SOLUTION BRIEF

Microsoft Sentinel and Endace

Accelerate Incident Response with Microsoft Sentinel Integrated with Endace Always-on Network Packet Capture

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 economically and realistically architected for is the ultimate network evidence: continuous full packet data. However, the most serious threats and issues require full packet capture evidence that exposes what's happening before, during, and after any event so analysts can confidently investigate, respond to, 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 your environments, allowing you to fully understand and respond to any threat. Simple workflow integration with your SIEM platform is crucial to helping team members quickly search for, and analyze, relevant packet data and 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.

The Solution

By combining Microsoft Sentinel 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-premise and cloud networks.

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 Microsoft Sentinel, with one-click access to definitive, full packet evidence, accelerates investigations and enables accurate event reconstruction.
- Enables compliance with mandatory data retention requirements including M-21-31, SAMA, HIPAA, PCI, etc.
- Definitive evidence trail with an accurate record of all 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 and NIAP NDcPP 2.2E compliant for security.

Microsoft Sentinel modernizes your security operations center with an intelligent, comprehensive security information and event management (SIEM) solution for proactive threat detection, investigation and response. Eliminate security infrastructure setup and maintenance and scale elastically to meet your security needs.

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

EndaceProbes continuously record 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.

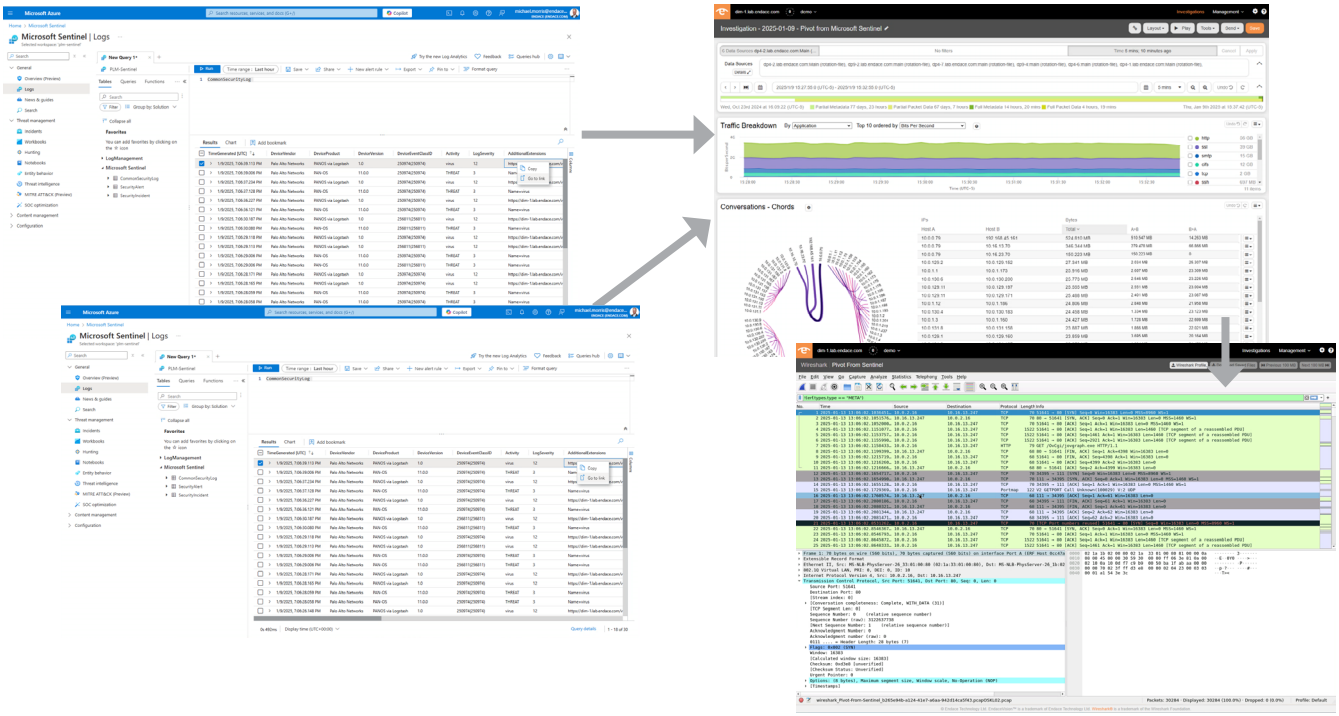
This fabric enables rapid, centralized search, data-mining and analysis of recorded traffic, and provides efficient, easy user workflows directly from Microsoft Sentinel SIEM or SOAR to provide faster, more efficient investigation and resolution of network security issues.

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 for analysis.

Conclusion

Together, Microsoft Sentinel and the EndaceProbe's 100% accurate, Always-On packet recording delivers a next generation AI-powered security platform that gives SecOps teams the definitive evidence they need to conduct successful investigations and defend against even the most advanced threats quickly and effectively.

How it works



Streamlined Investigations

- Analysts can click directly from Microsoft Sentinel alerts, log records or playbooks 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. Pcaps can also be downloaded for archival, or for further analysis using other tools.
- Watch the demo video at **endace.com/micosoft**

Solution Components

- Microsoft Sentinel
- EndaceProbe™ Always- On Packet Capture for On-Premise and Cloud environments