Micro Focus ArcSight and Endace

Enterprise Security combined with Network History for fast, accurate incident investigation and response

When minutes matter, the combination of the EndaceProbe™ Analytics Platform and Micro Focus® ArcSight Enterprise Security Manager (ESM) dramatically reduces the time to detect, triage and respond to cybersecurity threats at scale.

ArcSight Enterprise Security Manager is a comprehensive real-time threat detection, analysis, workflow, and compliance management platform with powerful data enrichment capabilities. ArcSight detects and directs analysts to cybersecurity threats, in real time, helping security operations teams respond quickly to indicators of compromise.

By automatically identifying and prioritizing threats, ESM helps security teams avoid the cost, complexity and extra work associated with dealing with false positives. It gives organizations a powerful, centralized view into their multiple environments enabling workflow efficiency and streamlined investigation processes. The improved detection, real-time correlation, and workflow automation that ESM provides enables security teams to resolve incidents quickly and accurately.

Deployed together, Micro Focus ArcSight and EndaceProbes help security analysts rapidly investigate issues presented in ArcSight with in-context drill down to full packet data that enables them to confidently and accurately investigate any network issue or security threat.

EndaceProbe Analytics Platforms capture, index and store network traffic with 100% accuracy while simultaneously hosting a wide variety of network security and performance monitoring applications in Application Dock™, the EndaceProbe's built-in hosting environment. Hosted applications can analyze recorded traffic in real-time at full line-rate or analyze recorded Network History for back-in-time investigation.

Always-on network recording provides your SIEM environment with the detailed, packet-level forensic evidence that allows analysts to understand the full impact of any security threat, whether any external systems were contacted and what, if any, data may have been exfiltrated. Analysts no longer have to guess what might have been impacted because they have the network evidence to remediate, respond and report accurately to any threat.

Efficient Threat Hunting and Investigation

The Network History recorded by EndaceProbes can be integrated into workflows from ArcSight Enterprise Security Manager using the Pivot-To Vision™ function of the EndaceProbe's powerful API.

Pivot-To-Vision lets security analysts pivot from threat alerts in Enterprise Security Manager directly to EndaceVision™, the EndaceProbe's built-in investigation tool to analyze the related, packet-level Network History. Using the IP address and time range of the trigger event, Pivot-To-Vision focuses the analyst directly on pre-filtered incident data.

PRODUCTS

- Micro Focus ArcSight Enterprise Security Manager
- EndaceProbe Analytics Platform

BENEFITS

- Intelligent and powerful correlation of up to 100,000 events per second.
- Eliminate ineffective, security operations "swivel-chair" workflows by unifying and centralizing management, analysis, and reporting of all enterprise security events
- Rapid, conclusive and actionable investigations with drill-down to packet-level detail.
- Reduced threat exposure through greater analyst productivity and faster, more accurate incident investigation.
- Definitive evidence trail with an accurate record of all relevant packets.

EndaceVision lets analysts dissect, review and extract the relevant traffic from the terabytes of Network History recorded on the network. It enables analysis to microsecond level with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, allowing rapid insights and accurate conclusions.

Being able to get directly to the related packets with a single click lets security analysts rapidly establish the root cause of issues as they are responding to threat alerts or conducting threat hunting activity in their environment. They can respond quickly, dramatically reducing the time resolve critical incidents and minimizing the risk of security threats escalating to become more serious breaches.

Conclusion

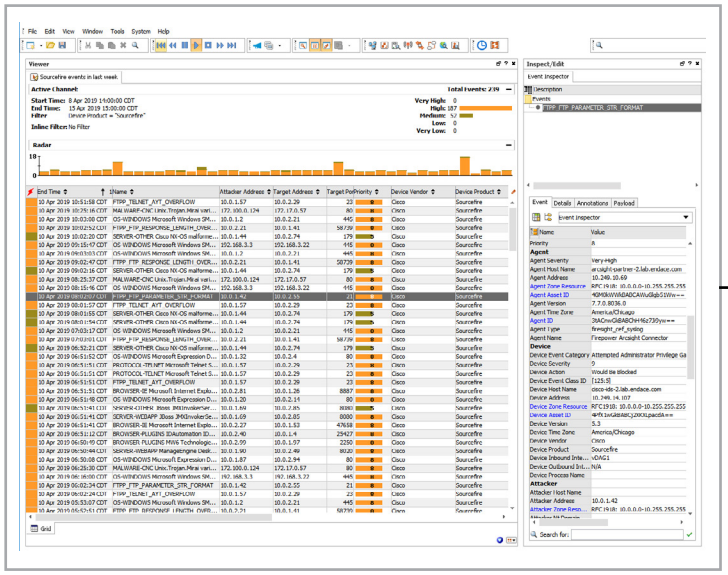
Combining ArcSight Enterprise Security Manager with EndaceProbes delivers leading Enterprise Security management that allows organizations to detect and respond to cyberthreats in real time across the entire IT infrastructure.

