LinkShadow and Endace

AI Powered Threat Detection and Absolute Network Forensics

Security analysts are overwhelmed by too many alerts and too much data, making it difficult to identify and resolve potential threats quickly before they escalate. Leveraging AI to highlight anomalous and potentially threatening activity and having a full recording of network activity enables security teams to accurately detect, investigate, assess and stop threats early in the lifecycle.

LinkShadow® CyberAI is an automated detection system which listens for threat signals. It studies the behavior of IT systems and searches for weak signals through deep machine learning by filtering gigabytes of data in real-time to proactively predict attacks. User and Entity Behavior Analytics (UEBA) analyzes the activities of employee devices connected from inside and outside the organization to identify unusual or suspicious behavior.

LinkShadow provides unparalleled detection of the most sophisticated threats which enhances an organization's defense against advanced cyber-attacks, zero-day malware and ransomware.

EndaceProbe™ Analytics Platforms capture, index and store days, weeks or months of network traffic with 100% accuracy. EndaceProbe deployments scale from small to large networks to make recorded network traffic rapidly searchable across your entire network.

Recording every packet means even the toughest security incidents or performance issues can be resolved with confidence. An open API and turnkey integrations with a wide range of third-party security solutions provide rapid access to recorded network traffic from within existing tools and workflows.

EndaceProbes can also host a wide variety of network security and performance monitoring applications in Application Dock™, the EndaceProbe's built-in hosting environment. Customers can extend their 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.

Confidently Accelerate Investigations

LinkShadow's birds-eye-view of all activities empowers defense systems with Threat Hunting intelligence for detecting and identifying an attack the second it becomes suspicious. By integrating EndaceProbe recorded network history with LinkShadow, analysts have rapid access to recorded network traffic relating specifically to suspicious activity so they can fully understand potential attacks.

With a click, analysts can drill down from LinkShadow alarms or threat indicators to related recorded network packet data. The EndaceProbe automatically zeros in on the IP address and time-range of the trigger event, focusing the analyst directly on relevant incident data. The integration workflow utilizes EndaceVision, a browser-based visual traffic analysis and forensics application included with EndaceProbes that lets analysts dissect, analyze and extract relevant traffic from the petabytes of Network History recorded on the network.

EndaceVision supports analysis with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, providing rapid insights and enabling accurate conclusions. EndaceVision can search for and analyze recorded traffic on a single EndaceProbe, or many federated EndaceProbes deployed across global networks.

Being able to get directly to the related packets lets security analysts quickly establish the root cause of issues as they are performing threat hunting in their environment. They can respond quickly to threats, dramatically reducing the time to resolve critical incidents and minimizing the risk of security threats escalating to become more serious breaches. Analysts can also quickly identify false positives to remove noise and focus activity on the threats that pose the greatest risk to the organization.

The integrated solution from Endace and LinkShadow supports the MITRE ATT&CK Cyber Kill Chain Framework to fully comprehend the threat landscape and make better use of Indicators of Compromise as part of the intelligence-driven defense.

PRODUCTS

LinkShadow

EndaceProbe Analytics Platforms

BENEFITS

- AI-driven threat hunting to overcome dynamic behavior changes and detect both known and unknown attacks.
- Enhanced SOC team productivity with automated cybersecurity analytics powered by advanced machine learning.
- Faster and more definitive incident response with 100% accurate recorded network history easily accessible from any detected anomaly.
- Detection of the most sophisticated threats with User and Entity Behavior Analytics
- Streamlined investigation workflows with rapid access to definitive packet evidence.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- Definitive evidence trail with an accurate record of all relevant packets

Conclusion

Combining LinkShadow with EndaceProbe's 100% accurate Network History delivers network wide security analytics and always-on recording for definitive evidence that enables SecOps teams to respond rapidly and confidently to even the most complex threat investigations.

Additionally, by hosting virtualized tools in the Endace Application Dock, customers can extend their monitoring coverage without additional hardware deployments, leveraging existing EndaceProbe hardware to extend their traffic monitoring and analysis capability.

