EndaceVision and EndacePackets

Powerful, application-aware investigation tools.

EndaceVision™ and EndacePackets™ are powerful, browser-based investigation tools that come bundled with all EndaceProbe™ Network Recorders and EndaceCMS™ Central Management Server. EndaceVision enables network operations, security, or incident response teams to navigate quickly through network history data, to identify the cause of network performance and security issues and take appropriate action without guesswork. EndacePackets provides on-probe decoding of packet history, removing the need for analysts to download large packet trace files for analysis.

EndaceVision operates as a distributed application enabling a view of the entire network being monitored and a rapid pivot down to specific segments or links as required. It acts both as a visualization tool for viewing and analyzing traffic, and as a search engine for accessing traffic streams and packets of interest from recorded Network History.

The intuitive user interface lets users quickly drill-down by time, user, server, protocol, application, or a variety of other attributes to locate the 'packets of interest' relevant to a particular investigation. EndaceVision closes the gaps between detecting a problem, establishing why it happened, and remediating the issue. This can reduce the time needed to resolve issues from days or weeks to hours or even minutes.

Because EndaceVision reduces the amount of time it takes to investigate network issues or events, and enables many issues to be investigated and resolved without escalation to senior analysts, it reduces operating expenditure (OPEX) and mean-time-to-resolution (MTTR).

Network-wide visibility

A monitoring and recording fabric of connected EndaceProbes guarantees a complete and actionable network traffic history for the fastest networks, up to and including 100GbE links.

With an EndaceFabric in place, EndaceVision lets you:

- Construct a highly accurate real-time picture of what's happening across a global network based on a range of network attributes such as bandwidth utilization and application usage
- Rapidly extract specific packets of interest from any EndaceProbe across the network as a single file or multiple files to decode and use with any tools that support PCAP
- Perform retrospective forensic analysis of network events by mining and interrogating a 100% accurate source of Network History, with every packet carrying a highly accurate timestamp to enable accurate reconstructions
- Search and analyze packets from multiple EndaceProbes simultaneously as easily as from a single source.

ENDACE VISION AT A GLANCE

Powerful application-aware, browser-based investigation tool that will run on any modern browser

Network-wide investigation of performance and security events with definitive, packet level Network History

100% packet visibility on network links from 10Mbps to 100Gb Ethernet (100GbE)

Expand range of visualizations including accurate microburst detection, bandwidth over time and top talkers

Support for role-based access control (RBAC) and Terminal Access Controller Acess-Control System (TACACS) security

BENEFITS

- Quickly analyze network traffic before, during, and after a specific period of interest, such as a security alert, outage or microburst
- Reduced mean time-to-resolution (MTTR) for network or security events
- Definitive evidence for investigations
- No license costs

Sharing and collaboration

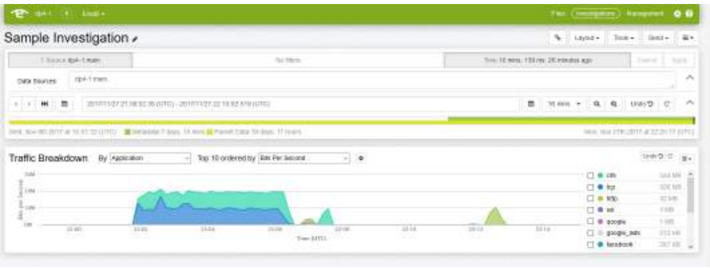
Recognizing how modern network teams are organized and the role team collaboration plays in resolving major network issues, EndaceVision enables easy collaboration between team members. Any visualization can be saved and shared between users, and common filters and visualizations can be templated. This allows repetitive tasks to be performed much more quickly and further reduces MTTR.

Easy to access, easy to integrate

EndaceVision runs on Endace OSm™ software, a hardened network operating system based on the CentOS Linux distribution. With appropriate credentials, an operator can access EndaceVision using any modern web browser on desktop or tablet devices.

