endace

DATASHEET

EndaceVision

Powerful, application-aware investigation tools.

EndaceVision™ is a powerful, browser-based investigation GUI built into all EndaceProbe™ Analytics Platforms and into InvestigationManager™, the VM that enables rapid estate-wide search and data-mining.

EndaceVision lets network operations, security, or incident response teams navigate quickly through network history data, identify the causes of network performance and security issues and take appropriate action without guesswork. It also provides on-probe packet decoding using a hosted instance of Wireshark™, removing the need for analysts to download large packet trace files for analysis.

EndaceVision provides a view of the entire network being monitored with the ability to rapidly 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.

By making it quick and easy for analysts to find and analyze the exact packets they're interested in, from amongst potentially petabytes of recorded network history, EndaceVision puts critical evidence right at the fingertips of analysts, enabling them to make confident decisions quickly.

EndaceVision's 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 investigate and resolve issues from days or weeks to hours or even minutes.

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 100 GbE links. Together, EndaceVision and InvestigationManager let 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 or decode without downloading using hosted Wireshark.
- 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)

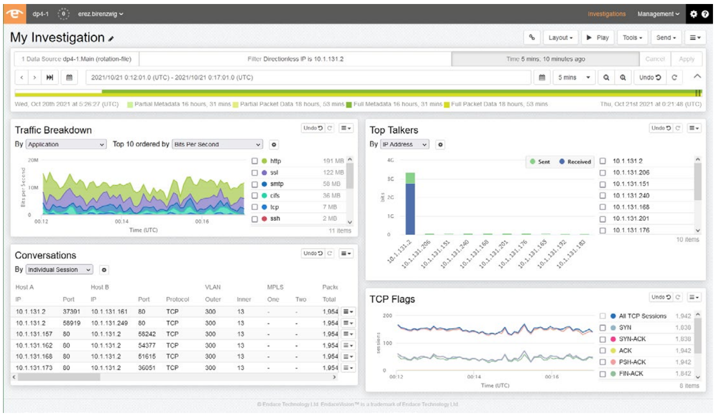
Expand range of visualizations including accurate microburst detection, bandwidth over time and top talkers

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

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 performance problems.



My Investigation

1 Data Source dp4-1.Main (rotation-file)

Filter Directionless IP is 10.1.131.2

Time 5 mins, 10 minutes ago

2021/10/21 0:12:01.0 (UTC) - 2021/10/21 0:17:01.0 (UTC)

Wed, Oct 20th 2021 at 5:26:27 (UTC) Partial Metadata 16 hours, 31 mins Partial Packet Data 18 hours, 53 mins Full Metadata 16 hours, 31 mins Full Packet Data 18 hours, 53 mins Thu, Oct 21st 2021 at 0:21:48 (UTC)

Traffic Breakdown

By Application Top 10 ordered by Bits Per Second

Host A		Host B			VLAN		MPLS		Packe
IP	Port	IP	Port	Protocol	Outer	Inner	One	Two	Total
10.1.131.2	37391	10.1.131.161	80	TCP	300	13	-	-	1,954
10.1.131.2	58919	10.1.131.249	80	TCP	300	13	-	-	1,954
10.1.131.157	80	10.1.131.2	58242	TCP	300	13	-	-	1,954
10.1.131.162	80	10.1.131.2	54377	TCP	300	13	-	-	1,954
10.1.131.168	80	10.1.131.2	51615	TCP	300	13	-	-	1,954
10.1.131.173	80	10.1.131.2	36051	TCP	300	13	-	-	1,954

Top Talkers

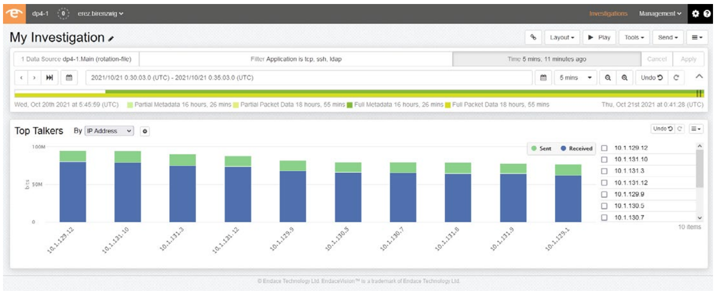
By IP Address

TCP Flags

© Endace Technology Ltd. EndaceVision™ is a trademark of Endace Technology Ltd.

