Introducing Endace
100% ACCURATE NETWORK RECORDING
NI USE IT ANY SPEED
ANY NETWORK
LATENCY MANAGEMENT
SECURITY
Introducing Endace

Since 2001, Endace has provided high-speed, network visibility solutions to operators of the world's largest, most complex networks including global banks, telecommunications and mobile carriers, media and broadcast companies, health organizations, ecommerce giants and governments.

Endace solutions deliver the actionable network data our customers need for security and network performance issue identification and resolution, forensic analysis of data breaches and other security events and to meet regulatory and governance obligations such as archiving and lawful intercept.

Our customers choose Endace because:

- We guarantee 100% accurate capture and storage of network traffic regardless of network types, speeds or loads
- Our open philosophy means Endace solutions integrate easily with a broad range of commercial, open-source and custom-developed security and network performance solutions
- Our solutions are highly scalable and capable of supporting the largest, fastest and most complex networks.

Endace solutions are used when customers need access to a 100% accurate record of network packets as a reliable, irrefutable data source for the identification and resolution of security or network performance issues, or where lossless capture and storage of network traffic is a requirement.

Our Philosophy

We believe a comprehensive and accurate record of network traffic is essential to enable truly effective investigation and resolution of network security and performance issues. It provides the definitive information that SecOps and NetOps teams need to quickly identify the root cause of issues so they can be resolved.

A network monitoring and recording solution should enhance the capability of existing processes, tools and infrastructure. It should reduce operational costs by delivering the visibility needed to improve the security and performance of the network.

To ensure this, we follow 3 simple principles:

- We design our solutions to work with a broad range of tools and applications, so customers can choose what suits them best
- We make our solutions easy and cost-effective to deploy and manage, reducing the cost of ownership
- We ensure our solutions are flexible and scalable so they can keep pace as our customers’ networks grow and their needs evolve.

An Open Architecture

In our view, a network monitoring and recording infrastructure should be able to support all of the applications and tools that need access to an accurate and complete source of network data to operate effectively - whether that's for security, network performance or other purposes.

Endace solutions are based on an open architecture to ensure compatibility with the widest possible range of applications. This gives customers the freedom to choose the tools that best meet their needs without being locked into a single vendor's solution.

Endace's open API, industry standard capture formats (PCAP and ERF) and the ability to host third-party applications on EndaceProbes, via the built-in Application Dock™ VM capability, are all part of what we call Endace Fusion™.

Endace Fusion offers a variety of ways for commercial and open-source partners such as Splunk®, Sourcefire®, Dynatrace®, SNORT®, Wireshark®, Bro™, Suricata™ and others, as well as custom in-house developed applications, to integrate easily with Endace solutions and access a single, authoritative and accurate source of network packets.
Endace Product Portfolio

Endace offers turnkey network visibility solutions for enterprise deployment, as well as a range of system components for system builders, OEMs and R&D labs looking to build their own custom packet capture solutions.

Our enterprise solutions include high-speed, high-performance network recorders, NetFlow generators, and network visibility head-ends. Endace system components include our industry-leading DAG™ packet capture cards and EndaceODE™ open development appliances.

Endace Network Visibility Solutions

EndaceProbes

EndaceProbes™ network recorders capture, index and record network traffic with 100% accuracy at data rates up to 100Gbps.

EndaceProbes can monitor and record data from multiple links from 10/100Mbps through to 40Gbps. When used with an EndaceAccess Network Visibility Head-End, EndaceProbes can also provide monitoring and recording on 100GbE links. They are available in a wide range of speeds and storage capacities. There are SSD-based models designed for on-demand deployment and monitoring high-speed segments, high-capacity models that provide deep storage for always on recording and small form factor models designed to suit remote office or other edge deployments.

The EndaceProbe™ vProbe is a virtual machine (VM) implementation of the EndaceProbe network recorder designed to complement hardware-based EndaceProbes in a network-wide, monitoring fabric. The vProbe integrates transparently with physical EndaceProbe deployments to expand visibility across the network. It is ideally suited for monitoring performance and diagnosing issues within virtualized applications, providing east-west traffic monitoring from within the virtual infrastructure without requiring physical appliances.

IT teams deploy EndaceProbes to troubleshoot and diagnose security, network and application performance issues. Multiple EndaceProbes can be combined to form a ubiquitous monitoring and recording fabric leveraging the bundled EndaceVision™ application for network-wide data search, visualization, retrieval and analysis, and EndaceCMS™ (Central Management Server) to provide powerful centralized management and deployment.

