

# Fortinet and Endace



## Accelerate your security investigations with Fortinet and Endace Network History

Integrating FortiGate™ Next-Generation Firewalls, 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 SOC team access to rich, contextual, network evidence for fast and accurate decisions.

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.

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 FortiGate Virtual NGFW - 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.

### 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.

### PRODUCTS

FortiGate NGFWs

FortiSIEM

EndaceProbe Analytics Platform

### BENEFITS

- Streamlined investigation workflows from 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.
- Simple threat investigation workflow from the FortiSIEM UI.
- Zero-day threat risk validation with recorded network playback and threat analysis.
- Hardware deployment efficiency leveraging your EndaceProbe packet capture appliance to host FortiGate-VM NGFW virtual appliances.
- Unparalleled security protection from the FortiGate and the Fortinet Security Fabric.

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 takes significant planning and effort. Extended deployment timeframes 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 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 FortiGate NGFW is processing heavy traffic loads.

## Conclusion

Combining Fortinet Network Security with the EndaceProbe's 100% accurate Network History delivers network-wide 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.

## Example Deployment Architecture

Figure 1: Events detected by FortiGate NGFW appliances are collected and collated in FortiSIEM. FortiGate-VM NGFWs can be hosted on EndaceProbes in IDS mode to extend monitoring footprint.

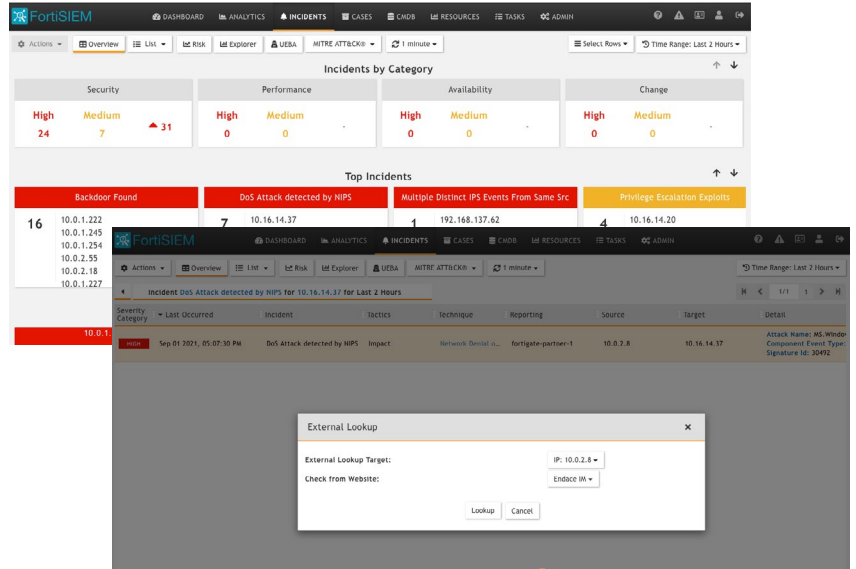
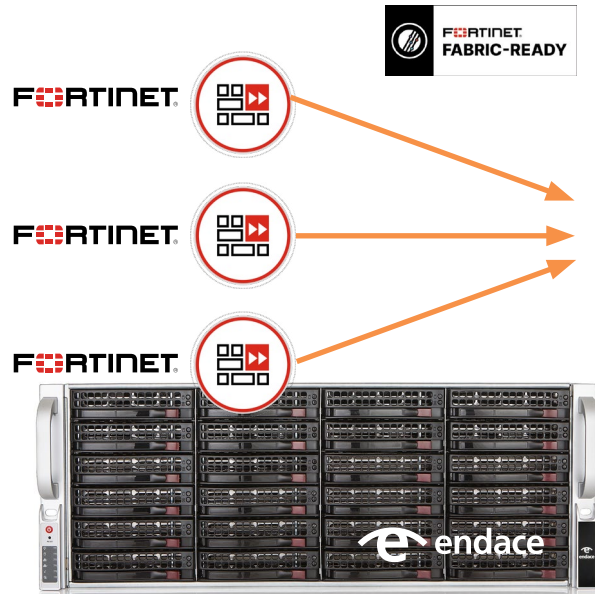


Figure 2: From any detected event in FortiSIEM, analysts can drill down with a single click to view the related traffic in EndaceVision.

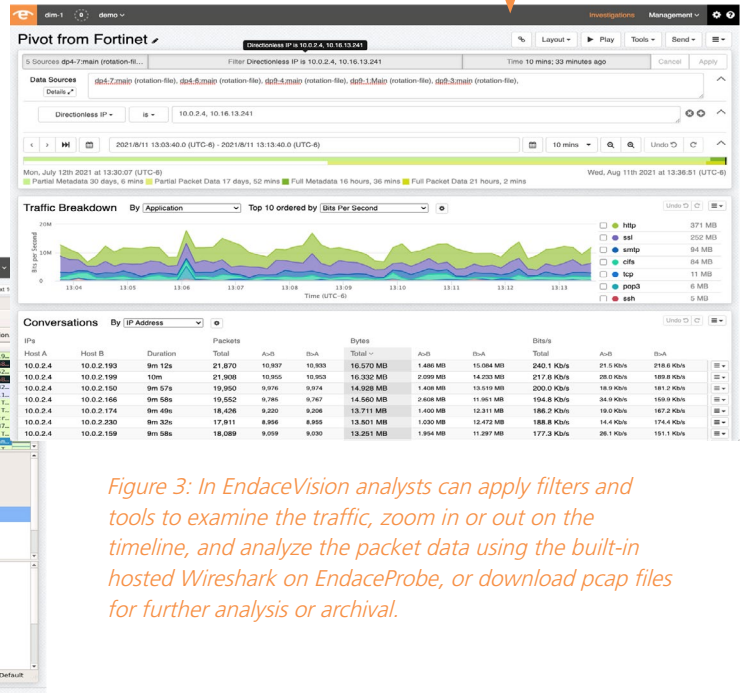


Figure 3: In EndaceVision analysts can apply filters and tools to examine the traffic, zoom in or out on the timeline, and analyze the packet data using the built-in hosted Wireshark on EndaceProbe, or download pcap files for further analysis or archival.