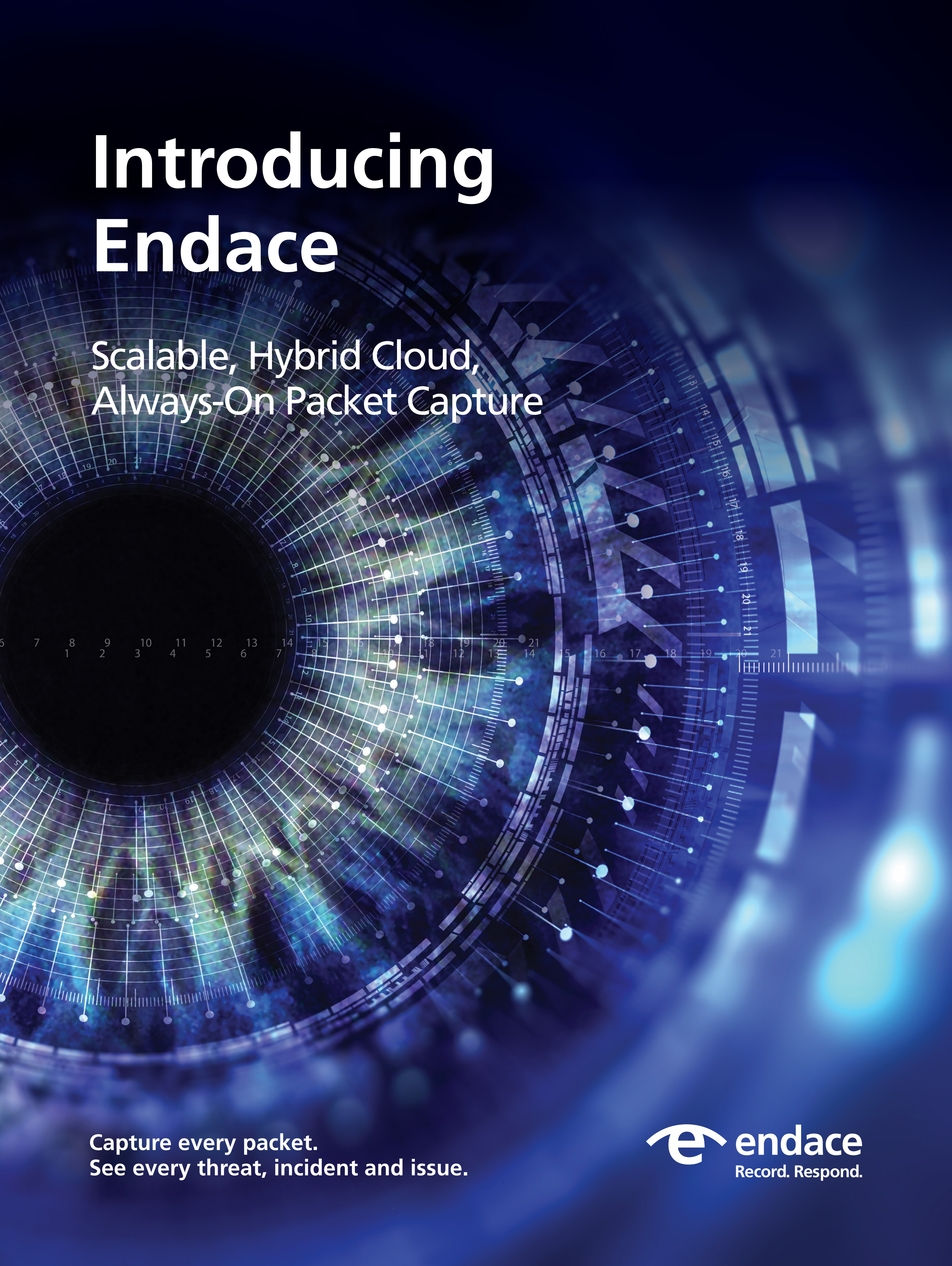


Introducing Endace

Scalable, Hybrid Cloud, Always-On Packet Capture

**Capture every packet.
See every threat, incident and issue.**

endace
Record. Respond.

The Truth is in the Packets

Packet capture provides complete visibility into every threat, issue, or incident. Because if it happened across the network, the definitive evidence of what took place is in the packets.

Endace's always-on, hybrid cloud packet capture brings clarity to every network activity from a central console. Giving all your teams and tools access to a single source of truth.

Cybersecurity

Packet capture provides hard evidence that enables security teams to hunt for and combat even the most serious threats.

With packet capture integrated into their preferred security tools, analysts can go directly from threats to evidence in a single click.