Endace Application Dock™ allows third-party commercial, open source or custom-developed applications to be hosted in virtual machines on the EndaceProbe itself, making them uniquely multi-functional devices. Hosted applications receive a high fidelity stream of packets, improving performance, density and configuration flexibility, including the option to load balance across multiple instances of the same application.

EndaceProbes:
- Record 100% of network traffic on multiple network links from 10/100Mbps to 40Gbps
- Provide 100% accurate data for back-in-time incident investigation and troubleshooting
- Allow analysis of network traffic before, during and after a specific period of interest, such as a security breach, outage or traffic microburst
- Offer powerful visualization and inspection of traffic on individual network segments or the entire network and centralized data mining and retrieval of captured traffic across all connected EndaceProbes
- Support easy exporting of traffic to desktop or other servers via the bundled EndaceVision and EndacePackets applications or via the open API
- Provide fast drill down to packet level analysis on multi-terabyte trace files
- Protect existing investments by integrating easily with commercial, open-source and custom-developed security, network and application performance monitoring tools and other network applications
- Support centralized deployment, configuration and management that enables fabrics of hundreds of connected probes to be managed efficiently and reduces cost of ownership.
EndaceVision and EndacePackets

EndaceVision™ Network Visibility Software is a browser-based application that helps IT teams investigate and resolve a wide-range of network related problems.

It is included free with every EndaceProbe and enables network engineers and security analysts to search, visualize, interrogate and retrieve historical network traffic recorded by EndaceProbes deployed inside data centers and across the network.

EndaceVision allows packets of interest to be quickly identified and transferred for analysis with third-party tools or using the browser-based EndacePackets™ protocol analysis application – also included free with every EndaceProbe.

Together EndaceVision and EndacePackets deliver a uniquely powerful, network-wide visualization tool that provides both a high-level view of network activity and the ability to quickly pivot down to packets of interest for extraction and analysis. They work efficiently with other analysis tools to provide faster network issue identification and remediation and allow network operations, applications and security teams to collaborate more effectively.

Key capabilities:
- 100% packet visibility on network links from 10 Mbps to 100GbE
- Segment-specific and network-wide analysis of network traffic and behavior
- Scalable analysis tools for investigating issues ranging from isolating the source of unexpected application traffic to the 10µs microburst root cause analysis.

EndaceFlow NetFlow Generator Appliances

EndaceFlow™ appliances can generate unsampled NetFlow records, eliminating the performance impact that switches and routers suffer when generating NetFlow, while delivering a 100% accurate view of flows on the network.

Each EndaceFlow appliance can monitor up to four 1Gbe/10GbE links (or one 40GbE link), with a total bandwidth capacity of more than 30Gbps and a total active flow cache size of 64 million flows.

EndaceFlows provide input for a wide range of network security, performance and network planning tools. They can deliver NetFlow in V5, V9 or IPFIX format, analyzing more than 30Gbps (or 16 million flows per second). Using a Network Packet Broker (NPB), multiple network links can be aggregated and fed into up to four monitoring ports.

EndaceFlows provide:
- Dedicated high-performance NetFlow generation for up to four links simultaneously
- Unsampled or sampled outputs, support for NetFlow V5, NetFlow V9 and IPFIX
- Flow-safe hash load balancing (HLB) to distribute NetFlow records to multiple NetFlow collectors
- High throughput capability
- Easy centralized management via EndaceCMS
- Low space, weight and power consumption with high reliability.
EndaceAccess Network Visibility Head-Ends

Security and monitoring tools are usually designed for 10GbE, which makes using them to monitor traffic on 100GbE networks a challenge.

The EndaceAccess™ Network Visibility Head-End solves this problem by ingesting 100GbE traffic and load balancing and splitting it over multiple 10Gbps ports, so 10Gbps-capable security or monitoring tools can be used in 100GbE environments.

EndaceCMS Central Management Server

The EndaceCMS™ Central Management Server provides powerful, centralized command and control for a connected fabric of EndaceProbe, EndaceFlow, EndaceAccess and vProbe appliances, reducing management overhead and lowering operational costs.

Designed to provide centralized management for entire estates of Endace appliances, EndaceCMS streamlines their configuration and management. Manually applying software updates and patches to a large number of appliances, particularly within short change control windows, can be a formidable task. EndaceCMS automates this process, ensuring all Endace appliances receive updates in a timely manner, without compromising monitoring visibility. Updates and configuration changes can be applied in real-time or scheduled for later deployment. Grouping of appliances and customizable configuration profiles make it easy to update multiple devices simultaneously and ensure consistent configuration.

