DATASHEET

Fidelis Network with Azure Virtual Network TAP

Azure Cloud Threat Detection, Threat Hunting and Data Loss/Theft Detection

Enable Cloud Network Traffic Analysis

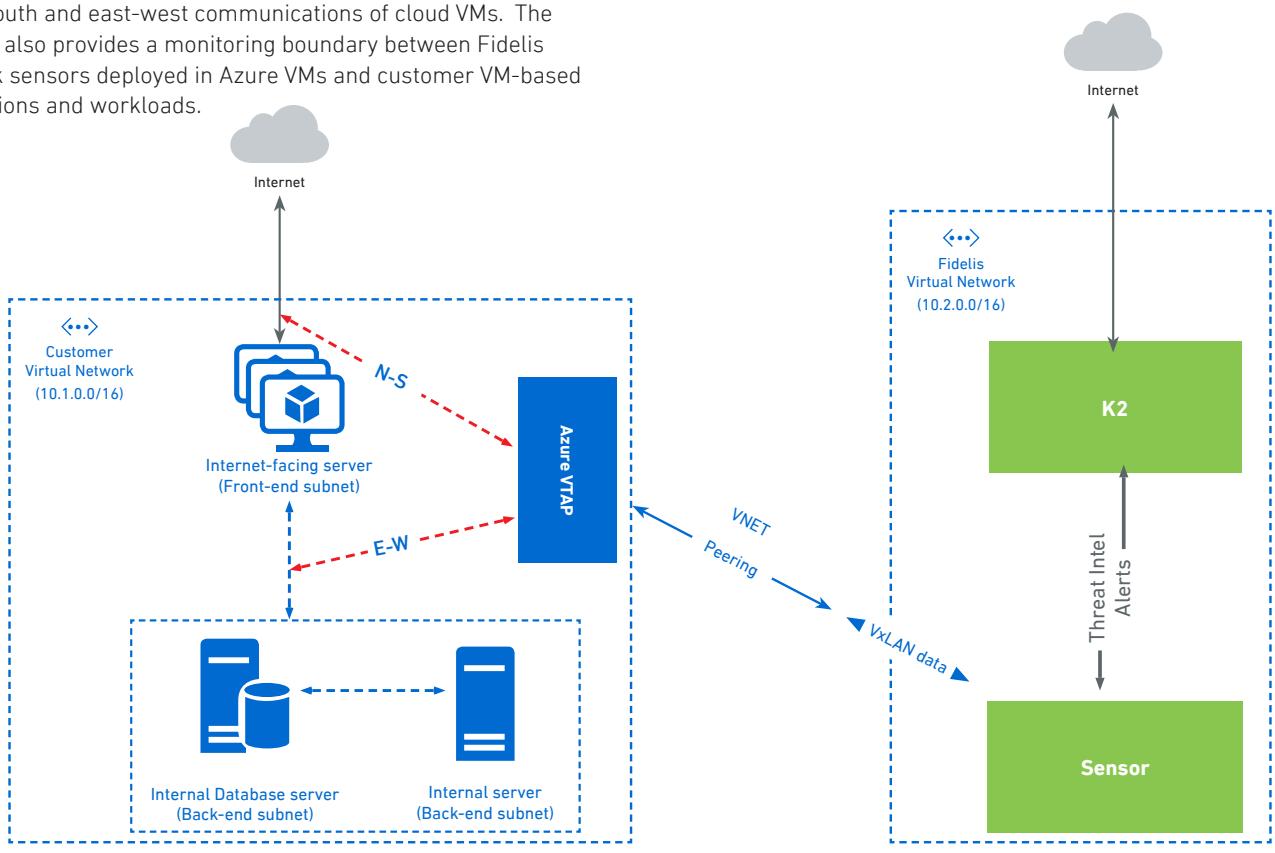
Enterprise security operations are complex, with siloed visibility across networks, endpoints, and cloud environments, combined with too many tools for understaffed and overwhelmed teams to manage. Security teams need bi-directional visibility into network traffic across all ports and protocols and need valuable metadata to analyze threats and data leakage. This comprehensive visibility combined with contextual threat intelligence leads to detections across the entire threat life cycle. This also allows organizations to respond quickly and effectively to malicious activity at every stage of the kill chain and mitigate data leakage and exfiltration.

Solution Overview

Customers of Fidelis Network enabling the Microsoft Azure Virtual Network TAP can quickly deploy cloud network traffic analysis for north-south and east-west communications of cloud VMs. The solution also provides a monitoring boundary between Fidelis Network sensors deployed in Azure VMs and customer VM-based applications and workloads.

