Elastic and Endace

Protect against security threats with powerful search that extends to recorded network traffic

Elastic™ Security is an open, unified platform that equips teams to better prevent, detect, and respond to threats at speed and scale and secure business operations more efficiently.

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.

Combining the flexibility and open architecture of Elastic with the scalability and performance of the EndaceProbe's always-on network recording 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.

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.

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. Hosting tools like Palo Alto Networks VM Series, Cisco Firepower and Stealthwatch, or AI/ML security solutions on EndaceProbes enables customers to comprehensively monitor and record everything that happens on the network and provides the flexibility to quickly and easily scale and adapt monitoring capability as needs evolve in the future.

PRODUCTS

- Elastic SIEM
- EndaceProbe Analytics Platform with EndaceVision

BENEFITS

- Detect, investigate, and respond to evolving threats with rapidly searchable evidence collected from across your enterprise.
- Consistently deliver exceptional digital experiences with greater observability down to the network layer.
- Streamlined investigation workflows for your Security and Network Operations teams. One-click access to definitive packet evidence that accelerates investigation and remediation and enables accurate event reconstruction.
- Reduced 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.

Confidently Accelerate Investigations

Elastic collects 100% of your meta-data, giving you the ability to quickly search, slice-and-dice, analyze and interpret data to stay ahead of threat actors and performance issues.

Simultaneously EndaceProbes continually record and index network traffic, with zero packet loss, providing a complete source of forensic evidence to support fast, accurate investigations. Operations teams can leverage workflow integrations using the Pivot-To Vision™ function of the EndaceProbe API. Pivot-To-Vision lets security analysts click on events in Elastic to go directly to the relevant network traffic in EndaceVision™, the EndaceProbe's built-in investigation tool. By analyzing the related, packet-level Network History analysts can see exactly what occurred before, during, and after any security alert, and determine the appropriate remediation actions to be taken.

EndaceVision lets analysts dissect, review and extract the relevant traffic from petabytes of Network History recorded on the network.

It supports analysis to microsecond level, with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, providing rapid insights and enabling accurate conclusions.

Being able to get directly to the related packets with a single click lets security analysts rapidly establish the root cause as they investigate threats and issues. This dramatically reduces the time required to resolve critical incidents and minimizes the risk of security threats escalating to become more serious breaches.

Conclusion

Integrating the EndaceProbe's 100% accurate, always-on network recording with Elastic delivers enterprise-wide visibility and provides definitive evidence for solving even the most complex security investigations and network performance issues.

Security teams can respond to alerts faster and investigate threats with more confidence across both physical and cloud environments.

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

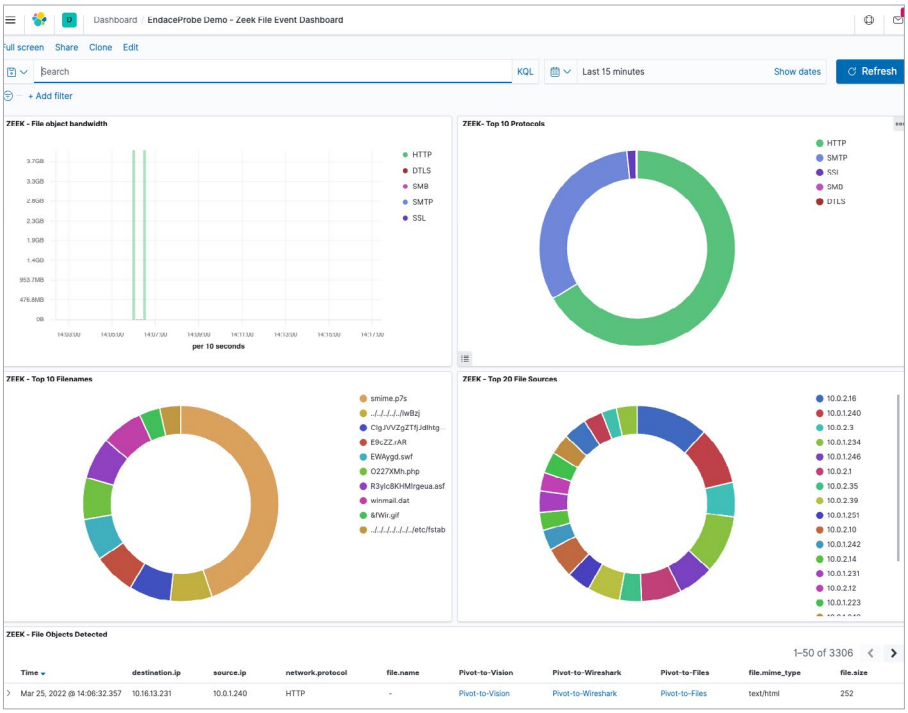

Figure 1: Analysts working from Elastic can drill-down from detected events directly to packet data for thorough investigations.

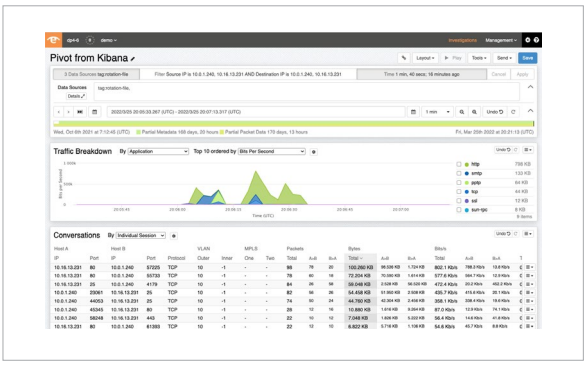

Figure 2: Related traffic can be analyzed in EndaceVision, and inspected in Wireshark™ directly on the EndaceProbe without the need to download large pcap files.

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

For further information, email: info@endace.com