Network Operations

With access to a complete record of network activity, network operations can see exactly what's happening and troubleshoot and resolve network problems quickly before users and customers even notice.

IT and DevOps

IT and DevOps teams can quickly pinpoint the cause of application slowdowns or downtime with full visibility across the network.

> “You need to know what happened and how to fix it fast when something goes wrong, whether it’s a cyber-attack or a system failure. That’s where network packet data comes in. It gives you the detailed information you need to understand the problem and take action. Without it, you’re flying blind.”

Ron Ross
Fellow, National Institute of Standards and Technology (NIST)

> “Packets are the best source of truth for any network, and many IT teams lack this source of truth today.”

Shamus McGillicuddy
Vice President of Research, Enterprise Management Associates

> “The intrusions I’m dealing with today are increasingly complex. Packets are the ground truth for those intrusions – ‘PCAP or it didn’t happen!’. I never see t-shirts with ‘Endpoint or it Didn’t Happen!’ or ‘Logs or it Didn’t Happen!’”

“Malware” Jake Williams
Former Senior SANS instructor and incident response expert

> “In the world of cybersecurity, network packet data is the real deal. It’s the truth-teller. Attackers are savvy; they know how to cover their tracks, manipulate logs, and leave you scratching your head. That’s where packet data steps in as the ultimate truth-teller.”

Justin Fier
Senior VP, Red Team Operations, Darktrace

You need Always-On Packet Capture

Security threats or performance issues often take time to detect. Without recorded packet data it can be difficult or impossible to reconstruct exactly what took place.

Only always-on packet capture from across your hybrid cloud network - with the ability to record weeks or months of traffic - ensures security and network teams always have the definitive evidence they need for fast, accurate investigation and response.

Cybersecurity teams can:

- Conduct fast, effective threat hunting with definitive forensic evidence at their fingertips.
- Accurately confirm the scope and severity of threats, breaches and data exfiltration so they can respond quickly and confidently, and comply with reporting regulations.
- Test and validate Zero Trust implementations and security tool configurations to eliminate human errors.
- Defend against attacks on critical infrastructure – including OT and IoT devices – with complete visibility into all network activity.
- Automate and accelerate investigation and response with forensic evidence integrated into their security tools (IDS, SIEM, SOAR) and workflows.

Network Operations teams can:

- See all network activity across on-premise, hybrid and multi-cloud infrastructure.
- Quickly pinpoint the root cause of service-affecting network problems such as latency, routing issues, packet loss, jitter and more.
- Determine if the cause of performance issues is network or application related.
- Monitor network loads, identify bottlenecks and forecast growth.
- Investigate abnormal traffic that may reflect a security issue or network routing problem.
- Monitor QoS and SLA compliance.

IT and DevOps teams can:

- Monitor application performance across hybrid and multi-cloud network infrastructure.
- Determine if the cause of performance issues is network or application related.
- Investigate application security and application performance issues quickly.
- Gain visibility into the performance and security of both North-South and East-West application traffic.
- Validate application security.
- Monitor QoS and SLA compliance.

Triggered Packet Capture isn’t the answer

Some vendors pitch “triggered” or “smart” packet capture as a way to save money while delivering the same benefits as always-on packet capture. Here’s 4 reasons why that’s not a good idea:

1. You can’t trigger on things you can’t predict.

Triggered capture can’t capture packets relating to things like Zero Day Threats or attacks hiding inside legitimate traffic streams where there’s no known trigger. What you already know or can predict isn’t what’s beating you. It’s what you don’t know or can’t predict.

2. You can’t see the whole picture.

Packets relating to a trigger event don’t provide the full picture – they just provide the packets related to that specific trigger.

With Always-On Packet Capture you have the complete context around every threat or issue. So you can answer crucial questions such as “what happened before and after this event?”, “was any data stolen or modified?”, “was there lateral movement?”.

3. Record it the first time - you may never see it again.

Enabling packet capture after an event has already happened in the hope it will reoccur is unreliable. With security threats or attacks it’s unlikely that same activity will happen again.

If triggered packet capture missed recording an event first time around, you’ll be missing vital evidence.

4. Doesn’t comply with regulatory obligations.

Many organizations must comply with regulatory obligations to collect full packet capture data. For example, US Government Mandate M-21-31 stipulates that US Federal agencies must provide 72-hours of full packet capture when requested by FBI or CISA. Triggered packet capture won’t satisfy these regulatory obligations because it’s incomplete.

Endace's Always-On Hybrid Cloud Packet Capture

Our EndaceProbe's provide always-on, full packet capture across on-premise, private cloud and public cloud infrastructure.

