Introducing EndaceProbe
EndaceProbe Overview

EndaceProbe™ appliances are a family of network recorders capable of capturing, indexing and recording network traffic with 100% accuracy on even the fastest, most complex networks.

EndaceProbes are used by some of the world’s largest banks, telcos and service providers, media and broadcast companies, health organizations, retailers, e-commerce giants and governments to deliver the accurate network data needed to effectively power their security incident response, network monitoring and other network applications.

Customers deploy EndaceProbes to troubleshoot and diagnose security breaches, network and application performance and other network related issues, or to deliver guaranteed lossless recording of network traffic to meet regulatory or governance obligations such as archiving and lawful intercept.

Why accurate packet capture is essential

Customers rely on the powerful packet capture and processing capability of EndaceProbes to provide their security and network monitoring applications with a complete, detailed and accurately time-stamped source of packet data.

Ultimately, only a 100% accurate source of network packets provides the irrefutable evidence needed to quickly and effectively identify and resolve security or network performance issues. NetFlow records, or incomplete, inaccurate sources of captured packets simply don’t deliver the detail necessary to reconstruct events and remediate issues such as intrusions, data breaches or network performance problems with certainty.

Ultimate Scalability

Multiple EndaceProbes can be connected to form a ubiquitous monitoring and recording infrastructure.

A connected fabric of EndaceProbes delivers network-wide data search, visualization, retrieval and analysis of captured packets through the EndaceVision™ and EndacePackets™ applications included free on every EndaceProbe.

EndaceProbes are available in a wide range of models - from ultra-high-speed models used in data center environments for recording traffic from multiple 10GbE and 40GbE networks simultaneously, to low cost models used in branch offices or other edge deployments.

Easy Centralized Management

EndaceCMS™ (Central Management Server) allows a connected fabric of hundreds of EndaceProbes (and other Endace appliances) to be centrally managed through a powerful GUI interface and a suite of command-line tools.

Updates and configuration changes can be applied in real-time or scheduled for later deployment. Grouping and customizable configuration profiles make it easy to update multiple devices simultaneously and ensure consistent configuration.

EndaceCMS monitors all connected appliances, providing at-a-glance estate health and status, along with customizable alarms and thresholds to ensure instant notification of any service-affecting issues.
Total Flexibility, Open Architecture

EndaceProbes are uniquely multi-functional. Their open architecture and application hosting capability enable them to be used with a variety of third-party commercial, open-source or custom developed applications.

Endace's open API and support for industry standard capture formats make it easy to integrate Endace hardware with third-party applications and tools. The API supports fast search and extraction of traffic for analysis by a wide range of security, network monitoring and application performance monitoring applications. This enables faster response to network and security issues before they impact on user experience or compromise data integrity.

Endace Application Dock™, the integrated virtual machine (VM) hosting environment on every EndaceProbe, enables commercial, open-source and custom-developed applications to be deployed directly on the EndaceProbe itself. This gives the hosted application full and immediate access to captured data on the probe without the need to transfer large data capture files across the network and removes the need for additional servers and rack space for hosting applications that consume packet data.

Endace works with a number of commercial partners – such as Splunk®, Cisco® and Dynatrace® – to provide integration between their software applications and Endace hardware. Additionally, a wide range of open source tools (such as SNORT®, Bro™️, Suricata™️, Argus™️ and Wireshark®) is compatible with EndaceProbes. Many Endace customers also integrate their own custom-developed applications either using Application Dock to host the applications directly or using the open API.

Maximum Functionality

EndaceProbes deliver:

- Guaranteed 100% capture and recording of network traffic across multi-1GbE/10GbE networks and on 40GbE links
- 100% accurate data for back-in-time incident investigation and troubleshooting
- The ability to analyze network traffic before, during and after a specific period of interest, such as a security breach, outage or traffic microburst
- Fast drill down to packet level analysis on multi-terabyte trace files stored locally on EndaceProbes
- Easy exporting of traffic to desktop or other servers from the bundled EndaceVision and EndacePackets applications or via the open, RESTful Application Programming Interface (API)
- Easy integration with leading security monitoring (IDS/IPS and SIEM), network performance management (NPM), application performance management (APM) and other network tools
- The ability to find rogue applications via deep packet inspection (DPI) and port identification
- Centralized deployment, configuration and management enabling fabrics of connected probes to be managed efficiently and reducing the cost of ownership.

