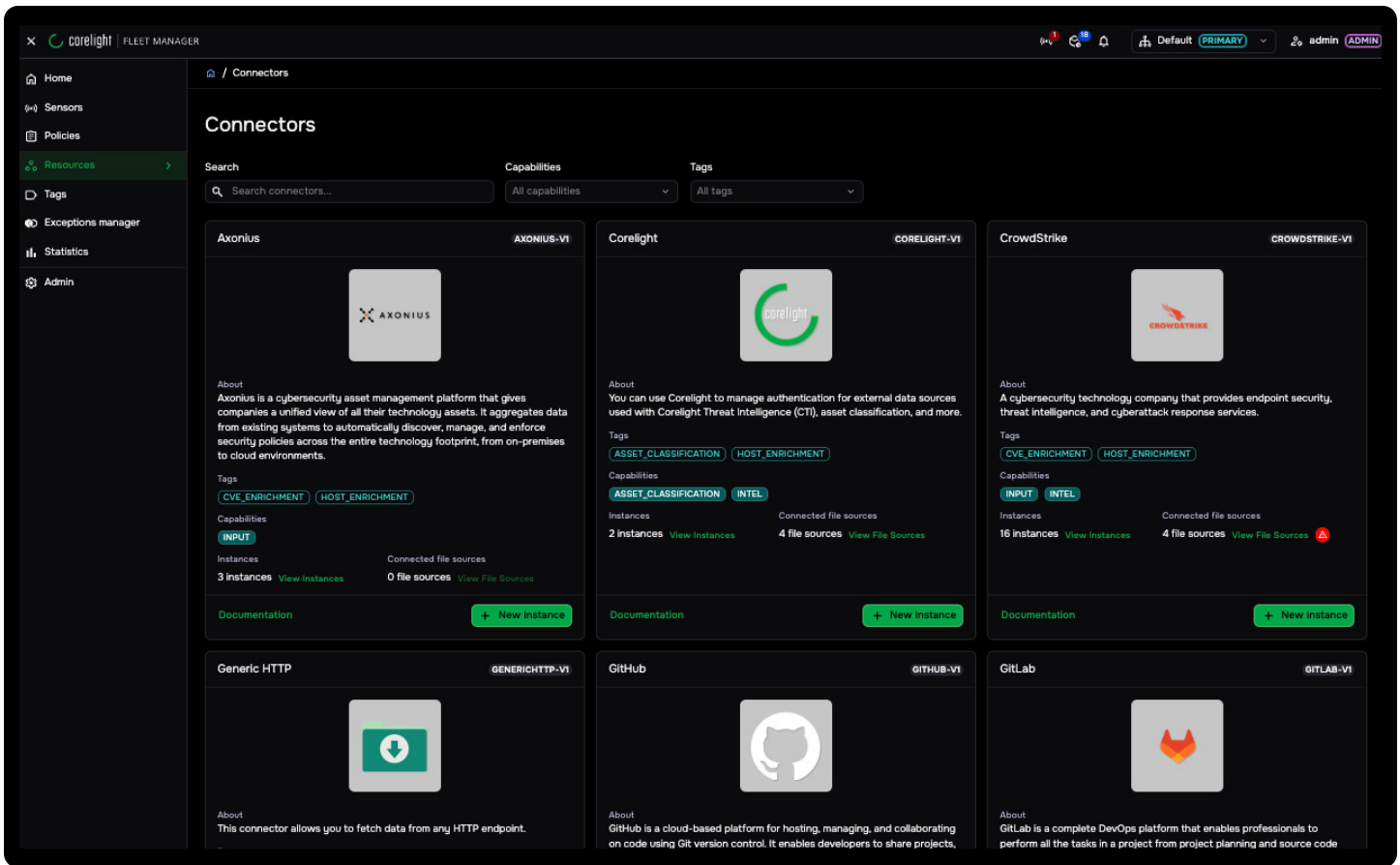
Fleet Manager serves as the central management point for third-party integrations. A connector-based architecture lets organizations configure, monitor, and manage external data sources directly from Fleet Manager—eliminating the need for custom scripts, manual feed imports, or standalone integration infrastructure. Available connectors span endpoint and vulnerability management platforms, threat intelligence feeds, asset classification sources, and generic file-based sources.

### Exception-driven reporting

Monitor sensor health and performance metrics—including Zeek log output rates, CPU and memory utilization, and traffic throughput—and quickly drill into individual sensors. Get immediate, actionable insight into issues ranging from sensor connectivity problems to available software upgrades.

### Compliance and audit

Demonstrate compliance using built-in audit logs that track all configuration changes, user actions, and policy deployments across the sensor fleet.



## Fleet Manager at a glance

Capability	Detail
Sensor management	Manage up to 250 sensors from a single interface
Fleet health dashboard	Overall fleet health in one pane of glass; drill into individual sensor metrics with one click
Sensor groups	Define custom sensor groups for policy management and reporting
Role-based access	Assign individual user roles and access levels; monitor-only roles for reporting
Policy templates	Create and deploy custom sensor policy templates for input filters, export targets, and Zeek packages
Software upgrades	Deploy Zeek packages and sensor software upgrades across the fleet
Audit logging	Full audit trail of configuration changes and user actions for compliance

## Fleet Manager at a glance

Capability	Detail
Connector authentication	Configure and manage third-party connectors including Axonius, CrowdStrike, Tenable, Generic HTTP, Microsoft Defender, and SentinelOne
Threat intelligence management	Distribute threat intelligence feeds to all sensors from a central policy configuration—no per sensor setup
Export configuration	Configure export targets for SIEM, SOAR, XDR, and cloud analytics platforms
Light and Dark Modes	Available UI themes for user preference
Deployment options	Linux package installed on physical host, virtual machine, or cloud IaaS instance

## Deployment specifications

Corelight Fleet Manager is delivered as a Linux package:

- Manages up to 250 sensors
- Deployable on physical host, virtual machine, or cloud IaaS instance

## Host machine requirements

Resource	Minimum requirement
RAM	32 GB
CPU	4x+ cores
Disk	500 GB

## Ecosystem integration:

Fleet Manager configures sensor export to Investigator, SIEMs (including CrowdStrike Falcon Next-Gen SIEM, Elastic, Google Security Operations, Microsoft Sentinel,) SOAR, XDR, data lakes, and cloud analytics platforms. Third-party connectors manage inbound data from threat intelligence and asset enrichment sources—making Fleet Manager the single control plane for all data flowing in and out of the sensor fleet.



To learn more about Corelight Fleet Manager, request a demo at

<https://corelight.com/contact>

info@corelight.com | 888-547-9497