Strengthening Threat Detection and Investigation With Network Traffic Analysis

Every year, attackers find new ways to bypass traditional controls and move across environments without detection. Security teams must interpret growing volumes of telemetry, while also dealing with skill shortages and rising operational demands. Much of the activity behind successful attacks happens on the network. Servers, unmanaged assets, cloud workloads, and connected devices communicate constantly, creating activity patterns that reveal early indicators of compromise (IoCs).

Organizations need a reliable way to observe these communication paths and extract the network metadata that accelerates threat detection and investigation. The right network traffic analysis solution provides structured, high-value evidence that enriches analytics, reduces unnecessary noise, and helps analysts understand what happened across hosts and users.

Exabeam NetMon gives security teams real-time visibility into network activity, actionable detections, and the context needed to confirm suspicious behavior. NetMon supplies critical network insights directly into Exabeam timelines, investigations, and threat hunting workflows, helping analysts work faster and make well-supported decisions.

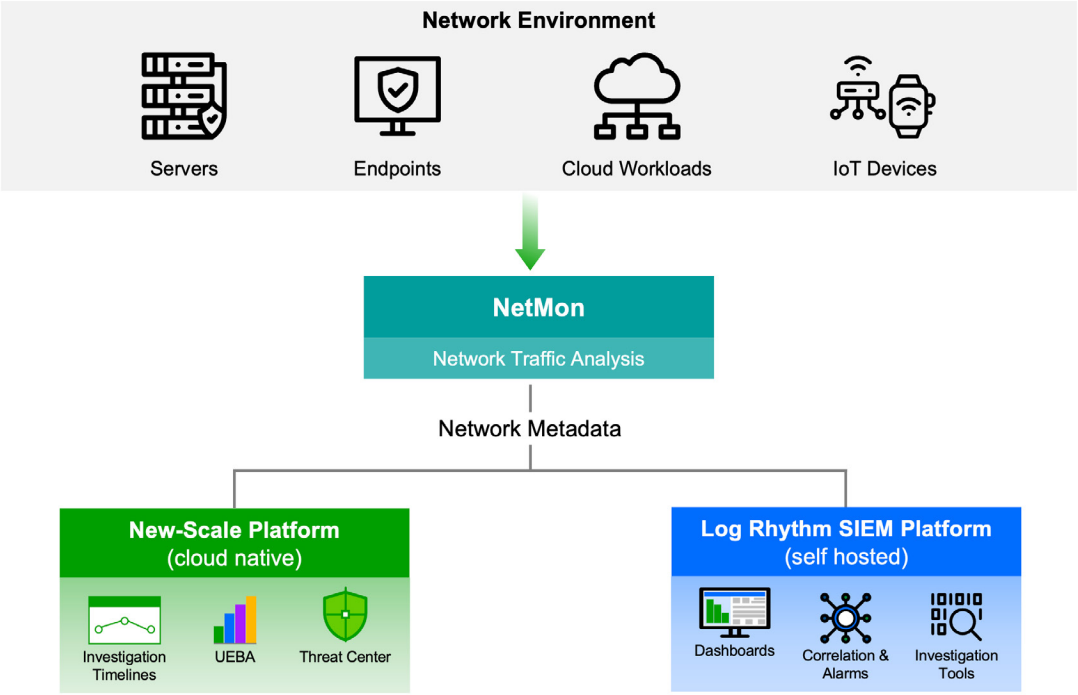

Figure 1. NetMon extracts network metadata and sends it to the New-Scale Security Operations Platform or the LogRhythm SIEM Platform for detection and investigation workflows.

Why Attackers Still Succeed on the Network

Attackers continue to take advantage of weak points across hybrid environments. Several trends contribute to the problem:

More Digital Connectivity

Modern organizations depend on cloud services, distributed applications, and an expanding mix of devices. Not every device supports an agent and traffic patterns shift constantly. As a result, some activity becomes difficult to observe using endpoint data alone. Endpoint security controls also may not stop lateral traffic and won't track movement between networks effectively.

