SOLUTION BRIEF

Fortinet FortiNDR and Endace

Advanced Network Detection and Response with Endace's Always-on Network Packet Capture

endace
Record. Respond.

FORTINET

The Problem

There are many Network Detection and Response (NDR) tools on the market that help customers identify and find threat actors and malicious activity so security teams can quickly isolate, contain, and remediate cyber breaches. The most serious threats and issues require in-depth packet evidence to connect the dots and expose exactly what's happening before, during, and after any event, allowing you to confidently respond, remediate, and report.

However, many teams lack the confidence and experience to search and analyze packet capture data when responding to threats. When logs and events have been wiped, manipulated, or just lack the essential details, always-on network packet capture gives you a tamper-proof record of all activity across all your entire network, allowing you to fully understand any threat so you can respond appropriately. Packet capture workflow integration with your NDR analysis platform is crucial in helping team members with fast search and easy analysis of packet data when dealing with serious threats.

Organizations need a solution that:

- Provides always-on packet capture (not triggered capture) to record every incident reliably.
- Can be deployed across the organization's entire infrastructure – including on-prem, private and public cloud.
- Delivers the required functionality while being easy to use and fast to implement.
- Can integrate with other security solutions (e.g. AI-ML solutions, SIEM, NGFW) and workflows that you use.
- Has the flexibility to change and scale easily to meet evolving needs.

Benefits

- Always-on recording to capture all traffic. Store weeks or months of full packet capture data for a complete record of network activity.
- Streamlined investigation workflows from FortiNDR, FortiNDR Cloud and FortiSIEM, with one-click access to full definitive packet evidence, accelerates investigations and enables accurate event reconstruction.
- Definitive evidence trail with an accurate record of all relevant packets related to any threat.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- Expose Zero-day threat risk by playing back historical traffic to threat detection tools using updated rules.
- Full visibility across complex networks, including Hybrid and Multi-Cloud and visibility into encrypted traffic.
- FIPS and NIAP compliant for military-grade security.

The Solution

By combining FortiNDR and/or FortiNDR Cloud with Endace's always-on packet capture, organizations improve their incident response, threat-hunting, and investigation accuracy with historical visibility into threat actor activity on their on-prem and cloud networks.

FortiNDR and FortiNDR Cloud, part of the Fortinet SecOps Platform, give your security team the ability to detect, prioritize, investigate, hunt, and respond to attacks across your network. Through the power of AI-based detections and expert analysis, security teams can spot evidence of attacker behavior early, enabling effective response across your IT/OT/IoT environments.

FortiNDR and FortiNDR Cloud leverage AI/ML, behavioral, and human analysis to analyze network traffic, including encrypted traffic, to detect malicious behavior while reducing false positives. FortiNDR solutions allow security teams to pivot from detection to investigation to threat hunting with a few clicks. Providing integrations with the Fortinet Security Fabric and EndaceProbes, FortiNDR solutions ensure you can automate investigation, triage, and remediation with the benefit of complete and accurate network forensic data.

EndaceProbes can record and store days, weeks or months of full packet capture data from on-premise, public or private cloud environments. Multiple EndaceProbes (including on-prem and cloud probes) can be connected to provide a unified, hybrid cloud recording fabric. This fabric enables rapid, centralized search, data-mining and analysis of recorded traffic, and supports streamlined "one-click" user workflows directly from within FortiNDR, FortiNDR Cloud, FortiSIEM, and other security tools, directly to the related packet evidence on EndaceProbes. This enables enable faster, more efficient investigation and resolution of network security and performance issues.

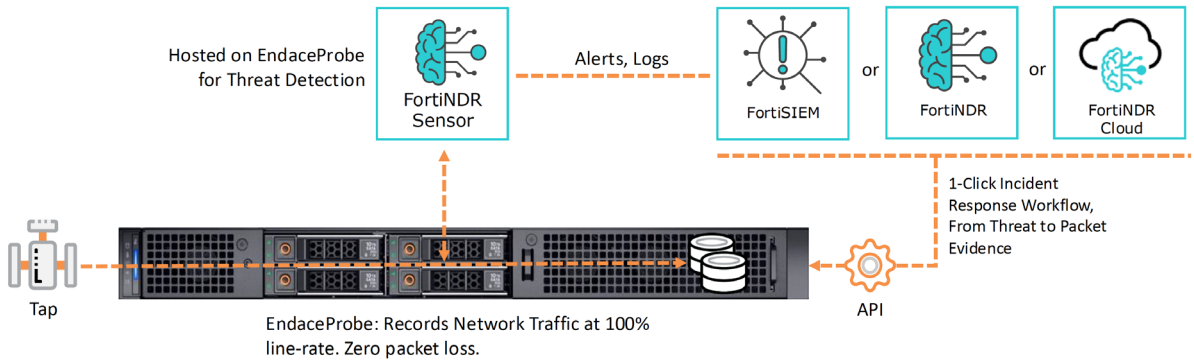
The EndaceProbe's Application Dock hosting capability also enables rapid deployment of FortiNDR sensors without deploying new hardware. With FortiNDR sensors hosted in Application Dock, every packet captured and recorded by the EndaceProbe can also be streamed to FortiNDR for real time for analysis.

EndaceProbes are designed to ensure system resources used for capture and recording are separated from the resources used by hosted applications. This means capture performance is never impacted by hosted applications and vice- versa, guaranteeing 100% accurate recording even when the hosted FortiNDR sensor is processing heavy traffic loads.

Conclusion

Combining FortiNDR, FortiNDR Cloud and FortiSIEM with Endace's 100% accurate, always-on packet capture delivers network-wide traffic analysis, inspection, filtering and always-on recording. SecOps and NetOps teams get the definitive evidence at their fingertips that they need to conduct successful investigations and defend against even the most advanced threats.

How it works



Solution Components

- FortiNDR and/or FortiNDR Cloud
- EndaceProbe™ Always- On Packet Capture for On-Prem and Cloud environments
- Optionally FortiSIEM