EndaceProbes are modular and can be combined to create a recording fabric – EndaceFabric - capable of recording weeks or months of traffic on even the largest, most complex networks.

EndaceFabric provides centralized search and data-mining, API integration for fast access to recorded data, and a centralized management console for easy, cost-effective operations.

Secure by Design

EndaceProbes are deployed in some of the most critical networks on the planet. Designed from the ground-up to be highly secure, EndaceProbes are thoroughly tested to ensure they comply with the world's most stringent cybersecurity standards including **FIPS 140-3**, **NIAP NDcPP 2.2E** (Common Criteria) and **DoDIN APL**.

On-Premise EndaceProbes

EndaceProbe appliances are available in high-speed, high-capacity models for core network deployments and high-speed, compact models for deployment at the edge of your network or for remote/mobile deployments.

EndaceProbe appliances also provide hosting for a wide range of third-party, commercial and open source network and security monitoring and analytics tools including IDS and AI/ML detection.

Public and Private Cloud EndaceProbes

Virtual EndaceProbe appliances can be deployed in AWS and Azure public cloud environments, as well as in VMware or KVM private cloud environments.

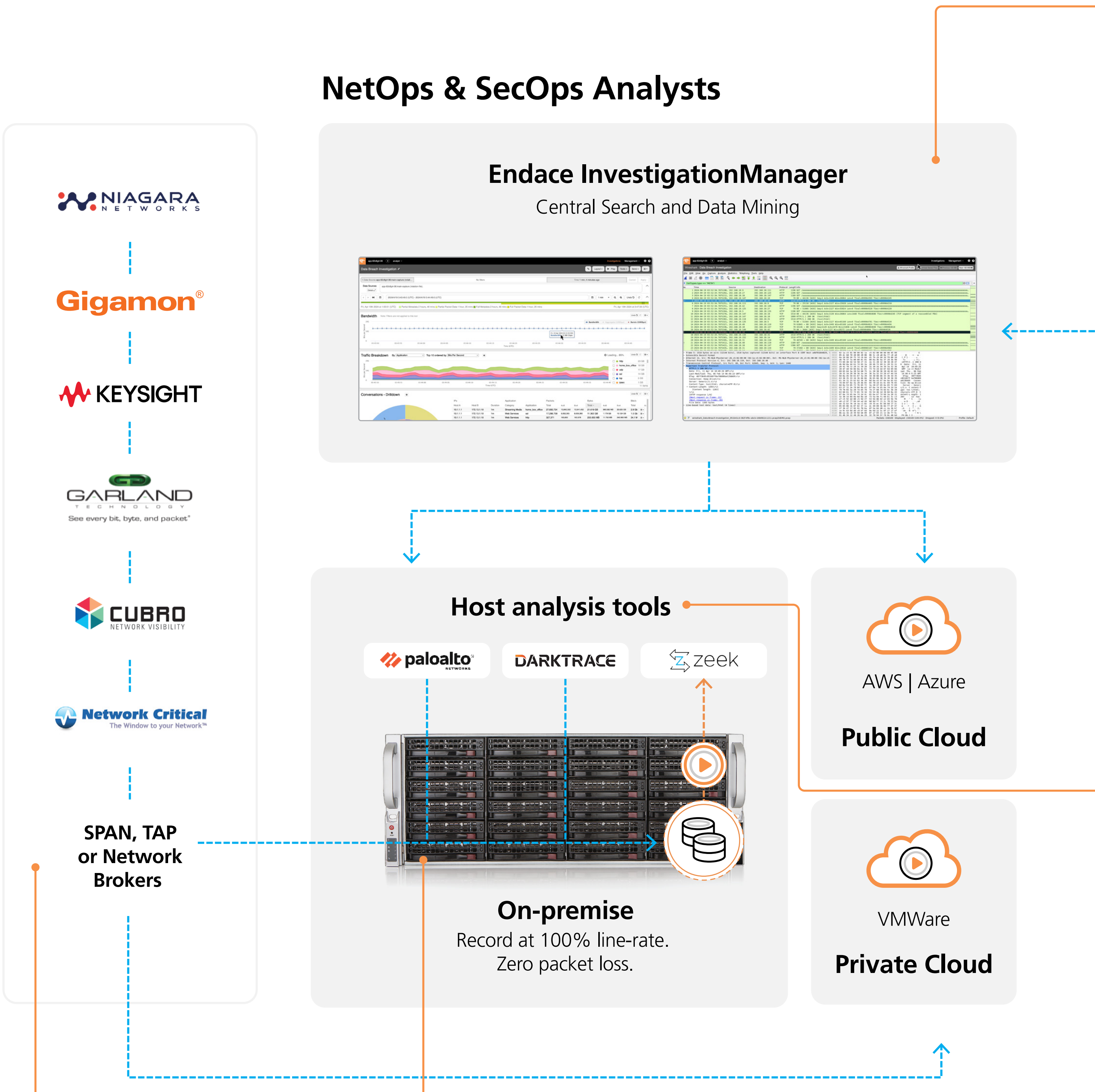
Central Search and Data-Mining

InvestigationManager is a Virtual Machine (VM) component that provides rapid, centralized search, data mining and API-based tool integration for estates of EndaceProbes. So you can easily make packet data available to all the teams that need access to reliable evidence, and integrate it into all their tools.