Increasingly Sophisticated Attacks

Attackers continue to refine their methods by blending in with routine traffic or hiding command-and-control activity inside encrypted sessions. They explore new entry points, including weak ports, VPN vulnerabilities, targeted phishing, and credential misuse. Once inside, they often move between internal systems using subtle, low-noise techniques that are easy to overlook without deeper network visibility.

Overwhelmed Teams

Security teams face talent shortages, time-consuming investigations, and telemetry sources that produce too many low-value alerts. Without clear evidence of how systems communicate, analysts can spend hours validating a single suspicious event with only a limited view into what's happening at the network layer.

High Volumes of Network Data

Networks generate enormous amounts of information. Monitoring every packet is unrealistic, yet ignoring network traffic leaves significant gaps. Security teams need distilled, structured network metadata that surfaces meaningful patterns without adding operational overhead.

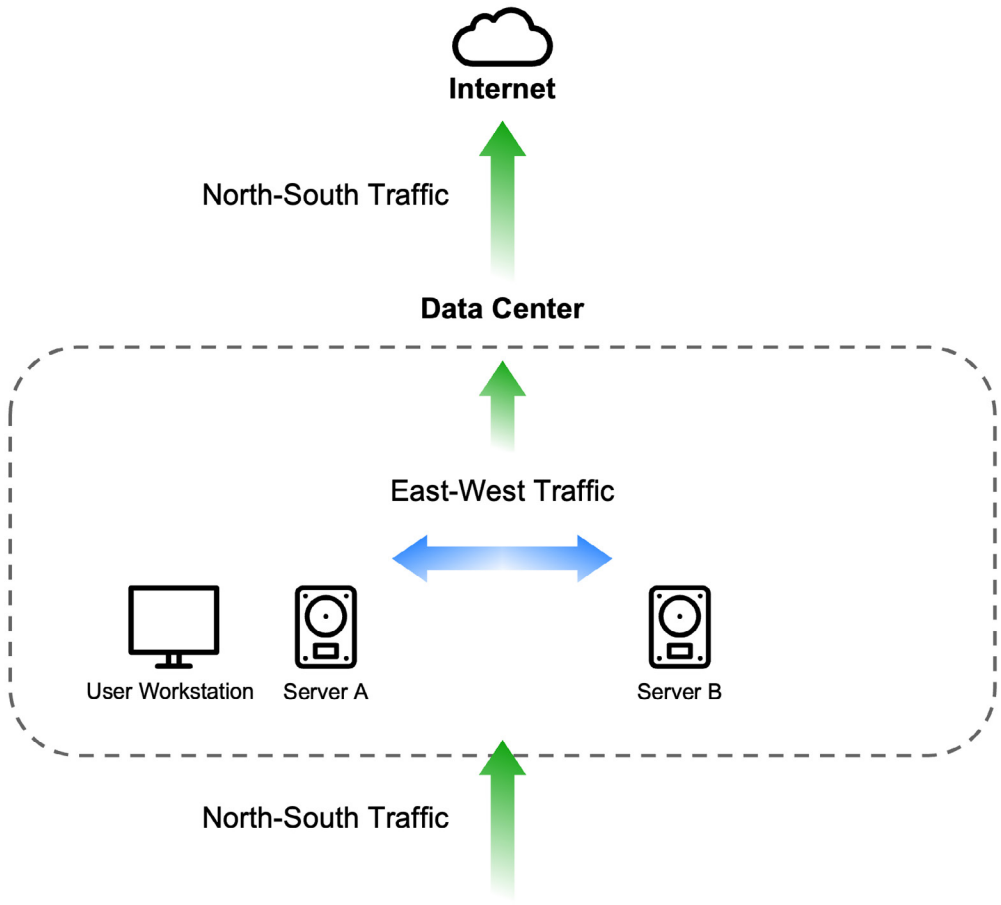

Figure 2. NetMon provides visibility into both north-south and east-west communication paths across the environment.

