

# Accelerate Incident Response with Google SecOps and Integrated Endace Always-on Packet Capture



Google SecOps

## The Problem

Next Generation Cloud SIEMs are evolving to gather as much telemetry and log data as possible from both on-prem and cloud infrastructures, but the one type of telemetry no SIEM is designed for is the ultimate network evidence: continuous full packet data. However, to solve serious threats and issues analysts need full packet capture evidence to see what happened before, during, and after the event they are investigating so they can confidently investigate and remediate threat activity.

When logs and events have been wiped, manipulated, or just lack sufficient detail, always-on network packet capture provides a tamper-proof record of all activity across all of your environments, enabling you to understand and respond to any threat fully.

Simple workflow integration with your SIEM platform and lightning fast search of packet data enables team members to quickly find and analyze the packet data they need to deal with serious threats.

Organizations need a solution that:

- Provides always-on packet capture (not triggered capture) to record every incident reliably.
- Can be deployed across the organization's entire infrastructure – including on-prem, private and public cloud.
- Delivers the required functionality while being easy to use and fast to implement.
- Is cost-effective and scalable.
- Has the flexibility to adapt and scale 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.
- Streamlined investigation workflows from Google SecOps with one-click access to full definitive packet evidence, accelerates investigations, and enables accurate event reconstruction.
- Comply with mandatory or best practice requirements including HIPAA, M-21-31, NERC CIP, PCI-DSS, SAMA.
- Definitive evidence trails with an accurate record of all relevant packets related to any threat.
- 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, and visibility into encrypted traffic.
- FIPS 140-3 Certified for security.

## The Solution

By combining Google SecOps with Endace's always-on packet capture, organizations can improve their incident response, threat-hunting, and investigation accuracy with the historical visibility to threat actor activity traversing their on-prem and cloud networks.

Google Security Operations offers a unified experience

across SIEM, SOAR, and threat intelligence to drive better detection, investigation, and response. It is a platform that enables you 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 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.

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 probes) can be connected to provide a unified, hybrid cloud recording fabric. This fabric enables rapid, centralized search, data-mining and analysis of recorded traffic, and with simple user workflows directly from Google SecOps SIEM or SOAR, enabling faster, more

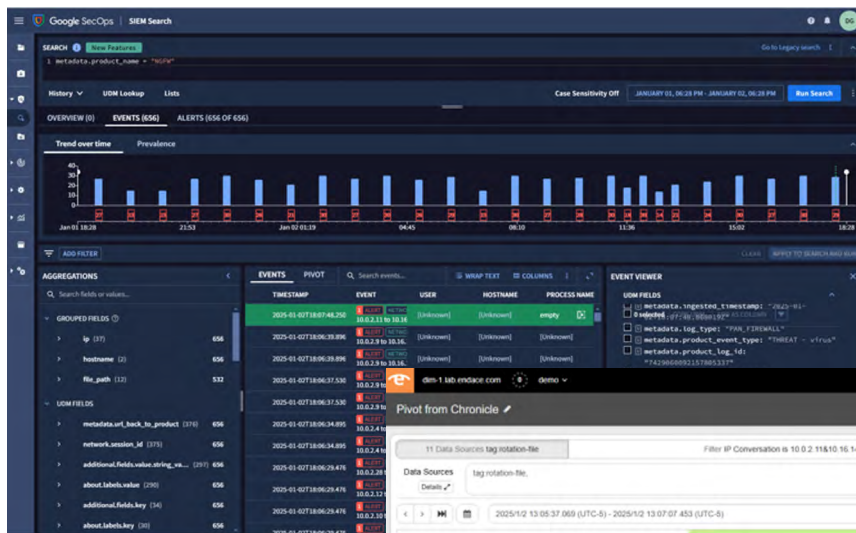
efficient investigation and resolution of network security issues.

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, Google SecOps with the EndaceProbe's 100% accurate Network History delivers next generation AI-powered security platform to detect threats with confidence and investigate with packet level network evidence at your fingertips. SecOps have the definitive evidence they need to conduct successful investigations and defend against even the most advanced threats.

## How it works

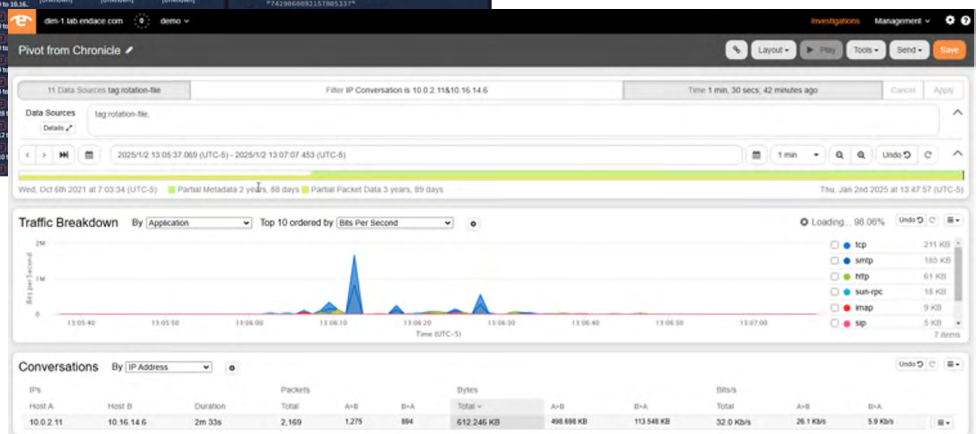


## Streamlined Investigations

- Analysts can click directly from Google SecOps alerts to view the related, recorded traffic in Endace InvestigationManager™.
- Zoom in or out on the timeline, adjust filters, and add different views to zero in on and analyze traffic-of-interest
- Decoded full packet data can be viewed directly in Wireshark™ (hosted in InvestigationManager) without downloading pcap files.

## Solution Components

- » Google SecOps
- » EndaceProbe™ Always-On Packet Capture for On-Premise 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).