corelight



White paper

Advancing Federal cyber operations under OMB M-26-14

How Corelight helps agencies move beyond log collection

New guidance from the Office of Management and Budget (OMB) signals a strategic evolution in how federal agencies approach cybersecurity operations. With the release of M-26-14, OMB has rescinded M-21-31 and shifted focus from large-scale log retention toward a more risk-informed, operational model centered on measurable security outcomes, real-time visibility, and effective cyber defense.

Rather than emphasizing the retention of increasingly large volumes of log data, M-26-14 prioritizes operational effectiveness, specifically the ability to rapidly detect, investigate, and respond to evolving cyber threats. The guidance identifies two critical operational capabilities agencies are expected to mature on accelerated timelines:

1. **Continuous Event Monitoring (CEM)**
   Real-time monitoring, anomaly detection, and operationalized Security Operations Center (SOC) workflows

2. **Threat Hunting, Investigation, Response, and Forensics (THIRF)**
   Threat hunting, digital forensics, attack reconstruction, and scalable long-term evidence retention

Many federal agencies continue to face growing operational challenges, including rising SIEM costs, fragmented telemetry, alert fatigue, and limited visibility across cloud, operational technology (OT), and unmanaged environments. M-26-14 reflects an important shift in federal cybersecurity priorities by recognizing that collecting more logs alone does not necessarily improve defensive outcomes. Instead, agencies are expected to prioritize telemetry and evidence that directly strengthen detection, investigation, response, and mission resilience.

Meeting these timelines with existing analyst capacity requires more than better data collection. Agencies are increasingly turning to AI-assisted SOC workflows and agentic triage to accelerate detection, investigation and response—making the quality and structure of underlying telemetry a strategic decision, not just a logging requirement.

Corelight transforms network and cloud activity into high-fidelity, structured, and correlated evidence federal security teams can use for real-time monitoring, threat hunting, incident response, forensic analysis, and to demonstrate measurable operational outcomes under M-26-14.

Where Corelight contributes:

- **Complete triad visibility (EDR + NDR + identity):** Corelight provides the critical Network Evidence pillar, enabling analysts to seamlessly correlate and pivot between endpoint alerts, identity logs, and network behavior via standardized correlation keys like Community ID
- **Coverage for HVAs, OT, and specialized environments:** For High Value Assets (HVAs), industrial control systems (OT), IoT, and unmanaged devices where host logging is absent or impossible, capturing rich, context-aware network traffic serves as the primary line of defense
- **Encrypted & cloud telemetry:** Passive network monitoring provides evidence across encrypted, cloud, and partner-connected environments without requiring intrusive break-and-inspect infrastructure

Accelerated federal logging maturity requirements

Under M-26-14, agencies are expected to rapidly advance logging and monitoring capabilities following publication of CISA's Logging Reference Architecture (LRA).

Maturity tier	Timeline	Operational focus
Initial Agency Logging Plan	Within 90 Days of LRA	Document mission risk priorities and logging strategy
EL1 (Basic)	Within 120 Days	Establish foundational real-time monitoring and essential logging
EL2 (Intermediate)	Within 180 Days	Expand encrypted traffic visibility and hybrid data workflows
EL3 (Advanced)	Within 320 Days	Fully integrate CEM and THIRF across enterprise, cloud, IoT, and OT environments

The accelerated implementation timelines leave little room for fragmented visibility or isolated telemetry. Agencies need network evidence that supports faster detection, investigation, and response across existing SOC operations.

How Corelight supports the LRA's two operational outcomes

Continuous Event Monitoring (CEM)

- **Add network-level visibility:** Convert network traffic into structured Zeek®, IDS, file-analysis, and protocol evidence for SOC monitoring
- **Supplement existing controls:** Identify lateral movement, DNS tunneling, anomalous SMB, C2, and activity on assets without endpoint agents
- **Support existing SOC workflows:** Send open, structured telemetry and detections to agency SIEM, XDR, data lake, and automation platforms

Threat Hunting, Investigation, Response & Forensics (THIRF)

- **Rapid Correlation:** Pivot seamlessly from an endpoint alert or identity event directly to associated network sessions, application protocols, extracted files, and packet captures
- **Support retrospective analysis:** Use high-fidelity metadata, threat-intelligence retro-matching, and Smart PCAP to investigate known or suspected compromise
- **Document evidence-supported findings:** Preserve inspectable network evidence that analysts can validate, explain, and use in incident reporting
- **Accelerate investigation and response with agentic AI:** Corelight's network evidence powers agentic AI workflows that compress multi-hour manual investigations into minutes

Five maturity elements. One network-evidence foundation.