The Role of Modern Networking

Network traffic analysis tools play an essential part in helping analysts detect threats earlier and investigate more effectively. They collect, organize, and analyze traffic across users, hosts, applications, and devices. This provides a richer view of activity inside the environment.

What Modern Network Traffic Analysis Delivers

- **Visibility into east-west and north-south traffic:** Understand how devices, workloads, and users transmit data.
- **Insights into unusual connections:** Identify rare destinations, suspicious protocol use, or unexpected volume changes.
- **Context for credential misuse:** Detect failed attempts, privilege escalation patterns, or lateral movement behaviors that rely on network hops.
- **Early indicators of malware activity:** Highlight command-and-control communication, data staging behavior, or anomalous outbound patterns.
- **Support for investigations:** Provide analysts with network-derived evidence to validate or disprove suspicious events.

As attack techniques evolve, structured network metadata becomes one of the most valuable inputs into detection and investigation workflows.

How NetMon Works

NetMon captures, inspects, and enriches network traffic to provide the insights that security teams need. Unlike full packet capture tools, NetMon focuses on metadata and high-value indicators so organizations receive meaningful information without unnecessary data volume.

Core Capabilities

Comprehensive Monitoring

NetMon observes traffic between servers, endpoints, cloud workloads, and connected devices. It extracts metadata that reveals who communicated with whom, when, and using what protocol or application.

Detection Based on Behavior and Signatures

NetMon includes rule-based detections that surface suspicious traffic patterns, rare connections, unapproved protocols, and indicators of compromise.

Dashboards and Workflows Tailored for Security Analysts

Analysts can explore network connections, unusual activities, and communication patterns in formats designed for rapid triage.

Evidence for Incident Timelines

Network metadata feeds directly into the New-Scale and LogRhythm SIEM platforms, giving analysts a chronological view of activity across hosts and users.

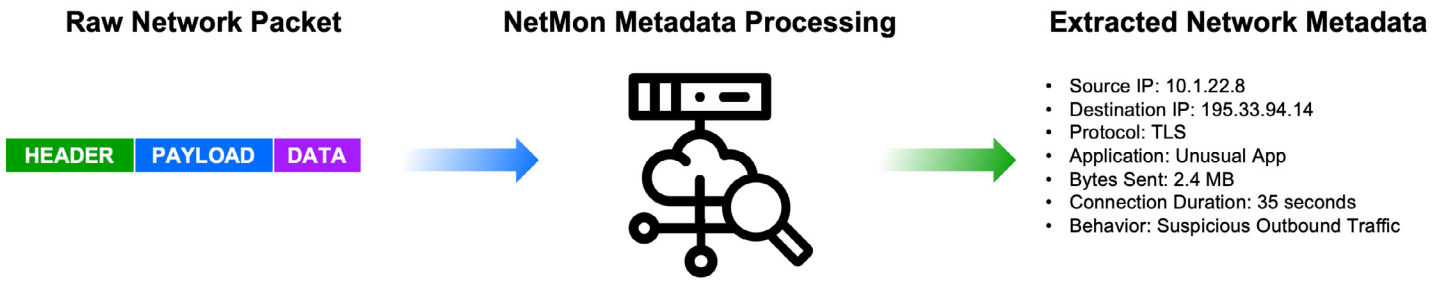

Figure 3. NetMon extracts structured metadata that helps analysts interpret traffic without requiring full packet capture.

