Palo Alto Networks and Endace

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

The cost of security breaches can be astronomical, causing lost customers, severe brand damage, costly legal action and potentially wiping millions off a company's valuation. Which makes rapid, accurate incident response and root cause analysis a critical business imperative. By combining next-generation security and 100% accurate network packet recording, teams can reduce threat exposure by detecting and remediating security events quickly and accurately to protect critical assets.

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™ Analytics Platforms 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 provides the critical evidence needed for fast and accurate investigations. Palo Alto Networks Next-Generation Firewalls and Panorama are easily integrated with Network History 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.

Increasing Detection Visibility with Application Dock

Deploying next-generation security hardware takes significant planning and effort. New rollouts can often take 6 months or more to acquire and deploy new hardware. This puts security teams at a disadvantage when trying to defend against criminals who can launch attacks at the click of a mouse.

Endace and Palo Alto Networks bring a new-found agility to deploying next-generation security across your network. Security Operations teams can dynamically deploy VM-Series Firewalls 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.

The 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 VM-Series Firewalls in real-time. 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 VM-Series Firewall instance is processing heavy traffic loads.

PRODUCTS

Palo Alto Networks Next-Generation Firewall
Palo Alto Networks Panorama
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.

END_fp_end_palo_alto_3.1_0420

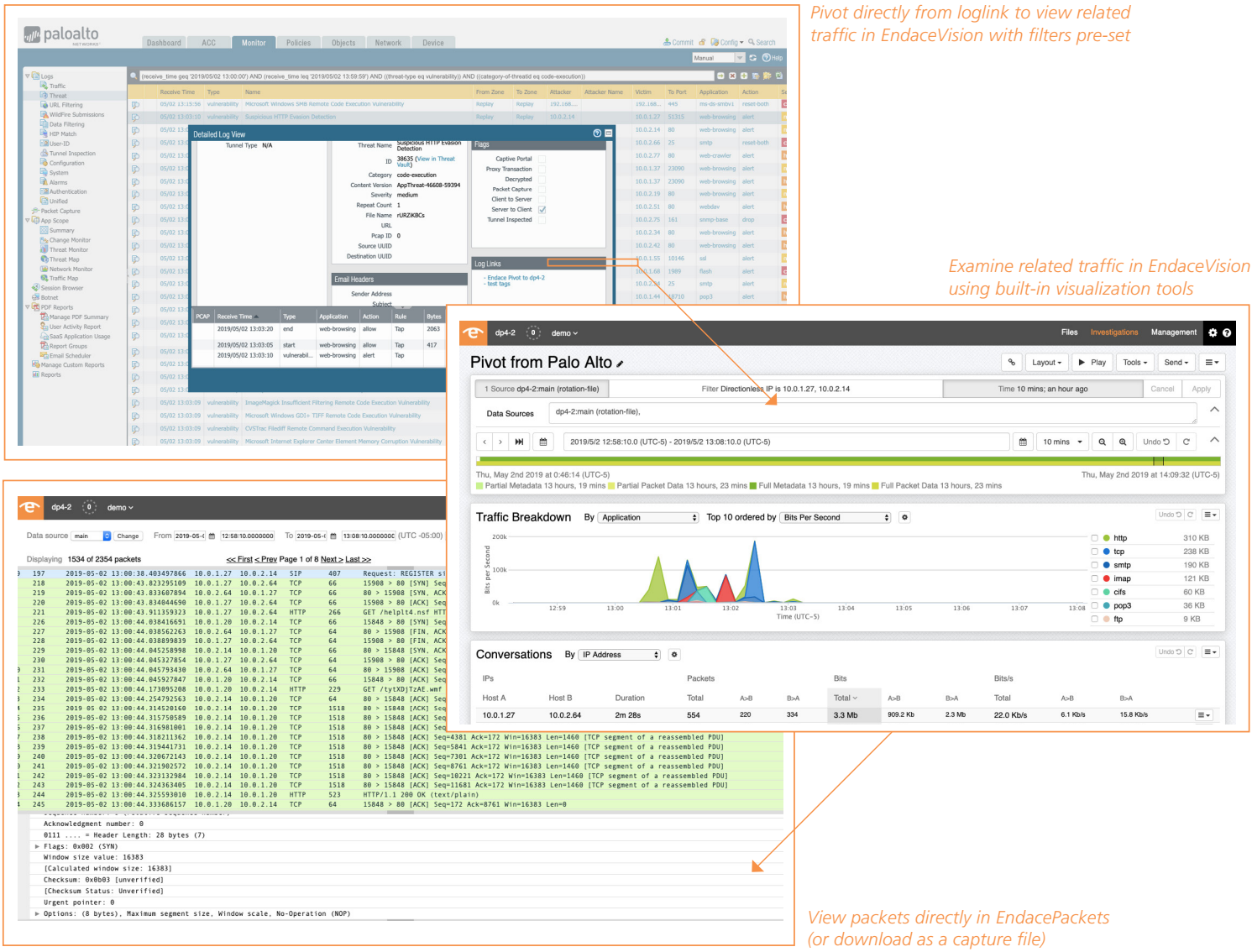
Conclusion

Palo Alto Networks' Next-Generation Firewalls and Panorama 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.

How it Works



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

For further information, email: info@endace.com