How it Works

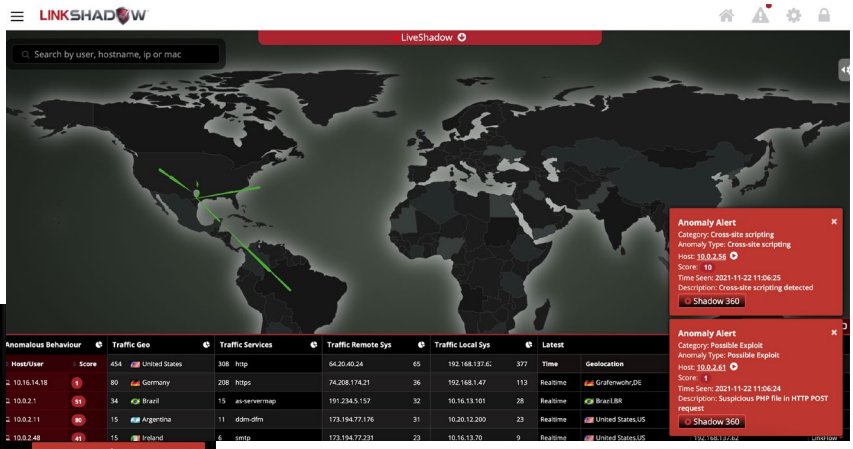
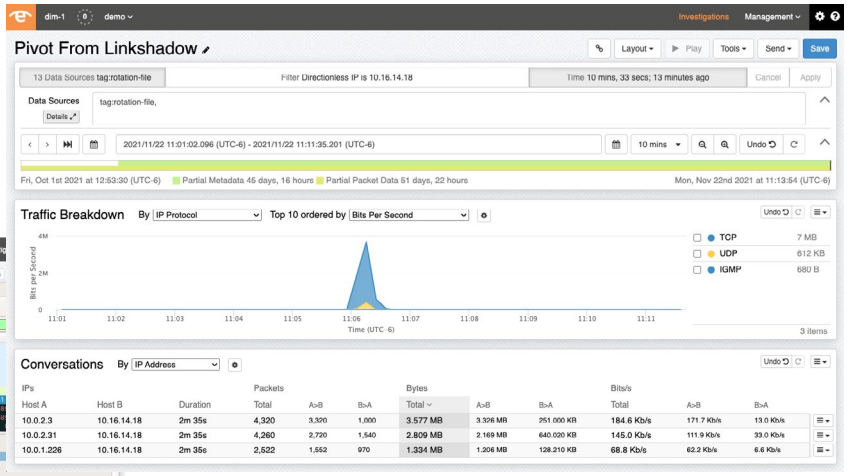
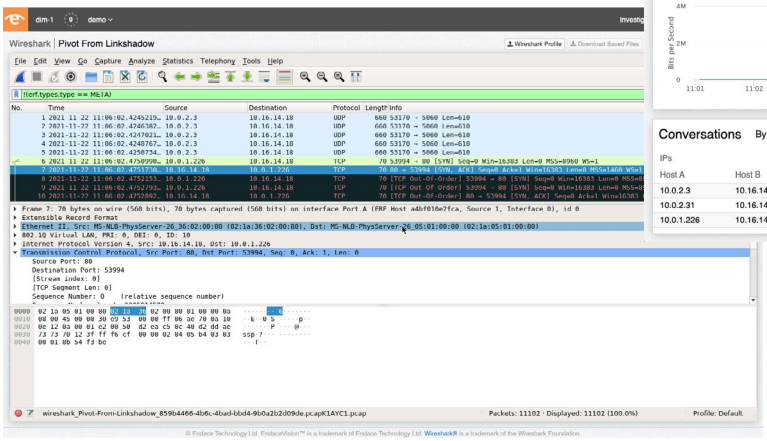


Figure 1. Drilling down from the LinkShadow dashboard to alert detail provides a Pivot-to-Vision link, Clicking on that link opens a new EndaceVision investigation focused on the related traffic recorded by EndaceProbes on the network.

Figure 2. From the EndaceVision GUI, analysts can filter traffic, zoom in or out on the timeline to view precursor or post event activity, view selected traffic using hosted Wireshark™, or download packet capture files for archival or further analysis.

In addition analysts can extract files from the traffic and generate rich analysis logs in Zeek format.





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

For further information, email: info@endace.com