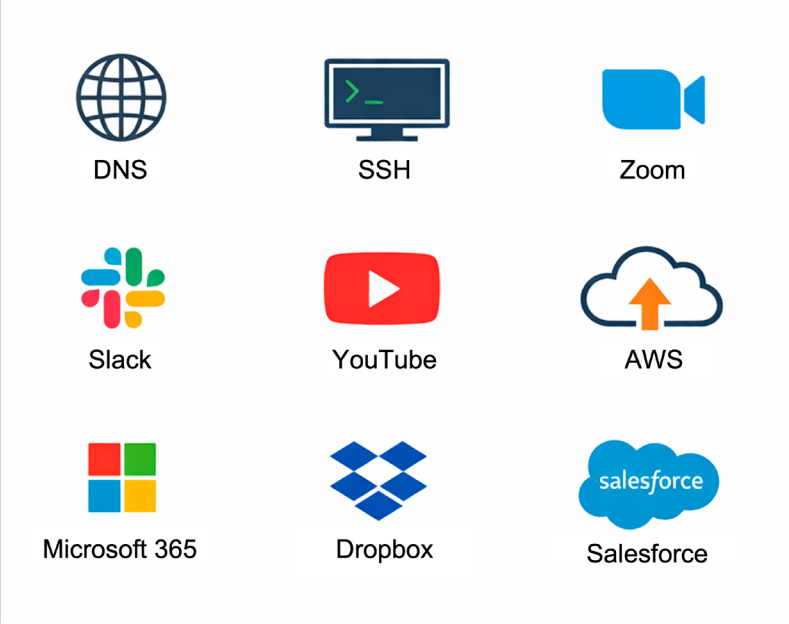

Figure 4. NetMon recognizes thousands of applications, helping analysts understand what is moving across the network.

How Exabeam Strengthens Detection and Investigation

NetMon becomes even more impactful when its network-derived evidence flows into timelines, detections, and investigations.

Better Detections Through Correlated Context

Exabeam combines network metadata with user, endpoint, and cloud data to reinforce signals and reduce unnecessary alerts. Suspicious network behavior is easier to understand when viewed in relation to user sessions, authentication patterns, and assets involved.

Faster Investigation of Suspicious Activity

Analysts can quickly see network connections associated with events, making it easier to confirm whether something is normal or unusual. Timelines display network activity alongside other signals such as file access, authentication, or policy changes.

Coverage for Unmanaged or Hard-to-Instrument Assets

Many organizations have devices where installing an agent is impractical. Network traffic analysis fills the observation gap by showing how these devices communicate within the environment.

Support for Threat Hunting

Security teams can search for rare connections, high-risk protocols, or communication paths related to known attack techniques.

Investigation Efficiency Snapshot

Stage of Investigation	Without NetMon	With NetMon
Identify unusual activity	Log-only visibility	Network evidence provides clearer signals
Validate behavior	Requires manual querying	Metadata shows communication patterns
Determine scope	Partial picture	Full view of internal and external traffic
Time to review	Longer	Shorter

Table 1. NetMon adds essential network evidence that supports faster, more informed investigations.

Use Case: Network Visibility for Growing Organizations

A rapidly expanding technology provider sought better visibility into the traffic flowing through its hybrid environment. With new services coming online and increased customer demand, the security team needed a way to observe internal communication patterns and detect suspicious activity earlier.

Challenges

- Limited visibility into east-west movement
- Difficulty verifying whether unusual alerts were meaningful
- Growing number of connected systems and cloud workloads
- Concern about data exfiltration and hidden command-and-control traffic

Solution

The organization deployed NetMon across its core network segments. NetMon provided structured metadata about communication patterns, highlighting rare destinations and unexpected protocol usage. Analysts used the automated timelines in the New-Scale Security Operations Platform to:

- Identify unusual sequences of authentication and network access
- Trace communication paths associated with potential malware activity
- Validate whether outbound traffic was intentional or suspicious
- Reduce time spent reviewing false leads

Outcome

NetMon helped the team detect early signals of malicious behavior, including attempted outbound connections to unrecognized destinations. By viewing network events alongside user and endpoint activity, analysts reduced investigation time and gained a clearer understanding of internal movement patterns. The organization strengthened its ability to protect expanding digital services without adding unnecessary operational overhead.

Conclusion

Network traffic analysis plays a central role in improving threat detection and investigation. NetMon gives security teams a structured, reliable view of how systems communicate. When used with the cloud-native New-Scale Platform or the self-hosted LogRhythm SIEM Platform, NetMon adds the network-focused evidence that strengthens detection, correlation, triage, and response.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam™

Learn more at
www.exabeam.com →