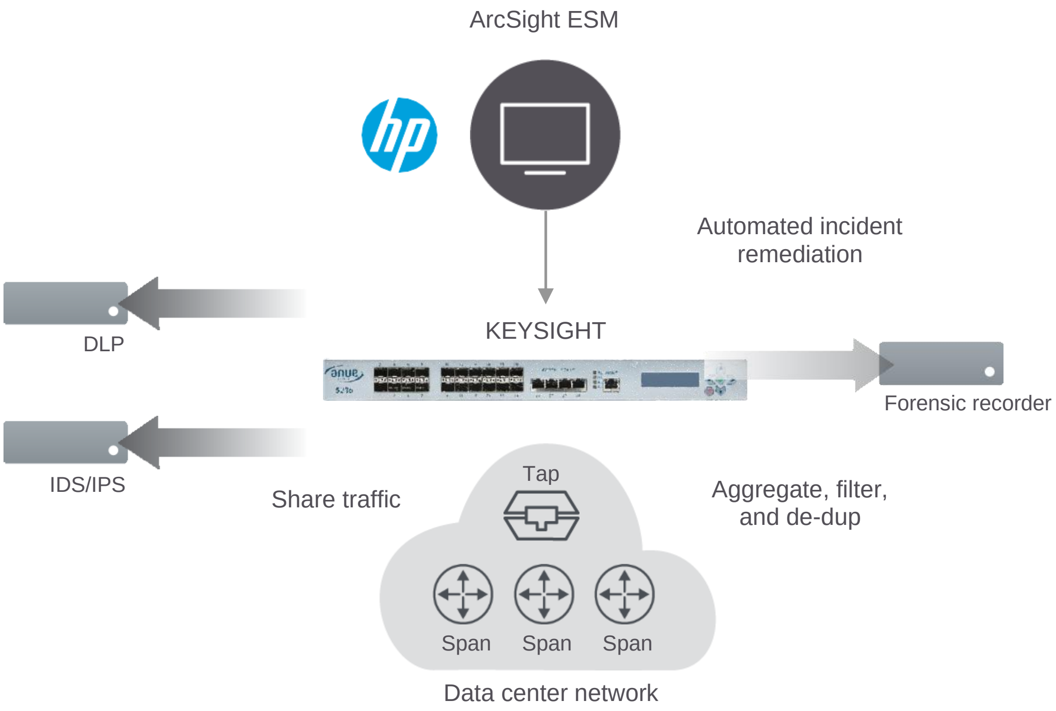
SOLUTION BRIEF

Automatically Trigger Packet Capture from HP ArcSight to Accelerate Incident Remediation

The Keysight Network Visibility Solutions automates packet capture to speed root cause analysis

Highlights

Security appliances are only as useful as the data they receive. The integrated Keysight network visibility and HP ArcSight solution sends the right traffic to the right security tool at the right time. By automating out-of-band monitoring traffic flow based on the alerting and correlation capabilities of ArcSight, issues can be resolved before they become a problem.



Solution

Keysight's network visibility solutions work in concert with HP ArcSight's Security Information and Event Management (SIEM) system and your security tools (forensic recorders, IPS/IDS, DLP and malware analyzers) to protect your network.

Keysight's network visibility solutions passively direct out-of-band network traffic from multiple access points (SPANs or taps) in the network to security tools for analysis. Traffic is aggregated from all needed access points in the network to provide comprehensive visibility.

Keysight's network visibility solution Automated Response Technology complements the ArcSight Enterprise Security Manager (ESM) product's ability to detect, analyze and respond to security threats. When the ArcSight ESM detects an anomaly, Keysight can automatically, or via a right mouse click from ESM, send the right traffic to a forensic recorder or other security probe. Incident remediation can begin the instant an anomaly occurs with the benefit of having all the required packet information. The joint solution speeds root cause analysis, eliminates time consuming manual steps and simplifies compliance.

Joint Solution Benefits

- Accelerate root cause analysis by capturing the required packets
- Simplify compliance reporting
- Provide security tools the right data at the right time from anywhere in the network
- Eliminate time consuming and error prone manual steps
- Compatible with any security tool – forensic recorder, IDS/IPS, DLP, or malware analyzer
- Easy to use from ArcSight ESM using a right mouse click or alert triggers
- HP Certified Keysight Action Connector available free for easy install

Keysight Network Visibility Solutions Efficiently Direct Traffic to Security and Application Monitoring Tools

Keysight network visibility solutions provide security and monitoring tools access to all necessary network traffic. Keysight sits between the access points in the network that require monitoring and security appliances. Simultaneously, Keysight aggregates traffic from multiple SPANs/taps in the network and directs it to any security or monitoring appliance. This approach provides efficient access to asymmetric traffic across large heterogeneous networks. Keysight also removes traffic, which does not need analysis, prior to consuming resources on monitoring appliances.

Keysight's network visibility solutions share traffic from a network access point with multiple monitoring tools. This capability eliminates the common SPAN/tap shortages that occur when another tool is attached to a needed access point. Additionally, by removing duplicate packets, Keysight can enhance the throughput and storage capacity of the any security appliance or forensic recorder.

Keysight's intuitive control panel makes the nework visibility solution easy to set up and use. Simply drag- and-drop a virtual connection between SPANs/taps and tools to make a live connection.

Understand The Who, What and Where Behind Every Risk

HP ArcSight ESM is the brain of the ArcSight SIEM platform. It analyzes and correlates every event that occurs across the organization – every login, logoff, file access, database query, etc. – to deliver accurate prioritization of security risks and compliance violations. The powerful correlation engine of ArcSight ESM sifts through millions of log records to find the critical incidents that matter. These incidents are then presented through real-time dashboards, notifications or reports to the security administrator. Once threats and risks are identified, ArcSight ESM uses its built-in workflow engine to manage incidents and prevent damage.

Automated Response Technology

Keysight's network visibility solution Automated Response Technology allows users to efficiently monitor more of their network without requiring additional staff or budget. Automation can adjust your monitoring configuration proactively in response to changes in the network. The integrated Keysight and HP ArcSight solution uses the technology to automatically send the right traffic to the right security tool at the right time based on triggers from SIEM security alerts.

Common automation applications include:

- Redirect suspicious traffic to specific monitoring tools for analysis
- Activate unused tools to distribute network monitoring bandwidth more effectively
- Configure ArcSight SIEM or network management systems (NMS) to trigger the Keysight NVS to automatically capture packets related to specified events

Once automation is configured on Keysight's network visibility solutions and HP ArcSight, you will have "always on" visibility into your dynamic network. So the next time network traffic spikes at 3:00AM, you can relax knowing that Keysight and HP will take care of the early troubleshooting tactics for you.

About HP

HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. With the broadest technology portfolio spanning printing, personal systems, software, services and IT infrastructure, HP delivers solutions for customers' most complex challenges in every region of the world. More information about HP (NYSE: HPQ) is available at http://www.hp.com

About Keysight

Keysight provides testing, visibility, and security solutions, strengthening physical and virtual network elements for enterprises, governments, service providers, and network equipment manufacturers.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications, or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT
TECHNOLOGIES