Introducing Endace Network History

Capture Every Packet. See Every Threat.

endace
Record. Respond.

endace.com

Endace — the Network History Specialists

Endace redefined the packet capture market in 2001 with the industry-leading DAG card, which quickly became the gold standard for accurate and reliable packet-capture.

In 2007 Endace shook the market up again with the innovative NinjaProbe, an open, packet recording platform that simultaneously recorded traffic and hosted packet analysis applications.

Endace has continued to set the benchmark for 100% accurate, packet-capture, Network Recording and Playback at high-speed on the world's largest networks.

Endace Network History is used by operators of the most complex networks on the planet. It enables them to quickly and conclusively investigate and resolve cybersecurity threats, network problems and application performance issues, using a 100% accurate, packet-level record of network activity.

Endace customers include some of the world's largest banks, telecommunications and mobile carriers, media and broadcast companies, healthcare organizations, web giants, retailers, governments, and militaries.

Our Open Platform Philosophy

These three principles underpin the design of our open network recording and analytics hosting platform:

1. 100% Network History

We believe recorded packet-level Network History is the only truly definitive source of evidence for investigating network security threats and performance issues. But it needs to be complete and precise - so you can reconstruct past events and see exactly what happened. That's why our platform is designed for 100% accurate, lossless recording.

2. Integrate all your tools

Because Network History is such a crucial source of evidence, we think it should be accessible to all the teams and applications that need it. That's why we created powerful APIs that can integrate Network History into your chosen analytics tools and streamline investigations for rapid response to network issues.

3. Virtualize your analytics

The time has come for the cost benefits, flexibility and agility that virtualization has delivered to datacenters and networks to be available for network security and performance analytics too.

That's why we built a virtualization environment into our network recording platform. Now you can deploy analytics quickly and inexpensively and gain back the rackspace that's currently used to house racks of costly, obsolescence-prone analytics appliances.

endace
Record. Respond.

Overcome the Challenge of Monitoring Network Security and Performance

Distributed applications, web and mobile applications, cloud services and ubiquitous Internet access have all delivered unparalleled flexibility and power. But complex network and application architectures have made it increasingly difficult to ensure the security, reliability and performance of networks and the applications that run on them.

In the event of a security breach or cyber attack, it can be difficult or impossible to quickly determine exactly what happened, how it happened and what was compromised.

And organizations frequently find themselves frustrated by costly application performance problems and network outages that reduce productivity and impact badly on reputation and customer experience.

Tracking down the root cause of these problems used to be frustratingly slow and time-consuming. Not any more.

Introducing Network History

The answer to these challenges lies in Network History. Evidence of all activity on the network – including malicious activity – resides in the packets that travel across it. But once those packets have traversed the network, only faint shadows of that activity remain. Which leaves SecOps and NetOps teams forced to try and reconstruct events from log files, NetFlow meta-data and other sources. A slow and often inconclusive process.

Endace technology lets you record copies of every packet that traverses your network. When a problem occurs, or there's a security breach, you can go back and look at the original packets to see exactly what happened. Without the guesswork.

We help customers ensure the security and performance of their networks and the integrity of their confidential data by enabling them to record an accurate history of exactly what has happened on their networks. Using this Network History, NetOps, SecOps, IT and DevOps teams can go back in time to quickly and accurately reconstruct events and respond appropriately.

Making Network History Useful

100% Accurate Recording

Endace technology provides 100% lossless packet recording with nanosecond accurate time-stamping of every packet. Using a common time signal – such as GPS – timestamps can be synchronized across geographically-distributed networks. This precision and completeness is essential to enable accurate event reconstruction after the fact.

Network History Playback

Playback lets SecOps and NetOps analysts replay recorded Network History to their analytics applications to analyze past events. This allows detailed back-in-time investigations and automated analysis that is simply not possible using conventional investigative techniques.

Analytics Workflow Integration

Endace's powerful API makes it easy to integrate Network History with your existing tools to streamline investigation workflows and enable rapid response.

Endace's Pivot-to-Vision and Pivot-to-Packets API integration lets analysts go from an alert in their analytics tool of choice directly to the related Network History. They can quickly analyze the historical traffic using EndaceVision™, analyze decoded packets directly using a hosted instance of Wireshark™ or download pcap files for analysis or archival. These APIs also enable automation with solutions such as SOAR tools for automated packet search and retrieval. Easily reconstruct files and logs from packet flows using built-in file extraction.

Provenance Enriched History

For Network History to be useful, you need to know where it came from, how it was recorded and the state of the environment at the time. Provenance™ enhances recorded Network History with rich contextual data, embedding it into the packet history every second.

Provenance data lives with the packets, so at any time you can examine it in decode tools like EndacePackets and Wireshark alongside the packet data itself. With detailed information about how and where the packets were recorded there's never any doubt about the veracity of your evidence.

