SOLUTION BRIEF

Fortinet and Endace Security Solution

Accelerate Your Security Investigations With Fortinet and Endace Network History

Executive Summary

Integrating Fortinet FortiGate Next-Generation Firewalls (NGFWs), Fortinet FortiSIEM, and EndaceProbe Network History provides security threat detection, correlation, automated response, and remediation in a single, scalable solution. Defend against even the toughest threats by giving the entire security operations center (SOC) team access to rich, contextual, network evidence for fast and accurate decisions.

Customer Challenges

Distributed applications, web and mobile applications, cloud services, and ubiquitous internet access have all delivered unparalleled flexibility and power. But complex network and application architectures have made it increasingly difficult to ensure the security, reliability, and performance of networks and the applications that run on them.

In the event of a security breach or cyberattack, it can often be difficult to quickly determine exactly what happened, how it happened, and what was compromised. And organizations frequently find themselves frustrated by costly application performance problems and network outages that reduce productivity and impact badly on reputation and customer experience. Tracking down the root cause of these problems can be frustratingly slow and time-consuming, and represents a key challenge for many organizations.

Joint Solution

Endace and Fortinet have partnered to deliver an industry-leading security solution to address these challenges. The integration of EndaceProbe Network History and Fortinet FortiGate Next-Generation Firewalls and FortiSIEM, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers security threat detection, correlation, automated response, and remediation in a single, scalable solution.

Fortinet's security-driven networking strategy tightly integrates an organization's network infrastructure and security architecture, enabling the network to evolve and grow without compromising security operations. FortiGate NGFWs deliver industry-leading enterprise security for any edge, at any scale, with full visibility and threat protection.

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

Joint Solution Components

- Fortinet FortiGate NGFWs, Fortinet FortiSIEM
- EndaceProbe Analytics Platform

Joint Solution Benefits

- Streamlined investigation workflows from FortiSIEM with one-click access to full 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
- Zero-day threat risk validation with recorded network playback and threat analysis
- Unparalleled security protection with FortiGate NGFW and the Fortinet Security Fabric

FABRIC-READY

EndaceProbe™ Analytics Platforms capture, index, and store network traffic with 100% accuracy, regardless of network speeds, loads, or traffic types. This recorded Network History provides the definitive evidence SecOps and NetOps teams need to quickly and accurately investigate and respond to security threats and performance issues.

The EndaceProbe's Application Dock™ hosting capability extends security and performance monitoring by allowing third-party analytics applications—including the FortiGate VM NGFW virtual appliance—to be hosted on the open EndaceProbe platform. Hosted tools can analyze and inspect recorded traffic in real time at full line-rate or analyze recorded Network History for back-in-time investigations.

Hosting FortiGate VM NGFW virtual appliances on EndaceProbes enables customers to expand monitoring on-demand without rolling out additional hardware. SOCs now have the flexibility needed to quickly adapt to changing needs.

