Palo Alto Networks and Endace

Prevent, detect and respond to even the most challenging cyber threats.

Next generation security and 100% accurate network packet recording combine to accelerate response to security events and reduce threat exposure.

Palo Alto Networks Next-Generation Firewalls safely enable all applications and deliver highly automated, preventive protection against cyber threats at all stages in the attack lifecycle without compromising performance.

Panorama™ network security management lets you view all firewall traffic, manage device configuration, push global policies, and generate reports on patterns or incidents—all from one central location.

EndaceProbe™ Network Recorders capture, index and store network traffic with 100% accuracy, regardless of network speeds, loads or traffic types. Application Dock™ extends security and performance monitoring by allowing third party analytics applications to be hosted on the open EndaceProbe platform.

Streamlining Security Investigations

The Network History recorded by EndaceProbes can be integrated with Palo Alto Networks' security platform using the Pivot-To-Vision™ function of the EndaceProbe's powerful API.

Pivot-To-Vision lets security analysts pivot directly from Palo Alto Networks threat logs 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, Pivot-To-Vision focuses the analyst directly on pre-filtered incident data. EndaceVision lets analysts dissect and review terabytes of network history down 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 lets security analysts quickly and conclusively establish the root cause of issues and respond appropriately, dramatically reducing the time to investigate and resolve critical incidents.

PRODUCTS

- Palo Alto Networks Next-Generation Firewalls
- Palo Alto Networks Panorama Management
- EndaceProbe Network Recorders
- Endace Application Dock

BENEFITS

- Safely enable applications and protect against threats with Palo Alto Networks Next-Generation Firewalls.
- Expand security coverage by deploying Palo Alto Networks VM-Series Firewalls on the EndaceProbe open platform.
- View all traffic and quickly spot incidents from one central location with Panorama.
- Respond to and remediate incidents quickly and efficiently with streamlined investigation workflows.
- Rapid, conclusive and actionable investigations with drill down to packet level detail.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- Definitive evidence trail with an accurate record of all relevant packets.
- Reduced false positives through improved detection tuning.

Increasing Detection Visibility with Application Dock

Palo Alto Networks VM-Series Firewall for KVM can be hosted in IDS mode on the EndaceProbe in Application Dock. Every packet captured and recorded by the EndaceProbe can also be streamed to Palo Alto Networks VM-Series Firewall in real-time.

Security Operations teams can dynamically deploy Palo Alto Networks VM-Series Firewall anywhere on the network that they have EndaceProbe Network Recorders deployed, allowing them to increase their detection footprint without truck rolls or lengthy hardware deployments.

EndaceProbes are designed to ensure system resources used for capture and recording are separated from the resources used by hosted applications.

This means capture performance is never impacted by hosted applications and vice-versa, guaranteeing 100% accurate recording even when the hosted Palo Alto Networks VM-Series Firewall instance is processing heavy traffic loads.

Conclusion

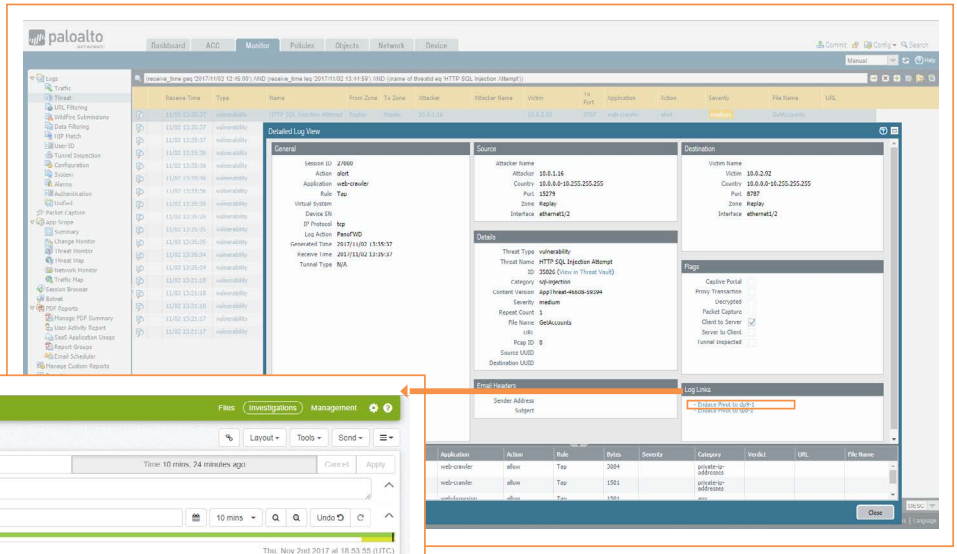
Palo Alto Networks Next-Generation Security Platform combined with the Network History recorded by EndaceProbes delivers comprehensive security and deep contextual insight for rapid investigation and response.

