SOLUTION BRIEF

Cisco XDR with Endace Always-on Packet Capture

The Problem

Organizations need to find ways to simplify their security operation tools and processes. Security analysts need to shift from endless investigation to remediating the highest-priority incidents with greater speed, efficiency, and decisiveness.

Organizations need to unify visibility regardless of vendor or vector to uncover complex threats deploying tactics, techniques, and procedures to streamline incident response. They need to prioritize actions with AI and elevate productivity with automation and guidance.

Organizations typically lack sufficient visibility into what's happening on their networks. New, or more advanced, threats may not be detected and crucial evidence – such as packet data - may not be collected. This leaves organizations blind to potential threats and unable to properly understand or accurately reconstruct security events.

Organizations need a solution that:

- Brings your security stack together for endpoint, cloud, network, and email telemetry.
- Provides always-on packet capture (not triggered capture) to record every incident reliably and provide a trusted source of network evidence.
- Can be deployed across the organization's entire infrastructure – including on-prem, private and public cloud.
- Is easy to use and fast to implement.
- Leverages smart AI to streamline and accelerate incident triage, investigation and response.
- Can flex and scale to meet evolving needs and integrate easily with other security tools and platforms.

Benefits

- Unify visibility regardless of vendor or vector to avoid blind spots.
- Detect complex threats sooner.
- Prioritize threats by impact so you act on what truly matters.
- Accelerate response times and automate with evidence-backed recommendations.
- Streamline investigations.
- Always-on packet capture delivers a complete history of network activity.
- Definitive evidence trail with an accurate record of all relevant packets related to any threat.
- Full threat visibility across the entire network with on-prem, private and public cloud deployment options.
- Robust security with FIPS 140-3 validation. Listed on DoDIIN APL.

The Solution

By combining the open Cisco XDR solution with Endace's open, always-on, packet capture platform, organizations can improve their threat detection, incident response, threat-hunting, and investigation accuracy with deep, historical visibility into threat activity across their entire network infrastructure – on-prem, private and public cloud.

Cisco XDR makes defenders more effective and efficient by detecting even the most sophisticated attacks more

accurately and using AI to prioritize incidents across multiple security controls. It's one of the fastest, easiest ways to achieve unified threat detection, investigation, and response (TDIR) and elevate your security posture.

Cisco XDR streamlines incident response by simplifying the incident lifecycle. It integrates with other security tools to provide a holistic view of the environment and streamlines the investigation process allowing analysts to quickly and accurately understand the scope and impact of an incident and respond faster to stop threats before they escalate.

EndaceProbes can record and store days, weeks, or even months of full packet capture data from on-prem, public, or private cloud environments. This provides security teams with a definitive, comprehensive record of network activity, giving them the clear evidence needed to understand exactly what occurred on the network.

Multiple EndaceProbes (including on-prem appliances and virtual private or public cloud instances) can be connected to form a unified, hybrid cloud recording fabric. This fabric provides rapid, centralized search, data mining, and analysis of recorded traffic including file extraction and rich metadata generation - including NetFlow/IPX and extended log data (using Zeek).

Integrating Cisco XDR with EndaceProbes gives analysts evidence at their fingertips so they can drill-down from any incident to the related traffic and examine right down to packet level with a single-click.

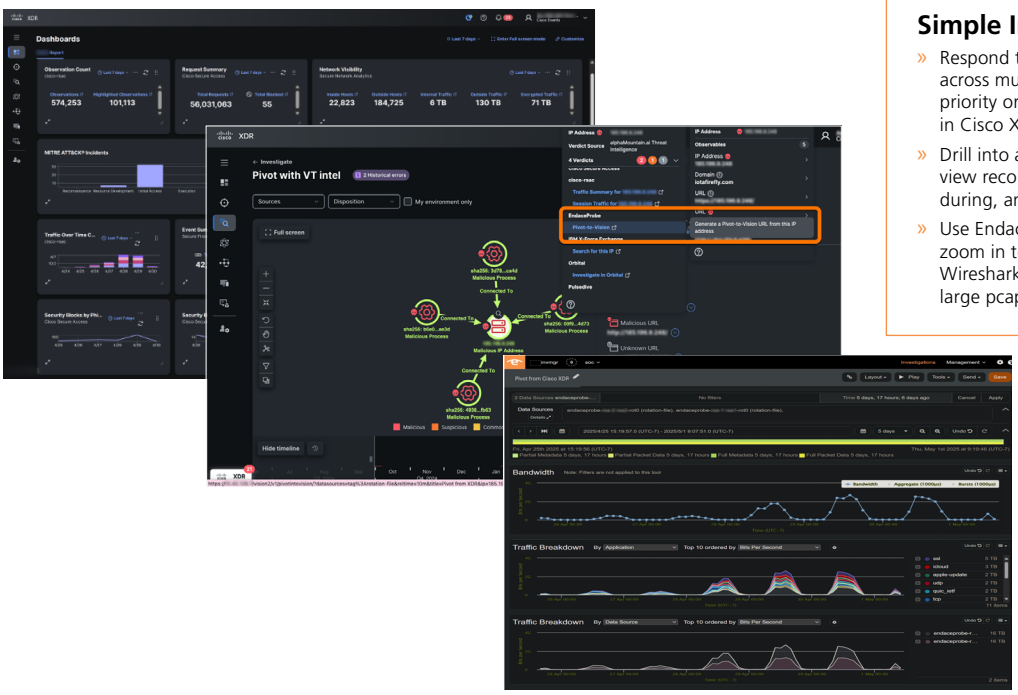
Conclusion

Cisco XDR combined with EndaceProbe and EndaceProbe Cloud's 100% accurate network packet capture provides the industry's most open and scalable XDR and integrated network security forensics solution for on-prem and cloud infrastructures.

These two best-in-class solutions deliver sophisticated threat detection, network-wide traffic analysis and inspection, streamlined incident investigation and response and the deep forensic evidence necessary to address any security threat.

Security teams can defend against even advanced threats with the confidence of knowing their responses are based on the definitive network evidence only full packet data provides.

How it works



Simple Integration Workflow

- Respond to correlated incidents detected across multiple security products, presented in priority order and including attack diagrams, in Cisco XDR.
- Drill into any event or IP address and click to view recorded packet-level evidence before, during, and after the event.
- Use EndaceVision to analyze traffic and zoom in to directly view packet payloads in Wireshark without the need to download large pcap files.

Solution Components

- Cisco XDR with Advantage license.
- EndaceProbe, EndaceProbe. Cloud, EndaceProbe vProbe.