EndaceFabric

Seamlessly connect multiple EndaceProbe Network Recorders to form a centrally-managed, network-wide recording and analytics fabric.

EndaceProbe Analytics Platforms

EndaceProbes provide 100% accurate recording of network traffic from multiple links – from 10 Mbps to 100 Gbps. With sustained recording speeds up to 40 Gbps, and up to 288 TB of native packet storage, EndaceProbes can scale to handle the largest networks with ease. There are EndaceProbe models to suit a wide range of deployment options, from the core to the edge of the network.

EndaceVision and Wireshark

EndaceVision and Wireshark™ are included on every EndaceProbe and in InvestigationManager. EndaceVision lets analysts visualize and search network history to quickly identify and locate packets-of-interest. Packet data can be analyzed directly on the EndaceProbe in a hosted instance of Wireshark,avoiding the need to download large pcap files across the network for analysis. Easily reconstruct files and logs from packet flows using built-in file extraction.

EndaceCMS Central Management Server

Connected EndaceProbes can be centrally monitored, managed and configured using EndaceCMS™ Central Management Server. This allows an EndaceFabric to scale to hundreds, or even thousands of individual EndaceProbes while minimizing OPEX overheads. EndaceCMS can be can be hosted in VMWare or KVM environments or natively in Application Dock on an EndaceProbe appliance.

InvestigationManager

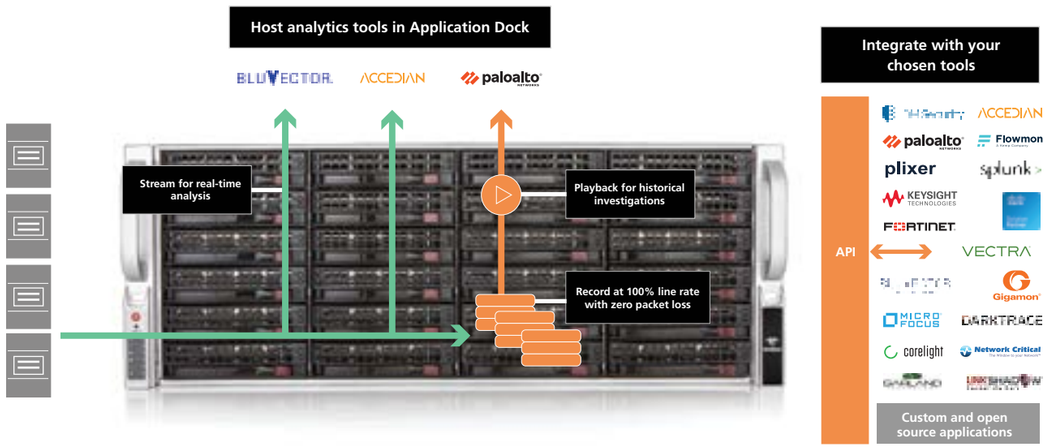
InvestigationManager™ is an application for ultra fast, network-wide data-mining across groups of EndaceProbes in an EndaceFabric using a single-pane-of-glass UI.

InvestigationManager can be hosted in VMWare or KVM environments or natively in Application Dock on an EndaceProbe appliance. Licenses are free-of-charge.

EndaceProbe Analytics Platform

The EndaceProbe is a unique packet capture, recording and analytics hosting platform.

In addition to recording Network History, the EndaceProbe™ Analytics Platform can simultaneously host a wide range of commercial, open-source and custom-built network security and performance monitoring applications in Application Dock™, the EndaceProbe's VM hosting environment, so you can deploy the tools you want when you want. The EndaceProbe's powerful API allows Network history to be integrated into all your security and performance analytics tools to streamline and automate the investigation and resolution of security threats and network or application performance issues.



Application Dock

The EndaceProbe's built in virtual hosting environment, Application Dock, builds on the concepts of Software Defined Networking (SDN) and Network Function Virtualization (NFV).

It enables the virtualization of network security and performance monitoring analytics, delivering the same cost benefits and flexibility to analytics that SDN and NFV have delivered in enterprise networks.

Application Dock lets you deploy analytics functions across the network wherever you need them and quickly change what you deploy as needed. All without requiring a truck-roll. Which means deployments can happen in hours not months, and you can slash costs by leveraging one common hardware platform to support your analytics needs.

Hosted applications can access a stream of live traffic for real-time analysis. Or, using Playback™, they can be fed a stream of historical traffic giving you the ability to go back in time and investigate past events using a complete and accurate recording of exactly what happened.

Open-Source Tools

Open source cybersecurity and network monitoring tools are ideal candidates for hosting in Application Dock.

Endace customers commonly deploy tools such as SNORT, Suricata, Bro and Argus on their EndaceProbes.