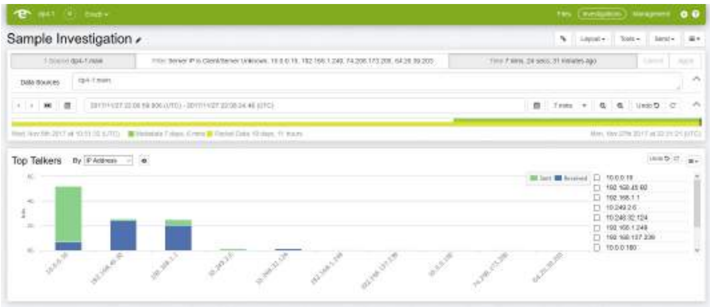
© Copyright Endace Technology Limited, 2017. All rights reserved. Information in this data sheet may be subject to change.

EndaceVision complements existing prevention and detection tools by bringing the definitive evidence of 100% accurate Network History and the forensic power of packet analysis to bear on investigating security threats and network or application perfomance problems.



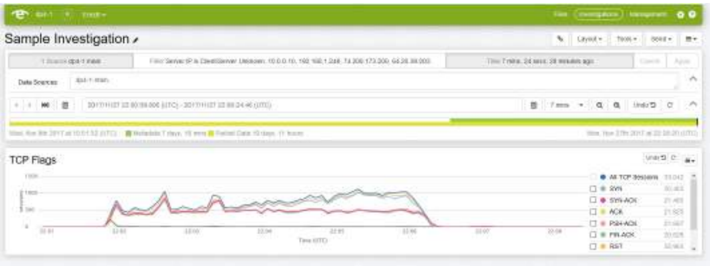
Dynamic network visualizations

EndaceVision presents a rich variety of data visualizations enabling real-time and retrospective analysis of network performance and security issues. Typical uses include drill-down diagnosis of network performance issues, locating unapproved application traffic, and pinpointing security infractions for fast remediation.



With fast toggling between views, users can rapidly zoom in to a particular time period or application to get a more granular view of behavior, or zoom out to get a macro view.

- Bandwidth utilization gives users the ability to visualize any time range with a resolution down to 10µs. Bandwidth shows both average and maximum values, so spikes are easy to identify and zoom in on.
- Protocol distribution and traffic-breakdown-over-time views give users visibility into the types of traffic on their network and how that distribution changes over time. An extensive variety of industry standard applications and protocols are recognized heuristically, regardless of port. Users can drill-down from application distribution to the specific internal and external IP addresses involved in the flow to identify unauthorized or unexpected applications.
- Top talkers allows users to find the busiest hosts on a network, both sending and receiving.
- Conversations view displays which hosts and users are exchanging data with each other at the MAC, IP, or Transport layers.
- TCP Flags visualizes the behavior of TCP sessions using the protocol's own built-in signaling. Since network forwarding devices are affected by both bandwidth and sessions, the TCP Flags visualization allows a user to track session activity by total count, creation, active data transfer, and tear-down, as well as detect network problems like SYN floods and server failures.
- Any number of network segments across one or more EndaceProbes can be aggregated with any of these views to provide visibility either for a single segment or across the entire network.

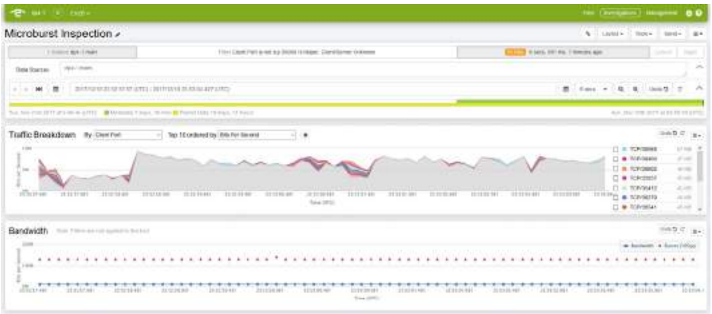


Each of the visualizations allows the analyst to progressively isolate related events by constructing hierarchical filters that refine the range of data being investigated. This ultimately leads to the packets of interest that can then be extracted for use in external tools, or investigated in situ using EndacePackets.

MicroVision

Small events can have a big impact, even on 10Gbps or faster networks. EndaceVision's MicroVision™ capability allows rapid investigation of timeframes down to 10µs to allow deep investigation with minimal effort. Those small events can be microbursts causing switch port queue drops and jitter, control channel traffic that's virtually invisible under high-bandwidth videoconference data, or even brief Distributed Denial of Service (DDoS) tests before the real attack. Endace MicroVision includes the full power of all EndaceVision views and filters to provide clarity quickly.

