

EndaceProbe vProbe



The EndaceProbe™ vProbe is a virtual machine implementation of the EndaceProbe Analytics Platform. It's designed to record crucial network history in private cloud environments and provide visibility into virtual network traffic, including East-West traffic. Network history is critical when tracking down security events or performance issues. vProbes are an ideal complement to physical EndaceProbes as common components of a Network-Wide EndaceFabric™.

The vProbe collects and records network traffic by tapping virtual switches or by collecting packets from a dedicated host Network Interface Card.

Like physical EndaceProbes and other EndaceFabric elements, vProbes can be centrally monitored and managed using EndaceCMS™ Central Management Server and the Network History they record can be centrally mined and searched.

The vProbe is ideal for monitoring the performance of, and diagnosing problems with, virtualized applications, providing visibility into difficult-to-see, East-West traffic from within the virtual infrastructure without requiring physical appliances.

REC

Recording in Virtualized Datacenters

- Increased visibility across virtualized environments
- Monitor the performance of virtualized applications. And diagnose problems with accurate evidence.



Built-In Investigation Tools

- Analyze Network history with EndaceVision™, a powerful, browser-based traffic analysis tool
- Decode packets without download using hosted Wireshark™
- Analyze to millisecond level with MicroVision
- Application classification for 1200+ applications.
- Mine network history, extract and download packet capture files for manual analysis.
- Built-in file extraction and deep analysis of selected traffic with a single click.

PERFORMANCE

	Write to disk	500 Mbps
	Maximum Flow Creation Rate	20k flows/sec
	Maximum Concurrent Flows	200K
	Number of Application Dock Instances	Supported in hypervisor
	Storage depth	1 or 2 Terabytes

BENEFITS

Accurate

On demand access to rich network history provides conclusive evidence for investigations.

Powerful

Automation and streamlined workflow integration enables faster investigations. This improves security and reduces the impact of network and application performance issues.

Open

Integrating commercial, open source and custom applications provides unified access to a single authoritative source of network history.

Scalable and Reliable

EndaceProbes are engineered for reliability, longevity and security. Centralized management enables scalability and reduces OPEX costs.



Provenance Enriched History

Provenance™ augments recorded network history with rich contextual data.

- Self-describing packet traces support Big Data analysis, improve post-event problem resolution and simplify archiving
- Rich evidential trail for effective legal prosecution



Workflow Integration

Rich APIs provide integration with commercial, open source and custom applications.

- Pivot directly from alerts in 3rd -party applications to view related packets of interest in EndaceVision™ with Pivot-to-Vision.
- Automate archival of packet traces with extensive RESTful API.



Fusion Partner Program

Our market-leading, cybersecurity and network monitoring partners use EndaceProbe's API integration and Application Dock™ VM hosting to connect their solutions directly to Network History.

- Streamline and automate detection and investigation
- Choose from industry-leading security and performance solutions
- Shared access to a common, authoritative source of network history for all applications.

Minimum VM Resources required by vProbe

CPU cores	4
Memory	12 GB
Storage	1 TB or 2 TB
Hypervisor	VMware vSphere ESXi 6.7, 7.0
Interfaces	1x virtual NIC or 1x 1 GbE NIC with PCI passthrough for monitoring

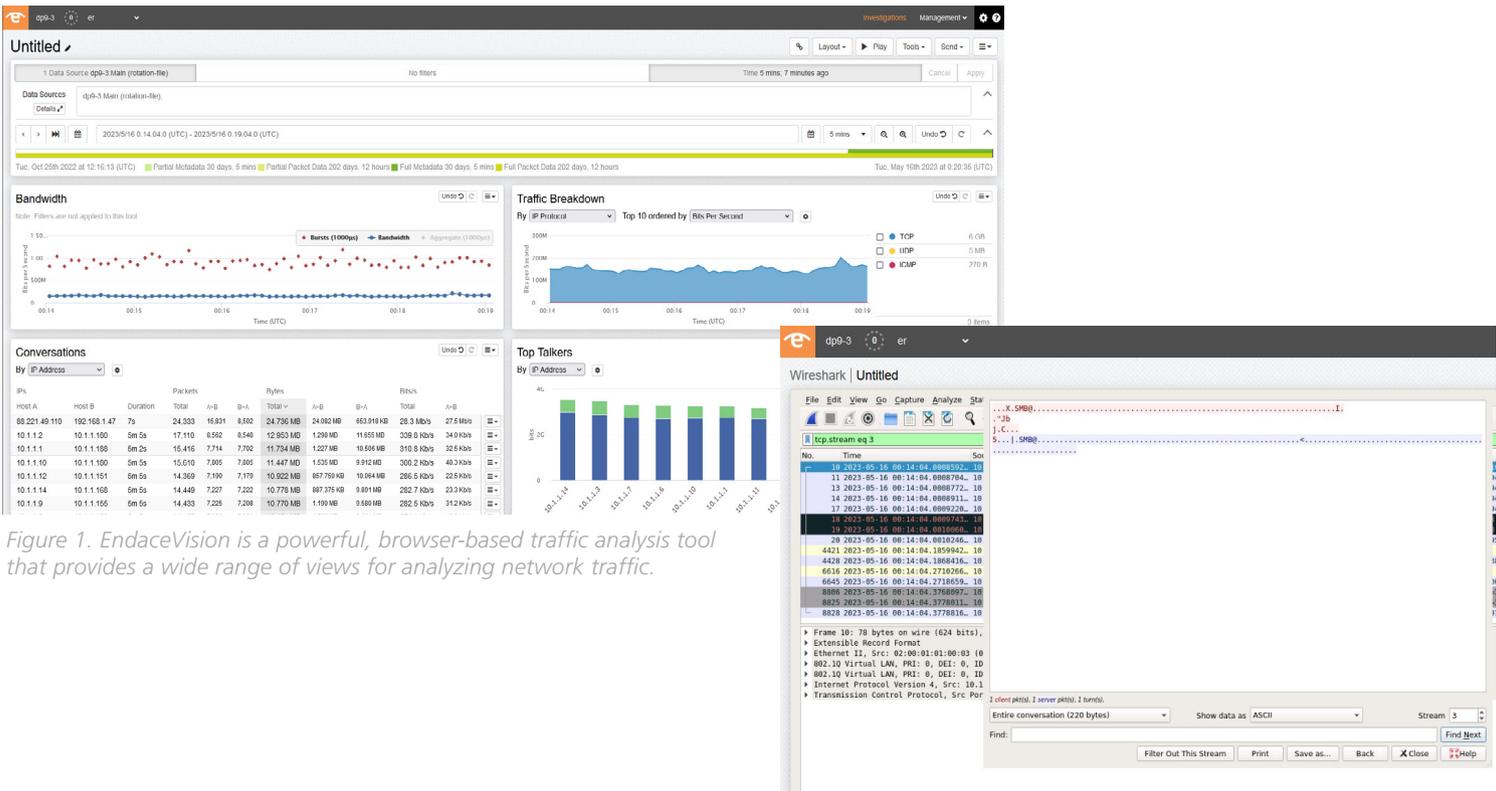


Figure 1. EndaceVision is a powerful, browser-based traffic analysis tool that provides a wide range of views for analyzing network traffic.

Figure 2. Hosted Wireshark™ running in the browser

Endace™, the Endace logo, Provenance™ 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