Integrating the two technologies lets security analysts respond to security threats with much greater speed and accuracy.

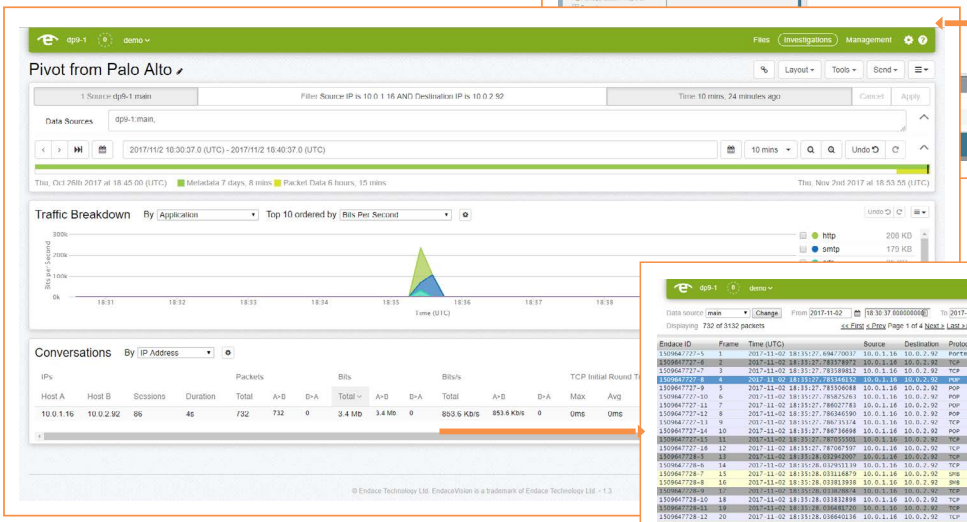
And, by hosting Palo Alto Networks VM-Series Firewall in Application Dock, security teams can extend their reach without truck rolls, leveraging existing EndaceProbe hardware deployments to extend their security monitoring and network recording capability.

The combined Endace and Palo Alto Networks solution provides improved security posture, reduces threat exposure and accelerates incident response with definitive evidence.

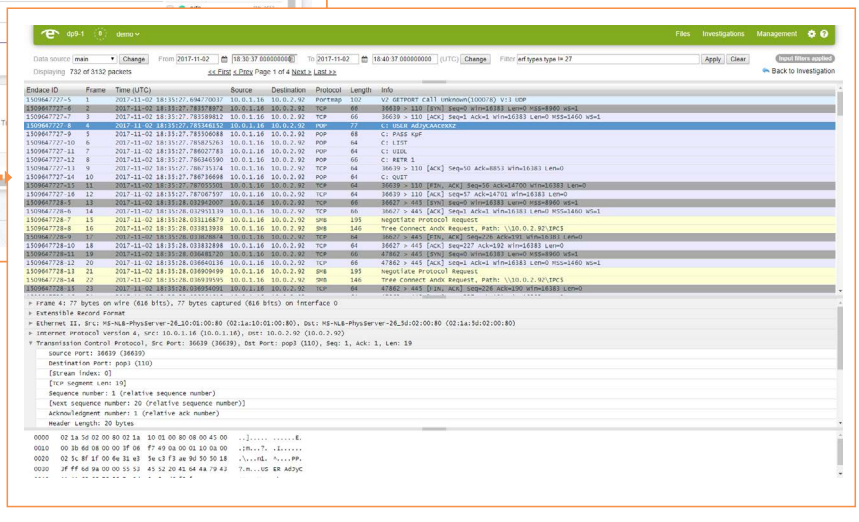
1. Pivot directly from a loglink to view related traffic in EndaceVision. Filters are pre-set to focus directly on related packets.



2. Examine related traffic in EndaceVision using built-in visualization tools



3. View packets directly in EndacePackets (or download as a capture file)



Contact sales@endace.com to arrange a demonstration of the power of integrating EndaceProbe Network Recorders, Palo Alto Networks Firewalls and Panorama Security Management