EndaceCMS monitors all connected appliances in real-time, providing at-a-glance estate health and status, along with customizable alarms and thresholds to provide instant notification of any service-affecting issues. Rapid identification of malfunctioning or overloaded appliances enables fast response and remediation, ensuring that when a critical event occurs there is no gap in coverage across the monitoring fabric.

Endace Fusion Ecosystem

Endace Fusion is a collection of technology integration options and alliance partnerships, driven by customers who use Endace solutions to solve real-world operational problems.

By bringing together companies and technologies that complement each other, Endace Fusion allows customers to streamline their workflows, lower deployment costs and improve the performance of their security and network monitoring tools.

Endace hardware supports open formats (such as PCAP and ERF) making it easy to integrate with third-party applications and tools. Endace's open API supports fast search and extraction of traffic for analysis by third-party applications such as IDS, SIEM and NPM solutions. Additionally the API also delivers the ability to pivot directly into the EndaceVision interface, using parameters from an event, alarm or alert, providing a rapid and seamless transition from a notification into a packet drill-down. These capabilities enable quicker 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 appliance itself. This gives the hosted application access to a highly accurate data stream, improves performance through CPU offload and reduces the need for additional servers and rack space to host network security, performance monitoring and other applications.

Endace works with a number of commercial partners – such as Splunk, Sourcefire and Dynatrace – to provide integration between their software applications and Endace hardware. Additionally, a wide variety of open source tools (such as Snort, Bro, Suricata and Wireshark) are compatible with Endace hardware and are used by many of our customers. Many Endace customers also use Endace Fusion integration options to integrate their own custom-developed solutions.
Endace System Components

Endace DAG Data Capture Cards

Endace DAG™ data capture cards ensure 100% packet capture on any network, regardless of packet size, interface type or network load.

They have been used for more than 15 years on some of the world’s most demanding networks and are designed to suit custom-built network security, network monitoring and packet capture solutions where guaranteed performance and reliability are mandatory.

Because of their accuracy, reliability and performance, DAG cards have become the industry gold standard for data capture and are used by a wide range of organizations including government agencies, high frequency traders (HFT), telecommunications and service providers, security, NPM, APM, and SIEM solution providers and many others.

Endace DAG models are available for all network types and interfaces from 10/100/1000 Ethernet to SONET OC192c/SDH STM64, 10GbE and 40GbE.

Key features include:

- Load balancing of up to 40Gbps of network traffic while maintaining flow and session continuity
- Packet filtering, classification and replication in hardware and direct memory access delivers high-performance and offloads packet processing overhead from host CPUs
- Highly accurate packet time-stamping and clock synchronization from external time references
- Drivers for Linux and FreeBSD (all DAG models) and Windows (selected DAG models).

EndaceODE Open Application Platforms

EndaceODE™ Open Application Platforms host packet-processing applications in managed data center environments.

These flexible and scalable systems are used extensively by organizations that wish to build their own customized capture and hosting solutions, but demand the very highest levels of packet capture accuracy and processing performance.

EndaceODE systems are built using optimized server hardware components, tightly integrated with proprietary DAG card technology.

EndaceODE platforms are configured with a very simple Linux OS can be used for a variety of applications, and feature:

- Support for SONET and Ethernet interfaces from 10 Mbps to 40 Gbps
- Sophisticated hardware-based packet processing features
- 100% accurate packet capture to memory
- Multi-core Intel x86 processor
- High throughput capability
- Low space, weight and power consumption, high reliability.
Timing and Accessories

To enable customers to take advantage of the nanosecond-level timestamping accuracy provided by DAG cards and Endace appliances, Endace offers a range of EndaceTDS™ Time Distribution Servers, which enable time signals to be accurately synchronized across multiple capture points simultaneously from a common external time signal source such as a Global Positioning System (GPS) time receiver.

Endace also offers a wide range of accessories including GPS time receivers and transceivers for all network types compatible with Endace hardware.

Endace Support and EndaceCare Professional Services

Endace Support is available globally, 24 hours-a-day, seven-days-a-week to ensure we’re always there when customers need us to help with questions, software maintenance tasks or on the rare occasion when a hardware unit requires replacement.

EndaceCare Professional Services is available to customers and partners, and offers accelerated and cost-efficient installation and maintenance options for increased return on investment and reduced total cost of ownership. EndaceCare lets customers get the most out of their Endace solutions quickly and efficiently. Our experienced engineers offer deep industry experience, proven deployment methods and best practices and can provide onsite or remote assistance depending on customer needs.