SOLUTION BRIEF

endace
Record. Respond.

sumo logic

Fast Troubleshooting And Investigation With Sumo Logic Integrated With Endace Always-On Packet Capture

The Problem

The most serious threats and issues require hard packet capture evidence that exposes exactly what's happening before, during and after any event, allowing you to confidently respond, remediate, and report. However, many teams lack the confidence and experience to search and analyse packet capture data when responding to threats.

When logs and events have been wiped, manipulated, or just lack the details, always-on network packet capture gives you a tamper-proof record of all activity across all your environments, allowing you to fully understand and respond to any threat. Packet capture workflow integration is crucial in helping team members with fast search and easy analysis of packet data when dealing with serious threats.

Organizations need a solution that:

- Provides always-on packet capture (not triggered capture) to record every incident reliably.
- Can be deployed on all the organization's infrastructure – including on-premise, private and public cloud.
- Delivers the required functionality while being easy-to-use and fast to implement.
- Is cost-effective and scalable.
- Integrates with existing security solutions and workflows
- Has the flexibility to change easily to meet evolving needs.

Benefits

- Always-on recording to capture all traffic
- Store weeks or months of full packet capture data for a complete record of network activity.
- Rapid search and data-mining
- Full visibility across complex networks including Hybrid and Multi Cloud, including visibility into encrypted traffic.
- Deliver accurate, reliable, tamper-resistant forensic data to your security tools and teams.
- Fast troubleshooting and investigation with AI/ML -powered log analytics
- Resolve cloud-native attacks with cloud-native scale
- Easy to deploy, integrates with existing infrastructure. Open architecture to work in multiple environments.
- Security hardened. Compliant with FIPS 140-3 and NIAP NDcPP 2.2E.

The Solution

When Sumo Logic is combined with Endace's always-on packet capture, organizations gain broad and deep visibility into their on-prem and cloud infrastructures. The full packet data captured by the solution become a valuable source of tamper-proof evidence for investigating the seriousness and extent of any threat.

The Sumo Logic SaaS Log Analytics Platform is designed to monitor, troubleshoot, and secure your applications, at scale, across hybrid environments. The platform provides scalable log analytics, SIEM, APM and more, all in one place.

EndaceProbes enhance your troubleshooting and investigations with comprehensive always-on network recording of all the traffic anywhere in your environment, enabling in-depth drill down to the ultimate network forensics.

EndaceProbes can record and store weeks or months of full packet capture data across on-premise, public or private cloud environments. Multiple EndaceProbes can be connected to provide a unified, hybrid cloud recording fabric. This fabric enables rapid, centralized search, data-mining and analysis of recorded traffic. It integrates directly into security tools from Sumo Logic, Cisco, Palo Alto Networks, and many other vendors to enable fast, efficient investigation and resolution of network security and performance issues.

Conclusion

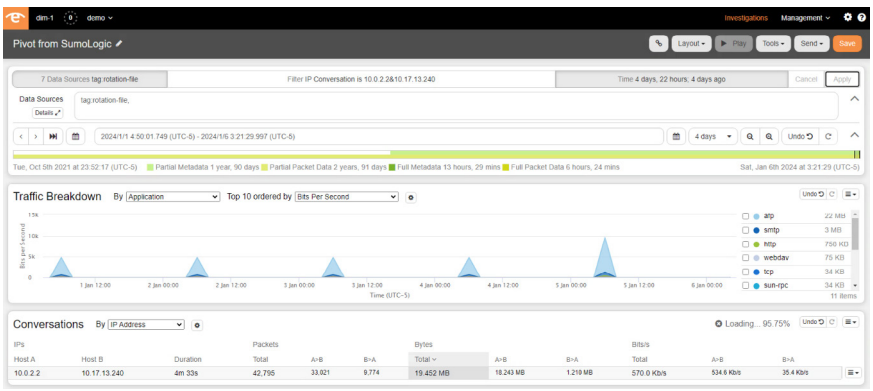
Together, Sumo Logic and Endace provide hard evidence required to hunt for and combat the most serious threats, and challenging IT and networking issues.

This joint solution ensures your network is underpinned by an architecture that dramatically improves your visibility into - and ability to defend against – current and future cyber threats. It also ensures your infrastructure has the flexibility to adapt as your organization's cybersecurity needs evolve.

How it works

Streamlined Investigations

- Analysts can click to pivot directly from alerts in Sumo Logic to view related packet data in InvestigationManager - which searches data recorded by EndaceProbes on the network.
- Analysts can zoom in or out on the timeline and apply different filters or views to analyze traffic related to the alert and look at packets-of-interest.
- Decoded full packet data can be viewed directly in Wireshark™ (hosted in InvestigationManager) without downloading pcap files.
- If desired, pcaps can be downloaded for archival, or for further analysis using other tools.



Solution Components

- Sumo Logic Troubleshooting and Monitoring, Cloud Infrastructure Security, and Cloud SIEM
- EndaceProbe™ Always-On Packet Capture for On-Premise and Cloud