MicroVision also enables the use of PCAP analysis tools on 10Gbps networks. One second of 10Gbps is a full gigabyte, which causes problems for many tools. Endace MicroVision solves this problem with a combination of filters and sub-second resolution, enabling users to export PCAP files from EndaceProbes at much smaller sizes while still containing the relevant packets of interest.



© Copyright Endace Technology Limited, 2017. All rights reserved. Information in this data sheet may be subject to change.

Easy to access, easy to integrate

EndaceVision runs on Endace OSm™ software, a hardened network operating system based on the CentOS Linux distribution. With appropriate credentials, an operator can access EndaceVision using any modern web browser on desktop or tablet devices.

EndaceVision complements existing prevention and detection tools by bringing the definitive evidence of 100% accurate Network History and the forensic power of packet analysis to bear on investigating security threats and network or application perfomance problems.

Traffic categorization

EndaceVision leverages a powerful distributed database of information relating to traffic captured by multiple EndaceProbes. This database allows analysis and itemization of traffic present at both individual monitoring points or scaled up across the entire enterprise including: Time, Application, IP protocol and port, IP version, IP address, MAC address, VLAN, Multiprotocol Label Switching (MPLS) and data source.

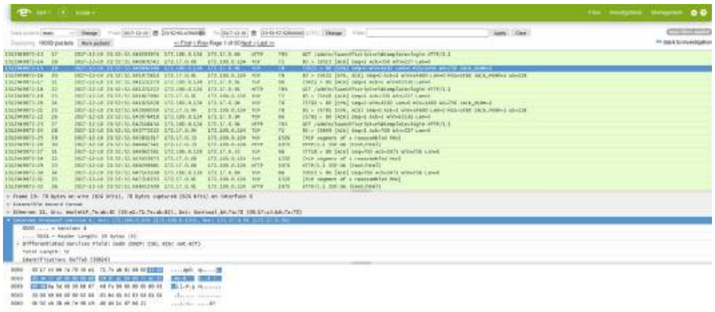
Download acceleration

EndaceProbes use a unique “download acceleration” technology that tracks all captured network traffic for ondisk storage. This ensures the EndaceProbe can easily identify the location of every packet on disk and retrieve any packet rapidly on-demand. Using download acceleration eliminates the search overhead of traditional packet capture solutions, dramatically reducing the time needed to extract a trace file for immediate investigation of security or network issues. All download types are accelerated, whether archiving traffic to the EndaceProbe, downloading from the web interface, or programmatically downloading via API.

Innovative EndacePackets on-probe protocol analyzer

EndacePackets™ is a powerful, integrated, web-based packet decoding tool. This protocol analyzer, based on the industry-standard Wireshark interface, runs on all EndaceProbes and is accessed directly within EndaceVision. EndacePackets integrates with the other views in EndaceVision, so a user can quickly identify traffic sessions of interest, create a filter, and pivot directly to the packets themselves.

- application distribution to the specific internal and external IP addresses involved in the flow to identify unauthorized or unexpected applications.
- Top talkers allows users to find the busiest hosts on a network, both sending and receiving.
- Conversations view displays which hosts and users are exchanging data with each other at the MAC, IP, or Transport layers.
- TCP Flags visualizes the behavior of TCP sessions using the protocol’s own built-in signaling. Since network forwarding devices are affected by both bandwidth and sessions, the TCP Flags visualization allows a user to track session activity by total count, creation, active data transfer, and tear-down, as well as detect network problems like SYN floods and server failures.
- Any number of network segments across one or more EndaceProbes can be aggregated with any of these views to provide visibility either for a single segment or across the entire network.



Summary

EndaceVision is an essential monitoring and forensic investigation tool for any organization running complex 1Gbps, 10Gbps or 40/100GbE networks. With the unique attribute of having a 100% accurate packet foundation, EndaceVision is the only monitoring solution that is built to meet the exacting demands of today’s and tomorrow’s ultra-high speed networks.

EndaceVision delivers true 100% network visibility that speeds network issue resolution and starts organizations on the road towards automating the resolution of network performance and security issues.

© Copyright Endace Technology Limited, 2017. All rights reserved. Information in this data sheet may be subject to change.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission [FCC] Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction document, may cause harmful interference to radio communications.

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).

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

For further information, email: info@endace.com

© Copyright Endace Technology Limited, 2017. All rights reserved. Information in this data sheet may be subject to change.