Vectra and Endace
The Right Data with the Right Context

Challenge

Despite multiple layers of cybersecurity defense such as next-generation firewalls, IDSSs, and AI security solutions, cyberattackers still get past to gain access into enterprise networks. Without visibility into what’s happening inside the network perimeter, it’s impossible to detect and defend against these attacks.

Solution

Together, Vectra and Endace provide rich insight into attacks across cloud, data centers, IoT devices, and enterprise networks.

Vectra’s threat detection and response platform delivers powerful analysis and detection that perfectly complements the EndaceProbe™ Analytics Platform’s always-on packet capture. By combining Vectra’s Platform and EndaceProbes, analysts have powerful threat detection coupled with the detailed forensic evidence they need to detect, investigate, and respond to cyberthreats and attacks quickly and definitively.

Vectra’s platform leverages a unique combination of data science, machine learning, and behavioral analysis to detect attacks at all phases – such as internal reconnaissance, command and control, lateral movement and data exfiltration. Over time, Vectra’s platform understands the naturally occurring communities in the network and continuously listens, thinks, and learns to adapt to the ever-changing threat landscape.

Vectra’s platform automatically detects cyberthreats – even those hidden in approved applications or encrypted traffic – and correlates these threats to the hosts that are under attack, delivering unique context about what attackers are doing. This gives IT security teams the insight they need to quickly identify, prioritize, and respond to the threats that pose the greatest danger.

The EndaceProbe Analytics Platform’s always-on network recording captures, indexes, and stores a 100% accurate record of traffic on the network. This comprehensive, packet-level forensic evidence lets security teams quickly investigate the threats that the Vectra platform detects so they can respond faster to stop attacks.

Efficient Investigation and Threat Hunting

The Network History recorded by EndaceProbes can be fully integrated into the Vectra platform’s workflows using the EndaceProbe’s Pivot-To Vision™ integration. This integration lets security analysts pivot from alerts in Vectra’s platform directly to EndaceVision™, the EndaceProbe’s built-in investigation tool, to analyze the packet-level Network History related to the event. Pivot-to-Vision uses the IP address and time range of the trigger event to rapidly dissect, review, and extract the relevant traffic from amongst petabytes of Network History recorded on the network. It supports analysis to microsecond level detail, with views filtered by Application, IP, Protocol, Top Talkers, and many other parameters, providing rapid insights and enabling accurate conclusions.

Directly accessing the related packets with a single click lets security analysts quickly discover the root cause of issues as they are threat hunting in their environment. They can respond rapidly to threats, dramatically reducing the time to resolve critical incidents and minimizing the risk of security threats from escalating to become more serious breaches.

Conclusion

Combining the Vectra platform with the EndaceProbe’s 100% accurate Network History delivers more effective threat detection, greater visibility into attack activity, and definitive evidence that enables SecOps teams to combat numerous and sophisticated attacks.

Integrating the two technologies empowers security teams to respond to alerts and investigate threats with speed and confidence.

PRODUCTS

• Vectra Threat Detection and Response Platform
• EndaceProbe Analytics Platform

BENEFITS

• Vectra’s platform automatically and in real time, detects in-progress cyber attacks that evade prevention security defenses and spread inside networks.
• Vectra’s platform combines data science, machine learning, and behavioral analysis to detect all phases of a cyber attack.
• Streamlined investigation workflows give SecOp teams one-click access to definitive evidence, accelerating the investigation and remediation of threats.
• Definitive evidence trail with an accurate record of all relevant packets.
How It Works

Figure 1. From alerts in the Vectra platform, you can drill-down directly to related packets in EndaceVision.

Figure 2. From EndaceVision you can use filters and views to analyze the traffic related to the event, zoom in or out on the timeline to view precursor or post-event activity and decode and analyze packets in a hosted instance of Wireshark directly on the EndaceProbe without needing to download a pcap.

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