1 Inventory visibility	2 Collection coverage	3 Collection operations	4 Data retention	5 Log management
Observe communicating IT, IoT, OT, and unmanaged assets.	Provide evidence where native logging is limited, unavailable, or on High Value Assets (HVAs).	Supply searchable telemetry, tunable detections, and out-of-the-box auto-normalization to meet CISA Minimum Event Fidelity standards.	Retain relevant insight while reducing repetitive log volume by 50–80%.	Capture data close to the authoritative source and route open telemetry into centralized or federated agency workflows.

Supporting Continuous Event Monitoring (CEM)

Endpoint tools provide important visibility, but many federal environments include systems where agents cannot be consistently deployed, including cloud workloads, operational technology (OT), IoT devices, unmanaged assets, partner-connected infrastructure, and legacy systems.

Corelight provides passive, network visibility across these environments by analyzing activity directly from network traffic. Because adversaries must traverse the network to move between systems, network evidence provides a reliable means of identifying suspicious or malicious activity.

Since Corelight's telemetry is collected passively, it also provides a source of evidence that adversaries cannot easily disable or manipulate, and collection will not risk disrupting critical operations.

Operationalizing the SOC

Corelight helps agencies move beyond log collection by delivering structured, high-fidelity network evidence mapped to widely used security schemas, including:

- Splunk Common Information Model (CIM)
- Elastic Common Schema (ECS)

This allows security teams to integrate network evidence into existing SIEM, UEBA, SOAR, and analytics workflows without extensive data normalization or custom parsing.

Derived directly from observed traffic, Corelight telemetry provides richer context for detection, investigation, and threat hunting across cloud, on-premises, hybrid, and operational technology (OT) environments. Built on widely adopted open standards including Zeek and Suricata, Corelight data integrates more easily across existing security architectures without requiring proprietary workflows or extensive customization. This gives agencies greater flexibility as they modernize SOC operations and evolve their security environments over time.

As agencies adopt AI-assisted SOC workflows, the quality of underlying telemetry becomes increasingly important. AI systems are only as reliable as the data they analyze. Corelight's approach focuses on providing high-integrity network evidence that helps analysts investigate activity with greater confidence, context, and consistency.

High-fidelity threat detection

To meet M-26-14's shift toward operational security outcomes,

Up to 5x
longer practical lookback for forensics

agencies require detection capabilities that extend beyond traditional signature matching. Corelight delivers multi-layered threat detection by combining signature analysis with behavioral detection engines built on open standards like Zeek and Suricata. This enables real-time identification of complex adversary behaviors, such as lateral movement, command-and-control channels, and data exfiltration, across hybrid, cloud, and unmanaged environments.

By generating pre-correlated, high-confidence detections directly at the network layer, Corelight helps SOC teams catch sophisticated threats earlier in the attack lifecycle while significantly reducing low-value alert noise.

Enabling agentic triage and AI-assisted workflows

As federal agencies integrate AI-assisted SOC workflows and autonomous AI agents to accelerate incident response, the reliability of these tools depends entirely on the

quality of their underlying telemetry. Corelight's structured, schema-aligned network evidence provides the clean, high-context data required for effective agentic triage.

Corelight's structured, schema-aligned network evidence gives AI agents the connected evidence graph they need to investigate autonomously. Using standardized correlation keys like Community ID, agents can trace activity from DNS resolution through connection to HTTP session to file extraction—following the same investigative path a senior analyst would, but completing it in minutes instead of hours.

Every investigative step is transparent and auditable, giving agencies a defensible record of how conclusions were reached. Expert-authored playbooks provide guardrails that deliver repeatable results, so the same alert produces the same conclusion every time – a critical requirement for agencies that must demonstrate consistent operational outcomes under M-26-14.

This accelerates initial alert triage and investigation, allowing security analysts to move faster and focus their attention on complex threat hunting.

Faster correlation and investigation

Corelight's Community ID enables analysts to correlate network events across multiple security data sources and investigative workflows. This supports faster pivoting between alerts, automated enrichment, and more efficient incident response operations.

The approach also aligns with Zero Trust principles by strengthening continuous monitoring, improving visibility across hybrid environments, and supporting rapid validation of suspicious activity.

Hybrid storage and long-term retention

Corelight supports concurrent event forwarding to multiple destinations, allowing agencies to:

- Send high-value telemetry to SIEM platforms for immediate analysis
- Preserve raw or filtered network evidence in long-term data lakes or object storage
- Balance investigative accessibility with storage efficiency

This architecture aligns with M-26-14's emphasis on scalable, risk-based data retention strategies while helping agencies reduce unnecessary data duplication and storage overhead.

Cloud workload visibility: Transforming VPC flow logs

As agencies migrate critical workloads to the cloud, raw cloud telemetry, such as Amazon VPC Flow Logs, often generates immense data volumes with limited investigative value. While these logs capture basic network routing details, their sheer size can quickly overwhelm SIEM architectures and storage budgets.