Monitoring for 40Gbps and 100Gbps networks

EndaceProbes can natively record and monitor traffic on 40GbE links. When used in conjunction with an EndaceAccess™ Network Visibility Head-End, they can also be used to record and monitor traffic from 100GbE links.

EndaceAccess Head-Ends ingest 100GbE traffic, load balancing and splitting it across multiple 10GbE egress ports, enabling the traffic to be fed to EndaceProbes for processing and recording. This extends the return on investment on 10Gbps-capable security and monitoring tools, giving them full visibility into traffic on 100GbE links.
The EndaceProbe Family

Choosing network recorders requires balancing considerations of rack space availability, the speed and utilization of the network segments being monitored, and the depth of storage required.

EndaceProbes come in a variety of configurations to suit a range of deployment options from edge deployments such as branch offices to deployment in data centers where heavily utilized network links demand high-speed capture and/or high capacity storage.

Ultra high-performance EndaceProbes

EndaceProbe 8100 Series

Our performance flagship EndaceProbes, the 8100 Series, are capable of sustained capture to disk at a market-leading 40Gbps and are perfect for heavily loaded, core network connections. The 24TB of reliable, ultra-fast SSD storage can store more than 14 hours of packet data for a 10Gbps link under moderate load. They come with either four or eight 1GbE/10GbE monitoring ports - which can also be combined to provide up to two 40GbE monitoring interfaces.

High-capacity EndaceProbes

EndaceProbe 9000 Series

When data retention and depth of storage is key, the EndaceProbe 9000 series provides industry-leading capacity to ensure sufficient storage to meet your needs. The 4U 9000 Series EndaceProbes provide up to 192TB of onboard storage on secure self-encrypting hot-swappable drives and can store more than 60 hours of traffic from a moderately loaded 10GbE network and deliver 20Gbps sustained write speed. This makes them perfect for deploying in data centers for investigating slow attacks or transient problems and to comply with stringent data retention policies. They come with either four or eight 1GbE/10GbE monitoring ports - which can also be combined to provide up to two 40GbE monitoring interfaces.

Space-saving EndaceProbes

Where available space is a paramount consideration, the 1RU EndaceProbes 400, 4000, and 4100 Series offer a range of compact but powerful monitoring and recording solutions.

EndaceProbe 404

Endace’s entry level recording appliance is ideal for branch environments or other edge deployments. It can store more than 40 hours of captured traffic on a moderately loaded 1GbE link and is capable of recording at a sustained write speed of 500Mbps to secure, hardware encrypted RAID drives. With four 10/100/1000 recording interfaces, it provides a flexible solution that simplifies deployment on different networks.

EndaceProbe 4000 Series

Endace’s 4004 and 4008 10GbE/40GbE 1RU appliances have all the features of the 404. But with up to four times the storage, and either four or eight 1GbE/10GbE recording interfaces, they offer sustained write-to-disk speed of 3Gbps and storage for up to four days’ traffic on a moderately loaded 1GbE link.

EndaceProbe 4100 Series

The diminutive size of the 4104 and 4108 EndaceProbes belies their power. They offer the ability to capture to disk at up to 22Gbps and either four or eight 1GbE/10GbE monitoring interfaces - which can also be combined to provide up to two 40GbE interfaces. This makes the 4100 Series a perfect solution for on-demand recording at data center speeds. The SSD storage provides capacity for an hour or more of packet data at full 10Gbps line rate, and their inherently reliable nature makes them suitable for picking up and moving for ad-hoc deployments when needed. The SSD-based storage also makes the 4100 Series a popular option for deploying in remote or hard-to-reach locations where ultra-high reliability is required.

Contact Endace

Endace has offices in the US, UK, Australia and New Zealand. For further information about Endace products and services or to speak with a representative, please contact us:

Email: info@endace.com
Web: endace.com/products

USA and Americas: +1 877 764 5411
United Kingdom, Europe, Middle East and Africa: +44 0800 088 5008
Australia: +61 1800 642 476
New Zealand: +64 9 582 0360

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).