Scalable Network Monitoring with Endace and Ixia

ixia
A Keysight Business

PRODUCTS

Ixia Vision Network Packet Brokers

EndaceProbe Analytics Platforms

BENEFITS

- Full network visibility – all required traffic from anywhere in the network, with no dropped packets.
- A 100% accurate source of definitive Network History that provides a single source of truth for SecOps, NetOps and DevOps teams.
- Integrated with your network security and performance monitoring tools for fast, accurate issue detection, investigation and resolution.
- Detect and remediate threats hiding inside encrypted SSL and TLS sessions including TLS 1.3.
- Respond to new and emerging threats with agile and ad hoc changes to monitoring topology.
- Host security or performance analytics tools on EndaceProbes simplify and accelerate deployment of analytics functions and extend network coverage.
- Easily add 1GbE, 10GbE, 40GbE or 100GbE ports to meet changing bandwidth requirements.

Ixia Visibility Solutions provide real-time, end-to-end visibility into physical, virtual, and cloud deployments, delivering control, coverage and performance to seamlessly protect and optimize crucial networking, data center and cloud business assets.

IT teams around the world use EndaceProbe Analytics Platforms™ to accurately record Network History and troubleshoot and diagnose network performance issues, application issues and security threats and breaches.

EndaceProbes also allow customers to host best-of-breed analytics and security software from our Fusion Partners, as well as open source and custom developed solutions, providing a powerful platform for deploying and hosting a wide range of security and performance analytics solutions.

Combining Ixia's Vision Portfolio with EndaceProbes

Together, EndaceProbes and Ixia's Vision portfolio of Network Packet Brokers (NPBs) give network and security teams visibility into encrypted and unencrypted traffic traversing all segments of the network. This allows teams to detect and investigate threats hiding inside encrypted packets, filter and steer traffic to make best use of their precious tool resources and efficiently deploy new security analytics solutions so they can respond to new and emerging threats.

The combination of Ixia's zero packet-loss, hardware-accelerated architecture and the EndaceProbe platform's 100% packet capture, recording and analytics hosting ensure that you never miss a packet.

Respond Rapidly to New and Emerging Threats

New and emerging threats don't wait for change windows, hardware installs, truck rolls or CAPEX approvals. With an architecture built around EndaceProbes and Ixia's Vision series NPBs, security and performance teams are armed with an agile and powerful platform for responding to threats and resolving issues.

Known for their easy-to-use web interface, Ixia's packet brokers do the heavy lifting when it comes to managing filter rules, making it easy to manage changes and freeing up valuable time to focus on other things. Changes to rules and monitoring points can be made on the fly at any time of the day without impacting other traffic.

EndaceProbes are the industry's only, truly open, packet capture platform. They enable both hosting of, and integration with, commercial analytics solutions from our market-leading Fusion Partners including Cisco, Palo Alto Networks, BluVector, Dynatrace, Splunk and Plixer as well as open-source tools such as SNORT, Bro IDS, Suricata and Argus or custom-developed applications.

Hosted applications can access live network traffic at line rate or use Playback™ to analyze recorded Network History, allowing real-time tools to be used for both real-time and back-in-time analysis. Deploying a new security tool to investigate suspicious traffic in your network becomes as simple as deploying a new VM to an EndaceProbe and dragging and dropping a monitoring connection in the Ixia Vision GUI.

Integrating the EndaceProbe's recorded Network History into analytics solutions enables fast, accurate investigation of security threats and performance issues: SecOps, NetOps and DevOps analysts can click on an alert to go directly to the related packets and see, definitively, what took place.

The Anatomy of an EndaceProbe Analytics Platform

EndaceProbe's capture, index and store network traffic with 100% accuracy, regardless of network speeds, loads or traffic types. They provide definitive evidence, and a single source of truth, that can be shared by SecOps, DevOps and NetOps teams.

With centralized management and datamining, EndaceProbes can be connected to form a network-wide, recording and analytics hosting fabric – an EndaceFabric. Built-in investigation tools, EndaceVision and EndacePackets, allow analysts to quickly find, retrieve and analyze packets-of-interest wherever on the network they may have been recorded.

The EndaceProbe's hosting capability allows teams to deploy the applications they want, when they want, without the hassle and expense of a hardware rollout. This frees them up from long, costly, CAPEX cycles and lets them deploy applications proactively and keep up-to-date with the latest threats and network issues.

EndaceProbes allow:

- SecOps teams to identify, investigate and quantify security events and data breaches.

- NetOps and applications teams to diagnose network and application performance issues quickly to identify the root cause and remediate the problem.
- Risk and compliance teams to comply with strict data retention policies.
- All teams to perform comprehensive, back-in-time investigations with Playback™, drilling down to packet level to see what's really happening on your network.
- Integration with existing network security and performance analytics tools to streamline and automate investigations with one-click from the security alert to the related packets.

Optimizing Access to Monitoring Data

Ixia Vision portfolio of Network Packet Brokers (NPBs) aggregate and direct traffic from all necessary access points including physical and virtual (vTaps) or SPAN ports to ensure comprehensive and efficient visibility.

