SOLUTION BRIEF

endace
Record. Respond.

FORTINET

# Accelerate Security Investigations with Fortinet NGFW, FortiSIEM and Endace Always-on Network Packet Capture

## The Problem

SOC Teams are overwhelmed by the volume and variety of alerts they receive from their security tools and the time it takes to collate data from system, authentication and application logs and other telemetry sources so they can investigate these alerts properly, meaning the risk and severity of many threats is never fully determined.

Unlike log files - which may have been wiped or modified by an attacker, or may simply fail to record crucial activity– full packet data provides a complete and accurate record of every network activity.

For analysts to properly investigate serious threats and issues they need access to in-depth packet evidence. Only full packet data enables them to definitively connect the dots and expose exactly what happened before, during, and after events, so they can respond, remediate and report on them quickly and accurately.

Organizations need a solution that:

- Provides always-on packet capture to reliably record every incident.
- Can be deployed across the organization's entire infrastructure – including on-premise, private and public cloud.
- Delivers the required functionality while being easy-to- use and fast to implement.
- Can integrate with existing security solutions and workflows
- Has the flexibility to change and scale easily to meet evolving needs.

## The Solution

By combining FortiGate and FortiSIEM with Endace's always-on packet capture, organizations ensure they have conclusive forensic evidence for fast, accurate investigation and response and effective threat hunting across on-premise and cloud environments.

Fortinet's security-driven networking strategy tightly integrates an organization's network and security architecture, enabling the network to evolve and grow without compromising security operations.

## 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 FortiSIEM with one-click access to full definitive packet evidence, accelerates investigations, and enables accurate event reconstruction.
- Definitive evidence trails with an accurate record of packets related to any threat.
- Reduce threat exposure through greater analyst productivity and faster incident investigation and response.
- Playback recorded packet data to determine Zero Day threat exposure or reanalyze historical incidents.
- Full visibility across Hybrid/Multi Cloud networks, including visibility into encrypted traffic.
- FIPS and NIAP certification for security.

FortiGate NGFWs deliver industry-leading enterprise security for any edge, at any scale, with full visibility and threat protection.

FortiSIEM combines visibility, correlation, automated response, and remediation in a single, scalable solution.

EndaceProbes can record and store weeks or months of full packet capture data from on-premise, public or private cloud environments. Multiple EndaceProbes can be connected to provide a unified, hybrid cloud recording fabric that enables centralized search, data-mining and analysis of recorded traffic, and integrates directly into security tools from Fortinet (and many other vendors) to streamline and automate investigation workflows.

The EndaceProbe's Application Dock hosting enables new security solutions to be deployed wherever EndaceProbes are connected to the network without requiring new hardware to be rolled out. This allows organizations to quickly respond to changing needs without time-consuming and costly hardware rollouts.

With FortiGate NGFWs hosted in Application Dock, every packet captured and recorded by the EndaceProbe can also be streamed to FortiGate in 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.

## Conclusion

The combination of FortiGATE and FortiSIEM and Endace's scalable, always-on packet capture provides a powerful solution for protecting against even the most advanced threats.

SecOps teams gain access to definitive forensic evidence at their fingertips, enabling them to quickly investigate and respond to attacks early in the kill chain before they have a chance to escalate and become more serious.

## How it works

**Figure 1:** Events detected by FortiGate NGFW appliances and/or other security protection and monitoring tools are collected and collated in FortiSIEM.

**Figure 2:** From any event in FortiSIEM, analysts can drill down with a single click to view the related traffic in EndaceVision, Endace's powerful traffic analysis tool.

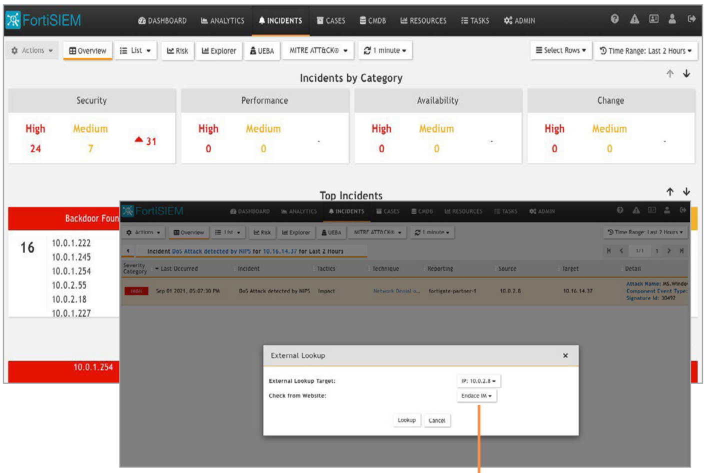
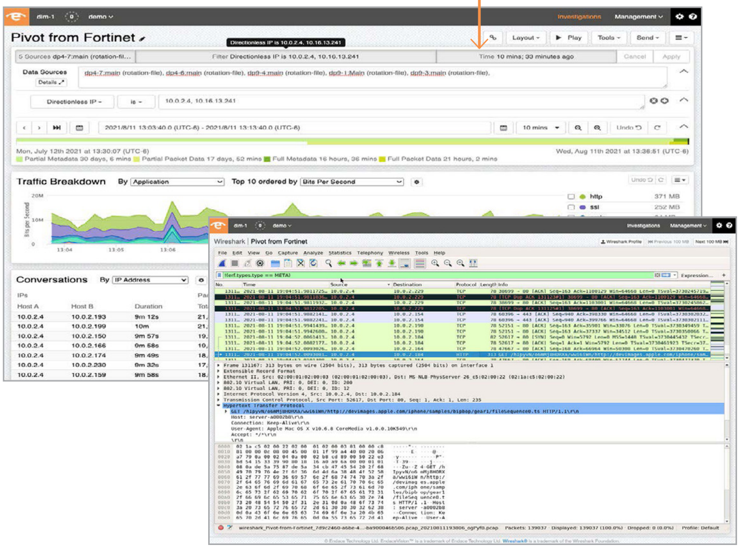


**Figure 3:** In EndaceVision analysts can apply filters and tools to examine the traffic, zoom in or out on the timeline, and analyze the packet data (without needing to download pcap files) using the built-in hosted Wireshark. If desired, pcaps can also be downloaded for analysis using other tools, or for archival.



### Solution Components

- FortiGate NGFWs
- FortiSIEM
- EndaceProbe™ Always-On Packet Capture for On-Premise and Cloud