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.



1 Data Source dp4-1.Main (rotation-file)
Filter Application is tcp, ssh, ldap
Time 5 mins; 11 minutes ago
2021/10/21 0.30.03.0 (UTC) - 2021/10/21 0.35.03.0 (UTC)
Wed, Oct 20th 2021 at 5:45:59 (UTC) 🟩 Partial Metadata 16 hours, 26 mins 🟩 Partial Packet Data 18 hours, 55 mins 🟩 Full Metadata 16 hours, 26 mins 🟨 Full Packet Data 18 hours, 55 mins Thu, Oct 21st 2021 at 0:41:28 (UTC)
By IP Address

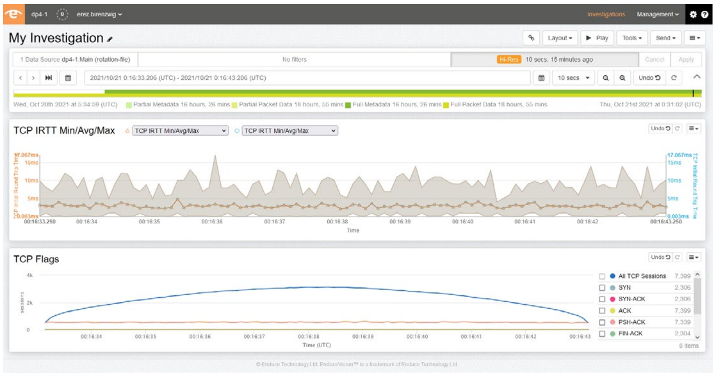
With fast toggling between views, users can rapidly zoom in to a particular time period or application to get a more granular view of behavior, or zoom out to get a macro view.

- 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 hosted Wireshark.

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.



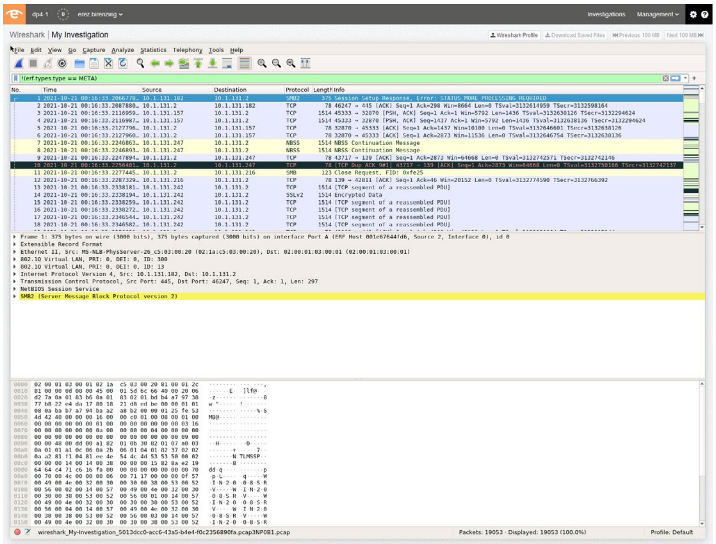
1 Data Source dp4-1.Main (rotation-file)
No filters
10 secs; 15 minutes ago
2021/10/21 0:16:33.206 (UTC) - 2021/10/21 0:16:43.206 (UTC)
Wed, Oct 20th 2021 at 5:34:59 (UTC) 🟩 Partial Metadata 16 hours, 26 mins 🟩 Partial Packet Data 18 hours, 55 mins 🟩 Full Metadata 16 hours, 26 mins 🟨 Full Packet Data 18 hours, 55 mins Thu, Oct 21st 2021 at 0:31:02 (UTC)
TCP IRTT Min/Avg/Max | TCP IRTT Min/Avg/Max

□	● All TCP Sessions	7,399
□	● SYN	2,306
□	● SYN-ACK	2,306
□	● ACK	7,399
□	● PSH-ACK	7,339
□	● FIN-ACK	2,304

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.