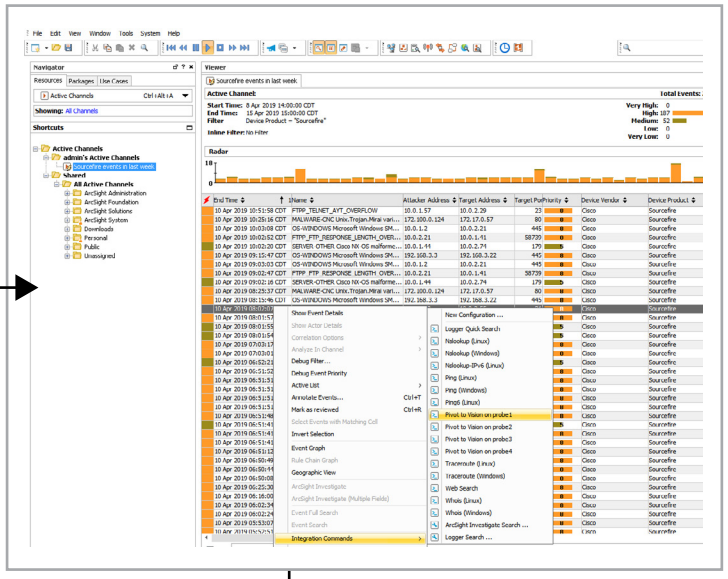
The combined Endace and Micro Focus solution delivers security insights from the endpoint to the datacenter and across the entire network. It gives your security analysts the capability they need to identify, investigate and remediate threats quickly, reducing threat exposure and accelerating incident response.

Integrating the two technologies gives security analysts the definitive evidence and rich context they need to understand the scope and impact of every threat and remediate attacks quickly, accurate and effectively.

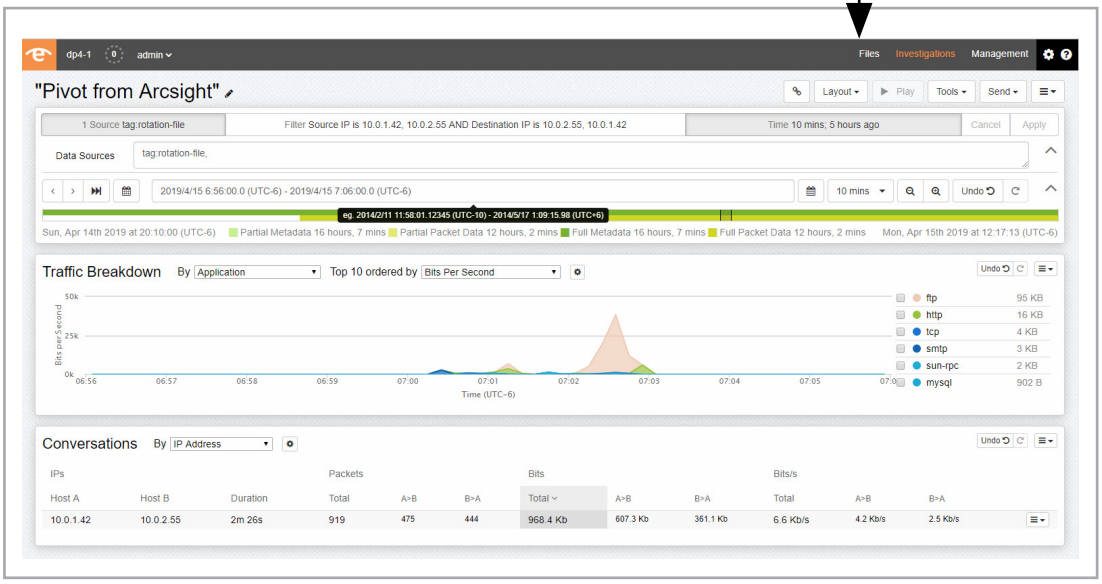
END_sb_Microfocus-1.0_0619

How it works





Pivot directly from an alert in Arcsight ESM to view related traffic in EndaceVision. Filters are pre-set to retrieve the traffic relating to that alert.



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

For further information, email: info@endace.com