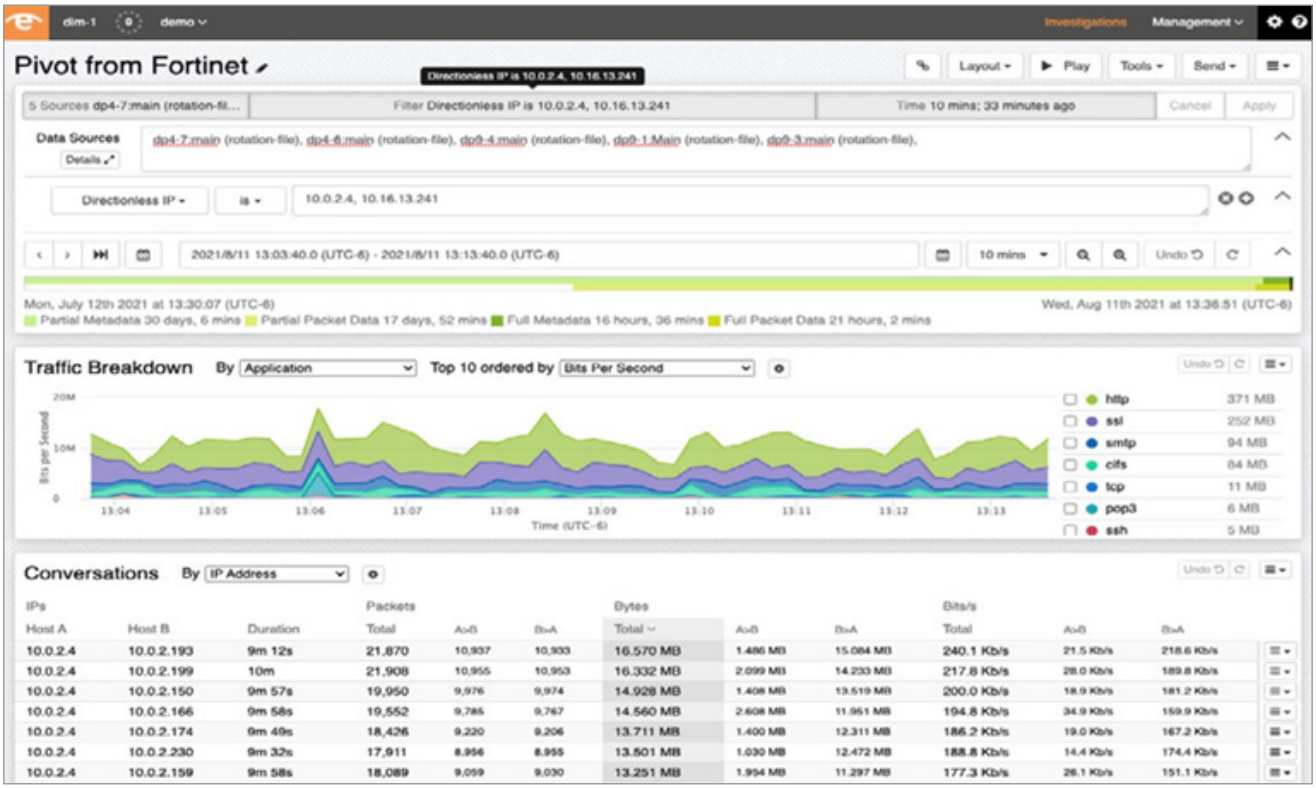

Figure 1: From any detected event in FortiSIEM, analysts can drill down with a single click to view the related traffic in EndaceVision.

Fast, Accurate Security Investigation and Threat Hunting

The full Network History recorded by EndaceProbes is integrated into Fortinet users' workflows using the Pivot-To-Vision™ function of the EndaceProbe API. Pivot-To-Vision lets security analysts pivot from security events detected by Fortinet directly to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History.

From FortiSIEM, security teams can pivot from threat indicators directly to related network packet data in EndaceVision. EndaceVision lets them dissect, review, and extract relevant traffic from within petabytes of Network History recorded on EndaceProbes deployed on the network. Analysts can examine traffic down to microsecond-level detail, with views filtered by Application, IP, Protocol, Top Talkers, and many other parameters.

Direct access to related packets with a single click lets security analysts rapidly identify the root cause of issues they are investigating. They can respond quickly, to dramatically reduce the time to resolve critical incidents and minimize the risk of security threats escalating to serious breaches.

Rapid Deployment With Application Dock

Deploying advanced security hardware can take significant planning, time, and effort. These extended deployment time frames put security teams at a disadvantage when trying to defend against criminals who can launch attacks at the click of a mouse. The ability to rapidly deploy new or upgraded security tools onto an existing hardware platform redresses this imbalance, allowing organizations to quickly respond to changing needs without time-consuming and costly hardware rollouts. The EndaceProbe's Application Dock hosting capability enables rapid deployment without the need to deploy new hardware.

With FortiGate NGFWs hosted in Application Dock, every packet captured and recorded by the EndaceProbe can also be streamed to FortiGate for real-time 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 FortiGate NGFW is processing heavy traffic loads.

Summary

Combining Fortinet Network Security with the EndaceProbe's 100% accurate Network History delivers networkwide traffic analysis, inspection, filtering, and always-on recording. SecOps and NetOps teams get the definitive evidence they need to conduct successful investigations and defend against even the most advanced threats.

About Endace

Endace specializes in high-speed, scalable packet capture for cybersecurity, network and application performance. The open, EndaceProbe Analytics Platform lets customers record a 100% accurate history of activity on their network and can host network security and performance monitoring tools that need to analyze real-time or historical traffic. Endace's Fusion Partners provide pre-built integration with the EndaceProbe platform to accelerate and streamline incident investigation and resolution.

September 23, 2021 4:35 AM
1270470-0-0-EN