Decode packets directly without having to download pcaps

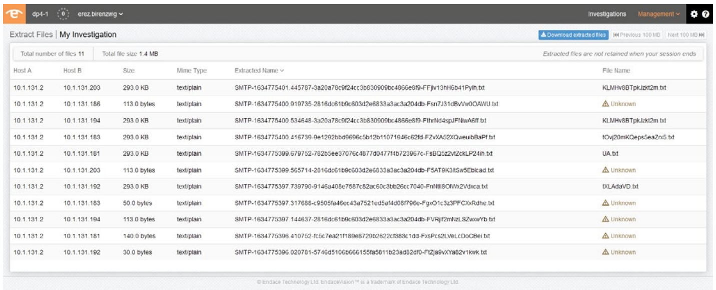
EndaceProbes and InvestigationManager provide hosted Wireshark, making it easy to decode packets directly without having to download large pcap files to the desktop. Users can quickly identify traffic sessions of interest, create a filter, and pivot directly to view the decoded data in hosted Wireshark.



```
!(erf.types.type == META)

No.  Time                          Source         Destination    Protocol Length Info
   1 2021-10-21 00:16:33.2066778… 10.1.131.182   10.1.131.2     SMB2      375 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED
   2 2021-10-21 00:16:33.2087880… 10.1.131.2     10.1.131.182   TCP        78 46247 → 445 [ACK] Seq=1 Ack=298 Win=8664 Len=0 TSval=3132614959 TSecr=3132598164
   3 2021-10-21 00:16:33.2116959… 10.1.131.157   10.1.131.2     TCP      1514 45333 → 32870 [PSH, ACK] Seq=1 Ack=1 Win=5792 Len=1436 TSval=3132638126 TSecr=3132294624
   4 2021-10-21 00:16:33.2116987… 10.1.131.157   10.1.131.2     TCP      1514 45333 → 32870 [PSH, ACK] Seq=1437 Ack=1 Win=5792 Len=1436 TSval=3132638136 TSecr=3132294624
   5 2021-10-21 00:16:33.2127796… 10.1.131.2     10.1.131.157   TCP        78 32870 → 45333 [ACK] Seq=1 Ack=1437 Win=10100 Len=0 TSval=3132646601 TSecr=3132638126
   6 2021-10-21 00:16:33.2127960… 10.1.131.2     10.1.131.157   TCP        78 32870 → 45333 [ACK] Seq=1 Ack=2873 Win=11536 Len=0 TSval=3132646754 TSecr=3132638136
   7 2021-10-21 00:16:33.2246863… 10.1.131.247   10.1.131.2     NBSS     1514 NBSS Continuation Message
   8 2021-10-21 00:16:33.2246893… 10.1.131.247   10.1.131.2     NBSS     1514 NBSS Continuation Message
   9 2021-10-21 00:16:33.2247894… 10.1.131.2     10.1.131.247   TCP        78 43717 → 139 [ACK] Seq=1 Ack=2873 Win=64668 Len=0 TSval=3132742571 TSecr=3132742146
  10 2021-10-21 00:16:33.2256401… 10.1.131.2     10.1.131.247   TCP        78 [TCP Dup ACK 9#1] 43717 → 139 [ACK] Seq=1 Ack=2873 Win=64668 Len=0 TSval=3132750166 TSecr=3132742137
  11 2021-10-21 00:16:33.2277445… 10.1.131.2     10.1.131.216   SMB       123 Close Request, FID: 0xfe25
  12 2021-10-21 00:16:33.2287329… 10.1.131.216   10.1.131.2     TCP        78 139 → 42811 [ACK] Seq=1 Ack=46 Win=20152 Len=0 TSval=3132774590 TSecr=3132766392
  13 2021-10-21 00:16:33.2338181… 10.1.131.242   10.1.131.2     TCP      1514 [TCP segment of a reassembled PDU]
  14 2021-10-21 00:16:33.2338194… 10.1.131.242   10.1.131.2     SSLv2    1514 Encrypted Data
  15 2021-10-21 00:16:33.2338259… 10.1.131.242   10.1.131.2     TCP      1514 [TCP segment of a reassembled PDU]
  16 2021-10-21 00:16:33.2338272… 10.1.131.242   10.1.131.2     TCP      1514 [TCP segment of a reassembled PDU]
  17 2021-10-21 00:16:33.2346544… 10.1.131.242   10.1.131.2     TCP      1514 [TCP segment of a reassembled PDU]
  18 2021-10-21 00:16:33.2346582… 10.1.131.242   10.1.131.2     TCP      1514 [TCP segment of a reassembled PDU]

▸ Frame 1: 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits) on interface Port A (ERF Host 001e67644fd6, Source 2, Interface 0), id 0
▸ Extensible Record Format
▸ Ethernet II, Src: MS-NLB-PhysServer-26_c5:03:00:20 (02:1a:c5:03:00:20), Dst: 02:00:01:03:00:01 (02:00:01:03:00:01)
▸ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 300
▸ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 13
▸ Internet Protocol Version 4, Src: 10.1.131.182, Dst: 10.1.131.2
▸ Transmission Control Protocol, Src Port: 445, Dst Port: 46247, Seq: 1, Ack: 1, Len: 297
▸ NetBIOS Session Service
▸ SMB2 (Server Message Block Protocol version 2)

0000  02 00 01 03 00 01 02 1a  c5 03 00 20 81 00 01 2c   ········ ········,
0010  81 00 00 0d 08 00 45 00  01 5d 6c 66 40 00 20 06   ······E· ·]lf@· ·
0020  d2 7a 0a 01 83 b6 0a 01  83 02 01 bd b4 a7 97 38   ·z······ ·······8
0030  77 b8 22 e4 da 17 80 18  21 d8 ed be 00 00 01 01   w·"····· !·······
0040  08 0a ba b7 a7 94 ba a2  a8 b2 00 00 01 25 fe 53   ········ ·····%·S
0050  4d 42 40 00 00 00 16 00  00 c0 01 00 08 00 01 00   MB@····· ········
0060  00 00 00 00 00 00 01 00  00 00 00 00 00 00 03 16   ········ ········
0070  00 00 00 00 00 00 0a 00  00 00 00 04 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 09 00   ········ ········
0090  00 00 48 00 dd 00 a1 82  01 0b 30 82 01 07 a0 03   ··H····· ··0·····
00a0  0a 01 01 a1 0c 06 0a 2b  06 01 04 01 82 37 02 02   ·······+ ·····7··
00b0  0a a2 81 f1 04 81 ee 4e  54 4c 4d 53 53 50 00 02   ·······N TLMSSP··
00c0  00 00 00 14 00 14 00 38  00 00 00 15 82 8a e2 19   ·······8 ········
00d0  64 64 c4 71 c6 16 fa 00  00 00 00 00 00 00 00 70   dd·q···· ·······p
00e0  00 70 00 4c 00 00 00 06  00 71 17 00 00 00 0f 57   ·p·L···· ·q·····W
00f0  00 49 00 4e 00 32 00 30  00 30 00 38 00 53 00 52   ·I·N·2·0 ·0·8·S·R
0100  00 56 00 02 00 14 00 57  00 49 00 4e 00 32 00 30   ·V·····W ·I·N·2·0
0110  00 30 00 38 00 53 00 52  00 56 00 01 00 14 00 57   ·0·8·S·R ·V·····W
0120  00 49 00 4e 00 32 00 30  00 30 00 38 00 53 00 52   ·I·N·2·0 ·0·8·S·R
0130  00 56 00 04 00 14 00 57  00 49 00 4e 00 32 00 30   ·V·····W ·I·N·2·0
0140  00 30 00 38 00 53 00 52  00 56 00 03 00 14 00 57   ·0·8·S·R ·V·····W
0150  00 49 00 4e 00 32 00 30  00 30 00 38 00 53 00 52   ·I·N·2·0 ·0·8·S·R

wireshark_My-Investigation_5013dcc0-acc6-43a5-b4e4-f0c2356890fa.pcap3NP0B1.pcap    Packets: 19053 · Displayed: 19053 (100.0%)    Profile: Default
```

