

Accelerate Incident Response by Integrating Exabeam LogRhythm with Endace Always-on Packet Capture



The Problem

Modern security operations centers rely on SIEM platforms like LogRhythm to gather as much telemetry and log data as possible from both on-prem and cloud infrastructures. However, the one type of telemetry no SIEM is economically and realistically architected for is the ultimate network forensic evidence: continuous full packet data. The most serious threats and issues require full packet capture evidence to expose what is happening before, during, and after any event so analysts can confidently respond, investigate, and remediate the issue.

When logs and events have been wiped, manipulated, or just lack sufficient detail, always-on packet capture gives you a tamper-proof record of all activity across your network, allowing you to understand and respond to any threat or issue quickly and accurately. Simple workflow integration with your SIEM platform is crucial in helping team members quickly find and analyze packet data to respond to serious threats or performance problems.

Organizations need a solution that:

- Provides continuous full packet capture (not triggered capture) for reliable incident recording.
- Supports deployment across on-prem, private and public cloud infrastructure.
- Delivers the required functionality while being easy to use and fast to implement.
- Is cost-effective and highly scalable.
- Has the flexibility to easily meet evolving needs such as SOAR and XDR solutions via API integration.

Benefits

- Always-on recording to record weeks or months of full packet capture data for a complete record of network activity.
- Streamlined investigation workflows from LogRhythm SIEM with one-click access to full definitive packet evidence, accelerating investigations, and enabling accurate event reconstruction.
- Comply with mandatory and best practice requirements including HIPAA, M-21-31, NERC CIP, PCI-DSS, SAMA and more.
- Definitive evidence trail with an accurate record of all relevant packets related to any threat or issue.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- Zero-day threat risk validation with recorded network playback and threat analysis.
- Full visibility across complex networks, including Hybrid and Multi-Cloud.
- FIPS and Common Criteria/NIAAP certification for deployment in high security environments.

SOLUTION BRIEF: EXABEAM

Accelerate Incident Response by Integrating Exabeam LogRhythm with Endace Always-on Packet Capture

The Solution

By combining LogRhythm SIEM with Endace's always-on packet capture, organizations can improve their incident response, threat-hunting, and investigation accuracy with complete historical visibility into threats and performance issues across their on-prem and cloud networks.

LogRhythm SIEM offers a unified experience across SIEM, SOAR, and threat intelligence to drive better detection, investigation, and response. It enables SOC teams to collect security telemetry data, apply threat intel to identify high priority threats and drive response with playbook automation, case management and collaboration.

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

Every EndaceProbe continuously records days, weeks or months of full packet capture data from on-prem, public or private cloud environments. Multiple EndaceProbes (including on-prem and cloud EndaceProbes) can be connected to provide a unified, hybrid cloud recording fabric. This fabric provides fast, centralized search, data-mining and analysis of recorded traffic, and powerful user

workflows directly from LogRhythm SIEM that put evidence at analysts' fingertips, enabling faster, more efficient investigation and resolution of network security issues.

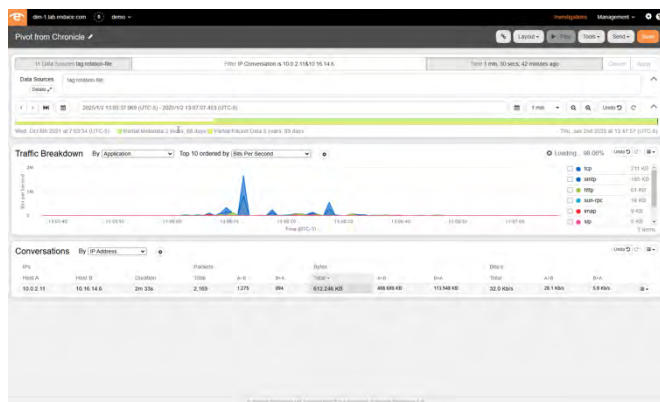
The EndaceProbe's Application Dock hosting capability also enables rapid deployment of agents or sensors without deploying new hardware. Whether it be NDR agents, or virtual NGFW instances hosted in Application Dock, every packet captured and recorded by the EndaceProbe can also be streamed to these tools for real time analysis.

Conclusion

Together, LogRhythm SIEM and EndaceProbes deliver a next-generation AI-powered security platform to accurately detect threats and issues and investigate with confidence with the benefit of full packet evidence at your fingertips. SOC and NOC teams have the definitive evidence they need to conduct fast, conclusive investigations and defend against even the most advanced threats.

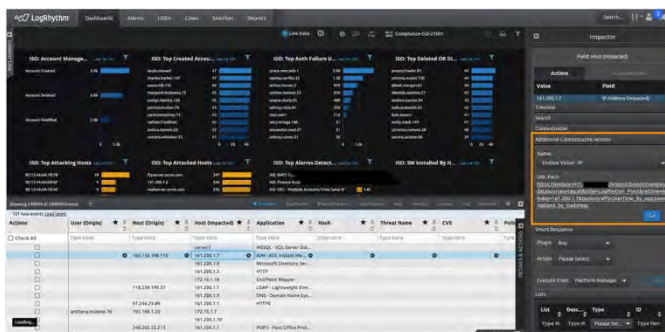
Decryption of traffic before it is recorded gives SecOps teams visibility into threats that might otherwise be hidden in encrypted traffic. Additionally, by hosting third-party analytics tools in the EndaceProbe's Application Dock hosting environment, customers can extend their monitoring coverage without additional hardware deployments.

How it works



Solution Components

- » LogRhythm SIEM
- » EndaceProbe™ Always- On Packet Capture for On-Prem and Cloud environments



© 2025 Endace Technology Limited. All rights reserved. Information in this data sheet may be subject to change.

Endace™, the Endace logo, Provenance™ and DAG™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).