Centralized Management

EndaceCMS provides centralized fabric management for estates of on-premise and/or cloud-deployed EndaceProbes. Centrally monitor the health of the EndaceFabric components, apply configuration changes and updates and make it easy and cost-effective to manage estates of EndaceProbes.

How EndaceProbes Work



NetOps & SecOps Analysts

Endace InvestigationManager

Central Search and Data Mining

Host analysis tools

On-premise

Record at 100% line-rate.
Zero packet loss.

AWS | Azure

Public Cloud

VMWare

Private Cloud

SPAN, TAP
or Network
Brokers

1

Packet data is collected from Span ports, TAPs or Network Packet Brokers

2

Captured traffic is analyzed – using Deep Packet Inspection – indexed, and recorded to local storage.

3

InvestigationManager™ is a powerful, lightweight, virtual-server application that allows rapid search and data-mining across multiple EndaceProbes simultaneously.

4

InvestigationManager's powerful API integrates packet searching and datamining directly into security and performance monitoring tools - such as SIEMS, IDS, SOAR, NPM and APM - so analysts can stay in the workflow they know and go directly from alerts to related packet data with a single click.

API

Integrate with your Chosen toolset

- ACCEDIAN
- BLUVECTOR A COMCAST COMPANY
- CISCO
- corelight
- DARKTRACE
- elastic
- FORTINET
- IBM Security
- LINKSHADOW Combat the Dark
- paloalto NETWORKS
- Plixer
- Progress Flowmon
- splunk>
- sumo logic
- telchemy
- tines
- VECTRA