Easy File Extraction

EndaceVision also enables analysts to perform easy file extraction from selected traffic. This feature uses a hosted version of the opensource Zeek™ engine to parse the selected traffic, produce Zeek logs, and reassemble files from any file transfers in the selected traffic. These files and logs can be downloaded allowing files to be submitted to file-scanners or sandbox environments and logs to be reviewed for additional context.



Extract Files | My Investigation

Total number of files 11 | Total file size 1.4 MB

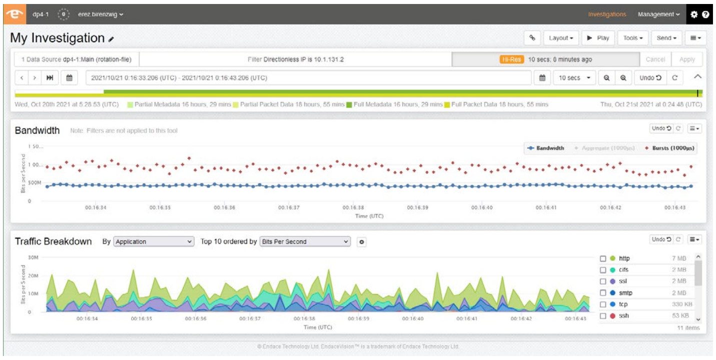
Extracted files are not retained when your session ends