Corelight helps agencies overcome this challenge by ingesting raw cloud flow logs and transforming them into structured, high-fidelity Zeek evidence. This process reduces log volume by up to 90% through intelligent deduplication while enriching the data with deep threat context. By standardizing cloud telemetry to match on-premises network evidence, agencies can achieve continuous monitoring across their cloud footprint without sacrificing storage efficiency or investigative speed.

50-80%

less network-log volume with data aggregation

SUPPORTING THREAT HUNTING, INVESTIGATION, RESPONSE, AND FORENSICS (THIRF)

Cost-effective evidence retention

M-26-14 specifically emphasizes retaining data that provides operational value. Corelight supports this model through Smart PCAP, which enables selective packet capture tied to high-confidence detections, investigative triggers, or defined threat profiles.

This allows agencies to retain detailed forensic evidence without maintaining prohibitively expensive full-packet archives across all network activity.

Visibility into encrypted threat activity

As adversaries increasingly use encrypted channels to conceal command-and-control activity and lateral movement, agencies need visibility that does not rely entirely on decryption infrastructure.

Corelight Encrypted Traffic Collection (ETC) provides metadata and behavioral insights into encrypted traffic without requiring full break-and-inspect architectures. This helps agencies strengthen detection efforts while reducing operational complexity and minimizing privacy concerns.

By focusing on high-fidelity telemetry rather than indiscriminate data collection, agencies can improve detection quality while reducing noise and downstream processing demands across SOC operations.

Corelight capability alignment to M-26-14

Maturity level	M-26-14 focus area	Corelight alignment
EL1	Standardized logging and foundational network visibility	Passive DNS, DHCP, flow telemetry, correlated timestamps, and SIEM integration
EL2	Encrypted traffic visibility and event correlation	Encrypted Traffic Collection, DPI-linked telemetry, Community ID correlation, and hybrid forwarding architectures
EL3	Enterprise-wide visibility and advanced investigations	Coverage across physical, virtual, cloud, IoT, OT, and containerized environments with advanced detection scripting and interoperable data formats

Corelight's open architecture helps agencies modernize security operations while avoiding vendor lock-in and preserving interoperability across evolving federal security stacks.

A practical path to LRA-aligned network visibility

Corelight complements agency system, identity, endpoint, application, and cloud logs. It provides an independent source of network evidence that can help agencies verify activity across domains, investigate gaps, and add context to other security data.

1 Prioritize

Map mission risk, HVAs, High Impact Systems, and critical attack paths.

2 Collection coverage

Place physical, virtual, and cloud sensors where network evidence addresses priority visibility gaps.

3 Operationalize

Route relevant telemetry and detections to CEM and THIRF workflows; tune them for agency use cases.

4 Measure and mature

Track asset visibility, coverage, searchability, operational value, retention, and governance over time.

Integration with existing agency architecture

- **Flexible deployment & source resilience:** Deploy via physical, virtual, cloud, or SaaS options. Sensors capture data at the authoritative network source and support local event buffering during disconnected states to preserve data provenance and ensure zero loss.
- **Open data and integration:** Natively streams auto-normalized, industry-standard Zeek logs into resilient event processing pipelines (Kafka, AWS Pub/Sub, Logstash) as well as existing SIEM, XDR, and Data Lake platforms.
- **Operational support:** Fleet management, curated detection content, Investigator, and technical services can assist teams with deployment, tuning, and sustainment.

Plan a phased approach to network evidence for the CISA LRA

Corelight can work with agency teams to assess priority visibility gaps, align network telemetry to CEM and THIRF objectives, and identify practical steps toward measurable logging maturity.

Conclusion

M-26-14 reflects a broader shift in federal cybersecurity priorities from collecting more telemetry to producing more operationally useful evidence.

As agencies prepare to meet accelerated implementation timelines, they are increasingly expected to demonstrate that logging and monitoring strategies directly support detection, investigation, response, and mission resilience. Meeting those expectations requires visibility that extends beyond endpoints and cloud APIs to include the network itself and the AI-assisted workflows that turn network evidence into faster, defensible outcomes.

Corelight transforms network and cloud activity into high fidelity evidence security teams can use to detect threats faster, investigate activity with greater confidence, and build the evidence-driven cyber defense operations M-26-14 demands.

7:1

average log consolidation reported in early access

corelight

To learn more about advancing federal cyber operations under OMB M-26-14, request a demo at

https://corelight.com/contact

info@corelight.com

The Z and Design mark and the ZEEK mark are trademarks and/or registered trademarks of the International Computer Science Institute in the United States and certain other countries. The Licensed Marks are being used pursuant to a license agreement with the Institute.

All rights reserved. © Copyright 2026 Corelight, Inc.