SOLUTION BRIEF

endace
Record. Respond.

Gain deep visibility and accelerate incident response with Elastic and Endace Always-on Full packet capture

elastic

The Problem

Security teams require rapid access to data from across the entire network, both on-prem and cloud, in order to combat the most serious threats. To detect, understand and resolve issues teams need to be able to search as much data as possible from multiple sources across the whole attack surface.

The ability to search metadata from sources across the network is crucial but metadata can only answer part of the question. Being able to pivot from relevant metadata to the full packet evidence closes the loop, letting SecOps teams understand what has happened across the network before, during and after incidents by using always-on full-packet capture, delivering forensic evidence fully integrated into the SIEM platform.

Organizations need a solution that:

- Lets them search and analyze metadata from across the entire network
- Integrates with always-on, full packet capture to ensure all evidence is available
- Can be deployed across the entire network infrastructure, both on-prem, private and public cloud
- Is flexible and can be rapidly scaled as needs change

Benefits

- Detect, investigate, and respond to evolving threats, with rapidly searchable evidence collected from across your enterprise.
- Gain greater observability down to the network layer.
- Streamline investigation workflows for your Security and Network Operations teams with one-click access to definitive packet evidence that accelerates investigation and remediation and enables accurate event reconstruction.
- Reduce threat exposure through greater analyst productivity and faster incident investigation and response.
- Consolidate hardware deployment for increased efficiency and reduced cost by leveraging EndaceProbes to deploy virtualized network monitoring tools across your environment.
- Enhance the power of Elastic metadata with comprehensive, always-on, packet data at your fingertips for faster, more conclusive incident investigation and resolution.

The Solution

By combining Elastic™ Security with Endace's Always-on, Full Packet Capture organizations can speed up threat response and incident resolution. Elastic™ Security is an open, unified platform powered by AI-driven security analytics that helps organizations protect against security threats.

Elastic collects 100% of your metadata with powerful search that extends to recorded network traffic, equipping teams to better prevent, detect, and respond to threats, at scale, quickly and confidently.

Combining the flexibility and open architecture of Elastic with the scalability and performance of the EndaceProbe's Always-on Packet Capture and EndaceFlow's high-resolution NetFlow generation gives IT, network operations and security teams the ability to see all the data all the time and know what's happening on their networks.

Integrating Elastic with the EndaceProbe™ Analytics Platform extends observability and powerful search to include weeks or months of continuously recorded network traffic, scaled across your entire enterprise. Having a complete view of all activity, including network traffic, accelerates incident response for even the toughest security threats.

EndaceProbes capture, index and store network traffic with 100% accuracy while simultaneously providing hosting for a wide variety of network security and performance monitoring applications in Application Dock™, the EndaceProbe's built-in hosting environment. Hosting EndaceFlow also enables EndaceProbes to generate high-resolution NetFlow data which can be exported to a variety of NetFlow collectors including the Elastic Stack.

Customers can extend network and security monitoring capability by deploying instances of virtual applications anywhere they have EndaceProbes deployed. Hosted tools can analyze and inspect recorded traffic in real-time, at full line-rate, or analyze recorded Network History for back-in-time investigation.

Conclusion

Together Elastic and EndaceProbe's 100% accurate, Always-on Packet Capture delivers enterprise-wide visibility and provides definitive evidence for solving even the most complex security investigations and network performance issues. Additionally, by hosting virtualized tools in the EndaceProbe's Application Dock, customers can quickly and cost-effectively extend network monitoring coverage, further improving security posture and network manageability.

How it works

Figure 1: EndaceProbes provide reliable, accurate, always-on packet capture across the network, capturing every packet.

Figure 2: Analysts working in Elastic can drill down from detected events directly to recorded packet data on EndaceProbes for fast, conclusive incident investigation and resolution.

Figure 3: In EndaceVision, analysts can inspect recorded traffic relating to the incident and apply filters and tools to analyze traffic patterns or zoom in or out on the timeline to look at precursor or post- event activity.

When they identify traffic of interest, analysts can view the decoded packet data directly using Wireshark hosted on EndaceProbe, or download pcap files for further analysis or archival.

Figure 1

Figure 2

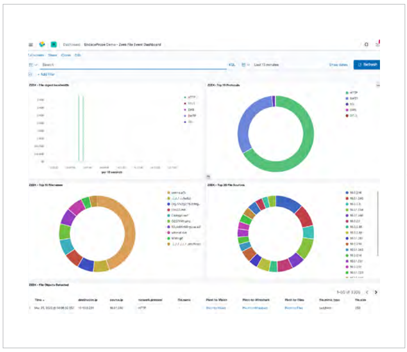
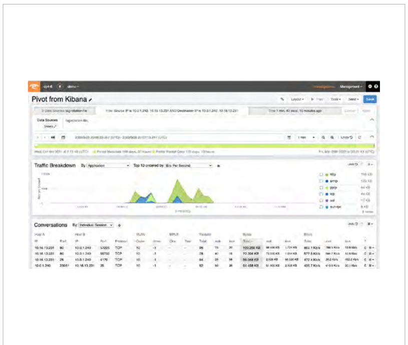


Figure3



Solution Components

- Elastic SIEM
- EndaceProbe Analytics Platform
- EndaceFlow NetFlow Generator

For more information on the Endace portfolio of products, visit: endace.com/products For further information, email: info@endace.com