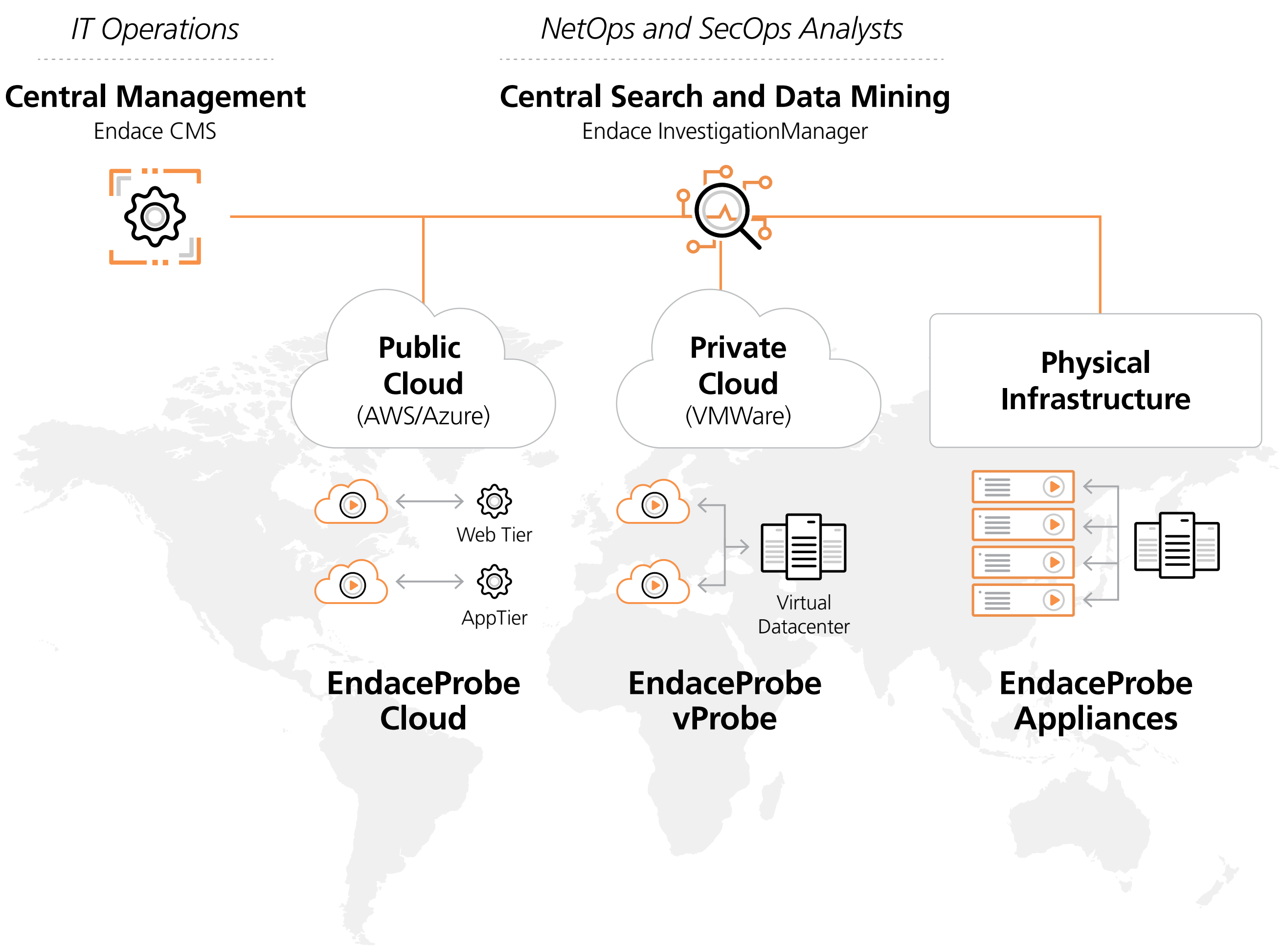
plus Open-Source Applications

- argus
- SNORT
- SURICATA
- WIRESHARK
- zeek

5

On-Premise EndaceProbes let you host a wide variety of commercial and open source tools that need access to packet data for real-time or post-event analytics. Allowing you to consolidate multiple functions onto a single platform to reduce cost and simplify deployment.

Unified Visibility Across On-Premise, Public and Private Cloud



IT Operations

Central Management
Endace CMS

NetOps and SecOps Analysts

Central Search and Data Mining
Endace InvestigationManager

Public Cloud
(AWS/Azure)

Private Cloud
(VMWare)

Physical Infrastructure

EndaceProbe Cloud

EndaceProbe vProbe

EndaceProbe Appliances

Industries we Serve

Endace's scalable, always-on packet capture solutions are used by some of the world's largest and most security-conscious organizations.

Here are some of the industries we operate in:

- Government
- Defense
- Enterprise
- Banking
- Healthcare
- Education
- Telecommunications
- Retail
- Energy

Trusted by the World’s Best

Experts in Packet Capture

For more than 20 years, Endace has been trusted by leading global customers and critical infrastructure providers to deliver highly scalable, reliable and accurate network recording solutions. Endace customers include Government, Defense, Telecommunications, Banking and Finance, Healthcare, Energy, and Fortune 1000 Enterprises.

Our packet capture solutions are recognized as industry-leading by our Technology Partners who integrate Endace’s packet capture technology into their products.

Partnerships that Deliver

Endace partners with the world’s leading security and networking vendors and open-source projects to integrate full packet capture directly into their solutions - giving you access to packet data from all your tools.

Meet our partners at endace.com/partners

argus	BLUVECTOR A COMCAST COMPANY	CISCO	corelight
CUBRO NETWORK VISIBILITY	DARKTRACE	elastic	FORTINET
GARLAND TECHNOLOGY	Gigamon	IBM Security	KEYSIGHT
LINKSHADOW Combat the Dark	Network Critical The Window to your Network	NIAGARA NETWORKS	paloalto NETWORKS
Plixer	Progress Flowmon	SNORT	splunk> a CISCO company
sumo logic	SURICATA	telchemy	tines
VECTRA	WIRESHARK	zeek	

Multi Award-Winners

Since its inception, Endace has consistently won industry awards and accolades for our world-class, innovative network packet capture and recording solutions.

Check out the list at endace.com/awards.

2024 Cloud Computing Winner Product of the Year

Global Infosec Awards Winner Cyber Defense Magazine 2024

Cybersecurity Breakthrough Award 2023

2023 Globee Awards Grand Winner Cybersecurity

2024 Globee Awards Gold Winner Cybersecurity

Top Infosec Innovator Winner Cyber Defense Magazine 2023

Cyber Security Excellence Awards Winner 2023

2023 Fortress Cyber Security Award

endace

Record. Respond.

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

endace.com