

EndaceProbe Cloud



EndaceProbe Cloud extends the world's most scalable, full packet capture platform to provide deep visibility into public cloud environments.

Continuously record days or weeks of full packet data, including east-west and north-south cloud traffic, to solve cybersecurity, network and application issues.

EndaceProbe Cloud is a full-featured EndaceProbe that can continuously record at 4 Gbps and store up to 250 TB of full packet capture data per instance. Multiple EndaceProbe Cloud instances can be combined to support higher-speed networks and provide increased storage capacity.

Visibility of Data-in-Motion in Public Cloud

It's critical your cloud workloads perform securely and reliably. Visibility into public cloud infrastructure is just as important as visibility into your private datacenter. Continuously recording cloud packet data lets you see exactly what is happening in your public cloud infrastructure so you can investigate and defend against even the toughest security threats and resolve performance issues or service outages before customers are impacted.

EndaceProbe Cloud can record network packet data from virtual Packet Brokers, VPC mirrors, virtual SPAN ports, load balancers, firewalls, vSwitches and virtual machines. All packet data recorded is securely held within your VPC or Virtual Network, ensuring you remain in full control of sensitive data. Multiple EndaceProbe Cloud instances can be combined to provide continuous recording of network activity for critical cloud workloads, applications, services, gateways and sensitive data assets.

Unified Visibility Across Hybrid Networks



EndaceProbes provide scalable, always-on, full packet capture across all your network infrastructure: on-premise, private cloud and public cloud. Analysts can seamlessly access recorded data regardless of where it was recorded. A single console provides centralized search and analysis across your entire hybrid-cloud infrastructure. Respond to incidents, alerts, or threats that originate from anywhere on your network.

REC Accurate Recording in Cloud

Purpose-built Virtual Machine for continuous network packet in AWS and Azure Public Cloud environments.

- Accurately record every packet before, during and after any event.
- Full packet level visibility across Azure and AWS environments.
- Definitive evidence for quickly and accurately resolving security threats and network or application performance problems

PERFORMANCE¹

	Write to disk	4 Gbps
	Storage depth	Native 250 Terabytes Packets > 500 Terabytes

¹ Performance is measured on minimum recommended instance size. Actual performance will vary based on instance used.

² Effective packet storage accounting for RAID and metadata overheads and assuming a 4.5:1 ratio for compression and Smart Truncation of packet data

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.

Efficient Storage

Built in Compression and Smart Application Truncation optimizes the use of precious cloud storage resources and maximizes retention time.



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.

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 Pivot-to-Packets.

Secure

- Only authorized users can view or download packet data.
- Role Based Access Control (RBAC) restricts who can access data.
- Data remains within your VPC or Virtual Network and under your full control.

Fusion Partner Program

Our market-leading, cybersecurity and network monitoring partners use EndaceProbe’s API integration to connect their solutions directly to Network History.

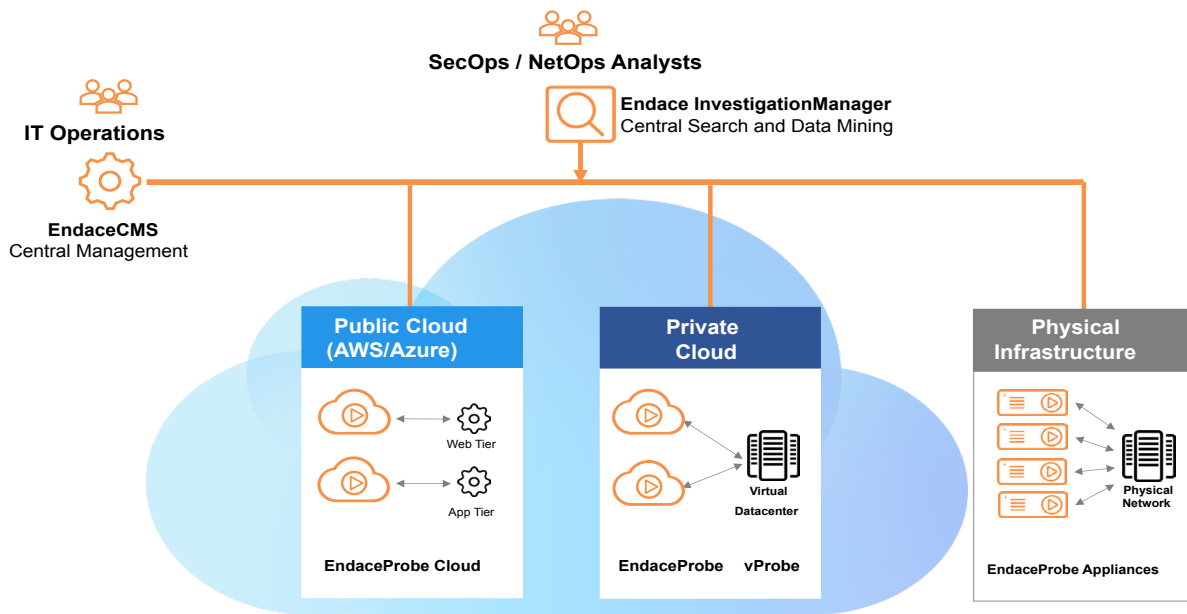
- Streamline and automate detection and investigation
- Shared access to a common, authoritative source of network packet capture evidence for all applications.

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.

Full Hybrid Cloud Visibility



Recommended cloud instance sizing

AWS	
Endace Probe	d3en.4xlarge
EndaceCMS	m5.xlarge
Endace InvestigationManager:	m5.2xlarge

Microsoft Azure	
Endace Probe	Standard_E16bs_v5
EndaceCMS	Standard_D4s_v4
Endace InvestigationManager:	Standard_D8s_v4

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

For further information, email: info@endace.com