This includes:

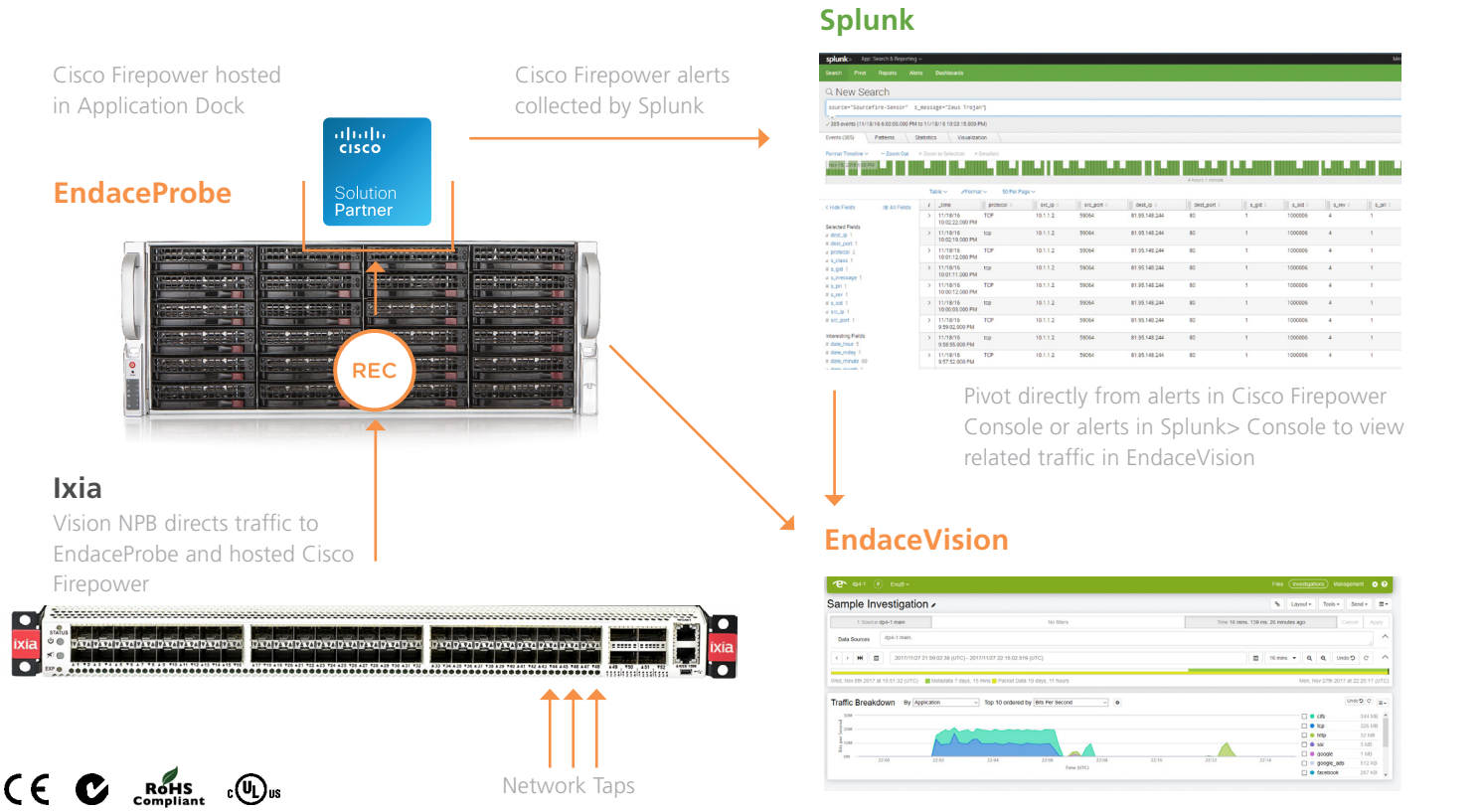
- Decrypting SSL and TLS traffic to record and detect threats that could be hidden inside encrypted sessions, including Diffie Helman Ephemeral (DHE) extensions for perfect forward secrecy (PFS) as specified in TLS 1.3.
- Removing duplicate packets by filtering out unneeded traffic to optimize use of resources, throughput and storage capacity.
- Eliminating SPAN/tap shortages that occur when additional tools are attached to access points by allowing traffic from a single network access point to be shared with multiple monitoring tools.
- Load-balancing across all of your EndaceProbes for greater capacity and scalability
- Simple drag-and-drop setup and operation through Ixia's easy-to-use graphical user interface (GUI).
- Eliminating VM-to-VM, East-West traffic blind spots.

Conclusion

Ixia Vision Network Packet Brokers and EndaceProbe Analytics Platforms work seamlessly to provide a dynamic and 100% accurate network visibility and security platform that integrates with a rich ecosystem of other tools and capabilities.

The combined solution empowers security and operations teams to hunt for threats, defend critical assets and ensure network and application reliability using the best available tools. It enables the agility they need to respond to today's challenging, and continually evolving, environment.

Deployment Example: Agile IDS and SIEM with Integrated Workflow



RoHS Compliant

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission [FCC] Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction document, may cause harmful interference to radio communications.Endace™, the Endace logo and DAG™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).

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

For further information, email: info@endace.com