Host A	Host B	Size	Mime Type	Extracted Name	File Name
10.1.131.2	10.1.131.203	293.0 KB	text/plain	SMTP-1634775401.445787-3a20a78c9f24cc3b830909bc4866e8f9-FFjlv13hH6b41Pylh.txt	KLMHv8BTpkJzkt2m.txt
10.1.131.2	10.1.131.186	113.0 bytes	text/plain	SMTP-1634775400.919735-2816dc61b9c603d2e6833a3ac3a204db-Fsn7J31dBvVw0OAWU.txt	⚠ Unknown
10.1.131.2	10.1.131.194	293.0 KB	text/plain	SMTP-1634775400.534648-3a20a78c9f24cc3b830909bc4866e8f9-FthrNd4spJFNiwA6ff.txt	KLMHv8BTpkJzkt2m.txt
10.1.131.2	10.1.131.183	293.0 KB	text/plain	SMTP-1634775400.416739-9e1292bbd9696c5b12b11071946c62fd-FZvXA52XQweuibBaPf.txt	tOvj20mKQeps5eaZrx5.txt
10.1.131.2	10.1.131.181	293.0 KB	text/plain	SMTP-1634775399.679752-782b5ee37076c4877d0477f4b723967c-FsBQ5z2vtZckLP24ih.txt	UA.txt
10.1.131.2	10.1.131.203	113.0 bytes	text/plain	SMTP-1634775399.565714-2816dc61b9c603d2e6833a3ac3a204db-F5AT9K3ltSw5Ebicad.txt	⚠ Unknown
10.1.131.2	10.1.131.192	293.0 KB	text/plain	SMTP-1634775397.739790-9146a408e7587c82ac60c3bb26cc7040-FnNtll8OlWx2Vdxca.txt	tXLAdaVD.txt
10.1.131.2	10.1.131.183	50.0 bytes	text/plain	SMTP-1634775397.317688-c9505fa46ec43a7521ed5af4d08f796e-FgxO1c3z3PFCXxRdhe.txt	⚠ Unknown
10.1.131.2	10.1.131.194	113.0 bytes	text/plain	SMTP-1634775397.144637-2816dc61b9c603d2e6833a3ac3a204db-FVRjlf2mNzLSZwxwYb.txt	⚠ Unknown
10.1.131.2	10.1.131.181	140.0 bytes	text/plain	SMTP-1634775396.410752-fc5c7ea21f189e8729b2622cf383c1dd-FxsPcs2LVeLcDoCBei.txt	⚠ Unknown
10.1.131.2	10.1.131.192	30.0 bytes	text/plain	SMTP-1634775396.020781-5746d5106b666155fa5811b23ad82df0-FtZja9vXYa82v1kwk.txt	⚠ Unknown

© Endace Technology Ltd. EndaceVision™ is a trademark of Endace Technology Ltd.

Traffic categorization

Together, EndaceVision and InvestigationManager leverage 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.



My Investigation

1 Data Source dp4-1:Main (rotation-file)

Filter Directionless IP is 10.1.131.2

Hi-Res 10 secs; 8 minutes ago

2021/10/21 0:16:33.206 (UTC) - 2021/10/21 0:16:43.206 (UTC)

Wed, Oct 20th 2021 at 5:28:53 (UTC) 🟩 Partial Metadata 16 hours, 29 mins 🟨 Partial Packet Data 18 hours, 55 mins 🟩 Full Metadata 16 hours, 29 mins 🟨 Full Packet Data 18 hours, 55 mins Thu, Oct 21st 2021 at 0:24:48 (UTC)

Bandwidth Note: Filters are not applied to this tool

Traffic Breakdown By Application Top 10 ordered by Bits Per Second

□	http	7 MB
□	cifs	2 MB
□	ssl	2 MB
□	smtp	2 MB
□	tcp	330 KB
□	ssh	53 KB

11 items

© Endace Technology Ltd. EndaceVision™ is a trademark of Endace Technology Ltd.

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.

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.

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 threat and issue resolution and starts organizations on the road towards automating the resolution of network security and performance issues.

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

For further information, email: info@endace.com