Built-In Investigation Tools

EndaceProbes include EndaceVision, a powerful, browser-based investigation and visualization tool.

Centralized data-mining enables analysts to quickly find and analyze packets-of-interest from anywhere on the network that EndaceProbes are deployed. Once packets-of-interest have been identified, they can be analyzed in a hosted instance of Wireshark on the EndaceProbe, or downloaded for archival or local analysis. Easily reconstruct files and logs from packet flows using built-in file extraction.

Fusion Partners

Integrate Network History with the tools you use every day.

Endace's Fusion Partner Program is an ecosystem of market-leading cybersecurity, network performance monitoring (NPM) and application performance monitoring (APM) vendors.

Endace Fusion Partners leverage the EndaceProbe's API integration and Application Dock hosting to integrate their solutions with network history, streamlining and automating detection and investigation and enabling back-in-time investigation using Playback.

Product Catalog

The EndaceProbe Family

EndaceProbe 9200 G4 Series

Delivering up to a Petabyte of effective packet storage, the flagship EndaceProbe 9200 G4 Series uses built-in compression and patent-pending Smart Truncation™ on top of 432 TB of fully RAID-protected raw storage. All in a single, 4RU appliance that can record at a sustained 40 Gbps.

Multiple 9200's can be stacked and used with a Network Packet Broker to provide monitoring for 100 GbE, or faster, links and petabytes of storage capacity.

The 9200 is ideal for data center deployments and always-on recording and comes with four or eight 1 GbE/10 GbE recording interfaces (or up to two 40 GbE interfaces).

EndaceProbe 8200 G4 Series

With a maximum sustained write-to-disk speed of 15 Gbps, storage capacity of 144 Terabytes (up to 360 Terabytes of effective packet storage with compression and SmartTruncation) and the ability to host up to 12 applications, the 8200 G4 Series combines speed, capacity and hosting density in a compact, modular 2RU appliance.

Multiple 8200's can be stacked to increase storage capacity and recording speed as network speeds and traffic volumes increase and add additional hosting capacity for deploying new analytics solutions across the network.

EndaceProbe 4100 G4 Series

The diminutive size of the 1RU EndaceProbe 4100 G4 Series belies its power. It delivers a maximum sustained write to disk speed of 20 Gbps and 7.6 TB of SSD disk storage (up to 20 TB of effective packet storage wtih compression and Smart Truncation). The 4100 G4 provides four 1 GbE/10 GbE recording interfaces (or one 40 GbE interface) making it ideally suited to on-demand recording at data center speeds.

EndaceProbe 4000 G4 Series

The compact, 1RU 4000 G4 Series EndaceProbes offer four 1 GbE/10 GbE recording interfaces (or one 40 GbE interface) and 48 TB of storage (up to 120 TB of effective packet storage wtih compression and Smart Truncation) and a maximum sustained write to disk speed of 3 Gbps.

EndaceProbe 2100 G5 Series

The 2100 G5 Series EndaceProbes provide sustained recording at up to 40 Gbps, and ultra reliable SSD storage for up to 120 TB of effective packet storage. The compact, rugged, 1RU short form-factor chassis is ideal for network edge locations, such as remote offices and branch offices.

The 2144 offers four monitoring ports capable of monitoring from 10 MbE to 10 GbE with sustained write to disk speed of 10 Gbps and 7.68 TB of SSD storage for up to 20 TB of effective packet storage.

The 2184 offers four monitoring ports capable of monitoring from 10 MbE to 10 GbE or 1 port of 40 GbE, with sustained write to disk speed of 40 Gbps and 46 TB of SSD storage for up to 120 TB of effective packet storage.

EndaceProbe vProbe

EndaceProbe™ vProbe is a virtual machine implementation of the EndaceProbe. It's designed to record crucial network history in virtual and cloud environments and provide visibility into virtual network traffic, including East-West traffic. It can be seamlessly included as part of an EndaceFabric of connected physical and virtual EndaceProbes.

Timing and Accessories

The EndaceTDS™ TDS-24 Time Distribution Server enables 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) receiver - we supply GPS time signal receivers from Trimble.

We also provide a wide range of transceivers including both optical and electrical devices, covering all interface speeds from 10M bE to 40 GbE.

Endace Support and Endace Professional Services

Endace Support is available globally, 24 hours-a-day, seven-days-a-week. We're always there when you need us to help with questions or on the rare occasion when a hardware unit requires replacement or servicing. There is also a Customer Support Portal containing documentation, software file downloads, a knowledgebase and a forum, where you can connect with Endace's product and support teams and other Endace customers.

Endace Professional Services offers accelerated and cost-effective training, installation, maintenance and product integration. Endace Professional Services helps 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. Services can be provided onsite or remotely depending on customer needs.

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: www.endace.com

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