Solution Benefits – Visibility, Simplicity, Speed

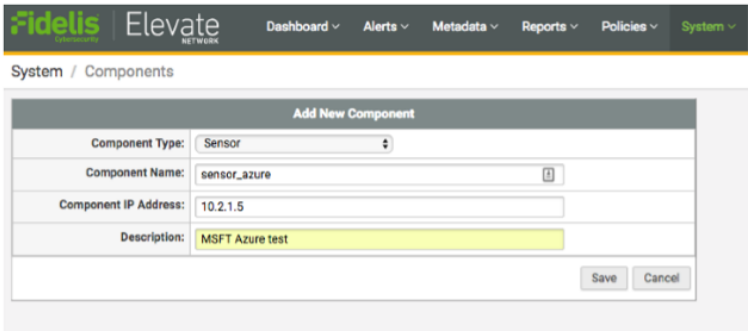
- **Visibility -** Azure Virtual Network TAP provides visibility to application and VM traffic for north-south communications, often through web front ends, and east-west traffic often between back end VM process workloads and databases.
- **Simplicity -** Azure Virtual Network TAP does not require any third -party agents and directly communicates with cloud-hosted Fidelis Network sensors across VNETs where the sensors are segmented from VM owners in a monitoring boundary.
- **Speed -** Fidelis Network VM sensors can each analyze up to 2Gbps on network traffic with no data sampling or packet drops, so every port and protocol is fully analyzed with Deep Session Inspection (DSI).



Azure Virtual Network TAP is a first of its kind cloud native network traffic monitoring solution.

Azure Virtual Network TAP – First of its kind direct native cloud VM monitoring network tap of north-south and east-west communications for VM based web front ends, process workloads and databases as examples. No third-party agents are required, and security monitoring is segmented from VM owners in a monitoring boundary using VNET peering.

- First native Network Virtual TAP for cloud scale monitoring
- Monitors north-south and east-west communications of Azure VMs
- Monitoring boundary between SecOps and VM owners
- No third-party agents required

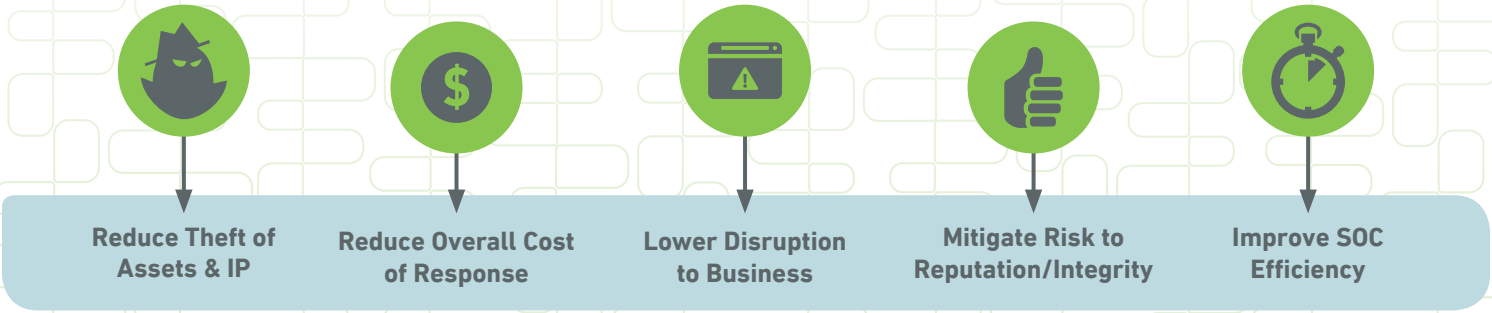


Easily add Azure VM sensors to accept VxLAN data via VNET peering from the Azure Virtual Network TAP.

Fidelis Network - Get direct cloud-based traffic analysis of Azure VMs via the Azure Virtual Network TAP including north-south and east-west VM communications via VNET peering to Fidelis Network VM hosted sensors. Analysis of traffic using Deep Session Inspection (DSI) includes hundreds of metadata attributes and custom tags for real-time and retrospective analysis for threat detection, threat hunting and data loss and theft detection. Fidelis also provides a Managed Detection and Response (MDR) service for 24/7 cloud monitoring of Azure VMs with proactive incident response (IR) services.

- Fidelis Network includes direct, internal, cloud, email and web sensors for unmatched visibility for hybrid multi-cloud networks.
- Deep Session Inspection (DSI) of Azure cloud VM-based communications for all ports and protocols to analyze sessions, content, and obfuscated files and archives.
- Cross session and multi-faceted analysis, plus machine learning anomaly detection enable real-time and retrospective analysis for threat detection, threat hunting and data loss and theft detection. Security analysts can query, pivot and hunt on content and context.
- Metadata for hundreds of attributes and custom tags with the ability store up to 360 days within cloud or on-premises providing content and context not seen in firewall logs or SIEM dashboards.
- 10Gbps appliance sensor and 2Gbps VM sensor analysis capacity with no data sampling or packet drops, multi-sensor configurations scale with network performance requirements.
- Fidelis Insight provides threat intelligence based on threat research team (TRT) research and analysis, plus multiple threat intelligence feeds.
- Expand to Fidelis Elevate with endpoint detection and response (EDR) and deception for a complete threat detection, threat hunting and data loss and theft detection platform or managed service.

Benefits



Contact Us Today to Learn More About Fidelis

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis is the leader in automated detection and response. The Fidelis Elevate platform dramatically improves the effectiveness and efficiency of security operations by delivering comprehensive visibility, intelligent deception, alert validation, and automated response across network and endpoints. Fidelis is trusted by the most important brands in the world. See what you've been missing. For more information go to www.fidelissecurity.com.

