Kemp Flowmon and Endace

Flowmon
A Kemp Company

Deep Network Visibility for Security, Network and Application Teams

Security, Network and Application Operations teams share a common goal - a secure, reliable, high-performance network.

Combining Kemp Flowmon with the EndaceProbe™ Analytics Platform provides powerful network wide traffic monitoring and analysis with definitive packet-level forensic evidence that gives teams the data they need to analyze and resolve even the most complex security and performance issues quickly and accurately.

Kemp Flowmon collects and processes network telemetry data, including IP flows and raw packets, from a variety of sources and analyzes it for relevant information, enriching the flow data with additional insight. Using machine learning, heuristics and advanced analytics, it improves network performance, alerts on incidents and enables early threat response. The data is stored and analyzed, and the resulting insights are displayed in an integrated console.

EndaceProbe™ Analytics Platforms capture, index and store a 100% accurate packet-level record of network activity regardless of network speeds, loads or traffic types. Integration with a wide range of security and performance monitoring tools enables analysts to drill-down from alerts in these tools directly to related packet history with a single click, giving analysts rapid, on-demand access to detailed forensic evidence.

The EndaceProbe's Application Dock™ hosting environment extends security and performance monitoring by allowing third party analytics applications – including Kemp Flowmon Probes - to be hosted on the open EndaceProbe platform, giving them access to both real-time and historical packet data.

PRODUCTS

Kemp Flowmon Collector

Kemp Flowmon Probe

Kemp Flowmon Anomaly Detection System (ADS)

EndaceProbe Analytics Platform

BENEFITS

- Robust, network-wide monitoring and diagnostics from cloud to on-premises for security, network operations and applications teams.
- Monitor and troubleshoot security, end-user experience, network, application and cloud/SaaS performance. Accurately forecast and plan for efficient resource utilization, infrastructure design and deployment.
- Remove the silos between SecOps, NetOps and DevOps teams with shared access to a common source of reliable data about network activity.
- Powerful security analytics tools for rapid threat detection, prevention, investigation and remediation
- Streamlined investigation workflows from Kemp Flowmon Monitoring Center and ADS giving analysts one-click access to definitive packet evidence for accelerated event investigation and accurate reconstruction of historical events.
- Host virtual Kemp Flowmon Sensors on EndaceProbe for flexible, cost-effective deployment to extend visibility across the network
- Maintain a definitive history of network activity with weeks or months of detailed full packet history for forensic investigations.

Rich, Contextual Evidence for Accurate Detection, Investigation and Response

Kemp Flowmon Collector is the component responsible for capturing, storing and analyzing flow data. The collected and analyzed network and application telemetry is displayed on a highly customizable centralized dashboard, which provides detailed statistical reporting, powerful visualization tools and drill-down for effective investigation, troubleshooting and capacity planning.

Kemp Flowmon Collector's functionality can be extended via add-on software modules that provide a range of advanced functions for security operations - such as Kemp Flowmon ADS (Anomaly Detection System) for network behavior analysis, unknown threat detection and encrypted traffic analysis - enabling SecOps teams to accelerate threat detection, investigation and response.

Kemp Flowmon ADS is a security solution that uses machine learning to detect anomalies hidden in network traffic. It complements conventional security tools and creates a multi-layered protection system capable of uncovering threats at every stage of compromise.

An optional, dedicated sensor - Kemp Flowmon Probe - provides detailed Layer 7 application information, such as hostnames, URLs, browser information and other fields, for protocols including DNS, DHCP, SQL, SMTP, and Samba/CIFS, delivering powerful contextual insight for security, network and application teams. Kemp Flowmon Probe can be deployed as either a physical appliance or a virtual appliance to provide monitoring across a wide range of cloud environments.

Kemp Flowmon's enriched data can be forwarded to other systems - such as SIEM or SOAR tools - or collected by Kemp Flowmon Collector for reporting on, and analyzing, critical security threats and performance issues.

Customers can extend their network and security monitoring capability by deploying instances of Kemp Flowmon Probes onto any EndaceProbe without rolling out additional hardware.

END_fp_kemp_flowmon_1.0_082101

Streamlined Workflows Accelerate Response

The Pivot-To Vision™ function of the EndaceProbe API enables powerful integration between Kemp Flowmon ADS and EndaceProbes. Analysts can drill down from alerts and threat indicators directly to related packet data in EndaceVision, the EndaceProbe's built-in traffic analysis tool.

Using the IP address and time range of the trigger event, EndaceVision focuses the analyst directly on the packets relating to the incident, letting them dissect, review and extract the relevant traffic from amongst the petabytes of Network History recorded by EndaceProbes on the network. It enables analysis to microsecond level detail with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, enabling rapid insights and accurate conclusions.

Analysts can quickly zoom in or out on the timeline in EndaceVision to look at precursor or post-event activity, allowing them to easily identify and analyze related traffic - for example, evidence of command-and-control, lateral movement, malware or data exfiltration during a security investigation.

Once traffic of interest is identified, the detailed packet data can be decoded and examined using Wireshark™ (hosted on all EndaceProbes), without the need to download large pcap files to a local host. Or it can be replayed to other analytics tools for deeper analysis.

Conclusion

The combination of rich flow data delivered by Kemp Flowmon solution, and the full packet history provided by EndaceProbes, gives SecOps, NetOps and Application teams the definitive evidence they need to detect, investigate and respond to security, network or application challenges quickly and confidently.

The ability to deploy and host Kemp Flowmon Probes on the EndaceProbe platform allows customers to seamlessly extend network visibility and monitoring quickly and easily as the network grows and needs change.

How it works

Figure 1: Kemp Flowmon Probe hosted in EndaceProbe Application Dock generates rich NetFlow and meta-data. This is collected by Kemp Flowmon Collector and can be analyzed in Kemp Flowmon ADS or sent to SIEM or SOAR tools.

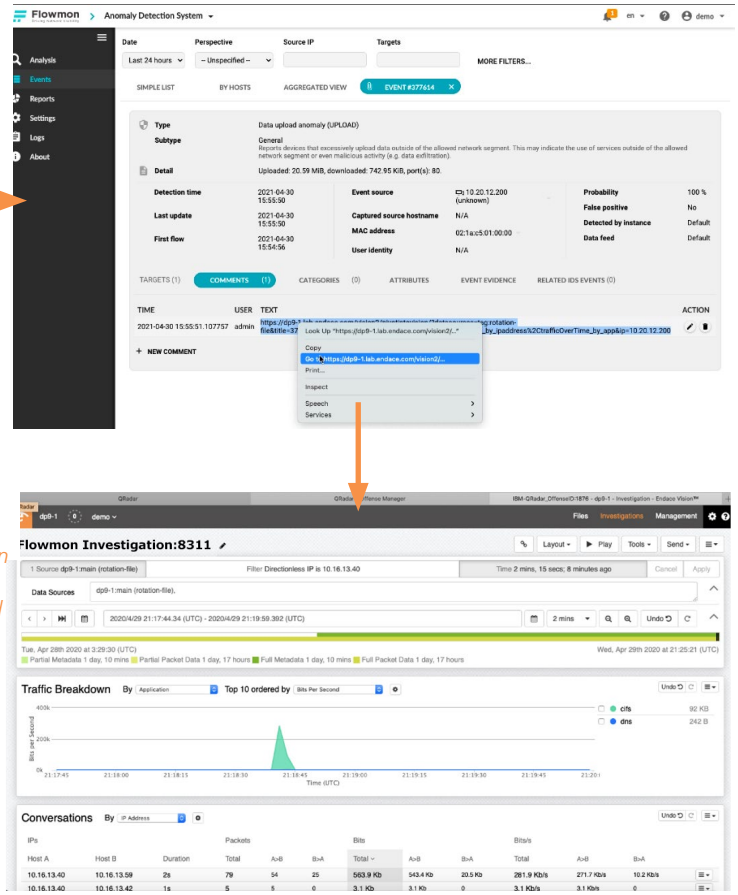

Figure 2: Analysts working in Kemp Flowmon ADS (or third-party SIEM or SOAR tools) can drill down directly from events to the related packet history for detailed forensic analysis.

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

For further information, email: info@endace.com

END_fp_kemp_flowmon_1.0_082101