CASE STUDY

# Leading Healthcare Provider Eliminates Millions in HIPAA Compliance Fines with Keysight Security Visibility Fabric

KEYSIGHT

## Organization

- U.S. regional healthcare provider that owns, operates, and manages 300 hospitals and surgery centers

## Challenges

- Demonstrate and document HIPAA regulatory compliance to avoid penalties
- Upgrade perimeter firewalls and integrate with other security infrastructure
- Maintain current levels of network availability

## Solutions

- 8x Keysight Vision ONE Inline Network Packet Brokers
- 16x Keysight DUO Inline Bypass Switches

## Results

- Achieved HIPAA compliance with high availability deployment
- Zero packet loss for inline security appliances
- Simple future security additions and upgrades
- Fastest security infrastructure failover

# Architecture Upgrade Supports Next Generation Firewall and Delivers Fastest Failover

This leading provider of healthcare services owns, operates, and manages over 300 hospitals and surgery centers in 20 states and employs approximately 200,000 people. The provider needed to upgrade its system-wide security infrastructure to comply with regulations of the Health Insurance Portability and Accountability Act (HIPAA). They faced $1.5 million in annual penalties for violations associated with not having adequate controls over security attacks on patient data, including medical data collected from the wireless medical devices and equipment.

The security team brought in a consultant with expertise in building HIPAA compliant security architectures and they proposed deploying a next generation firewall (NGFW) behind the existing firewall, to provide more robust threat detection and satisfy HIPAA regulations. In addition, with this significant security tool and IT resource investment, the company took the opportunity to also deploy a high availability, security fabric from Keysight to ensure the new NGFWs and the rest of their security infrastructure would work as efficiently as possible.

"Now we have the ability to load balance across our new and existing security appliances, to keep them in service longer and make better use of our security budget."

**Senior Director**

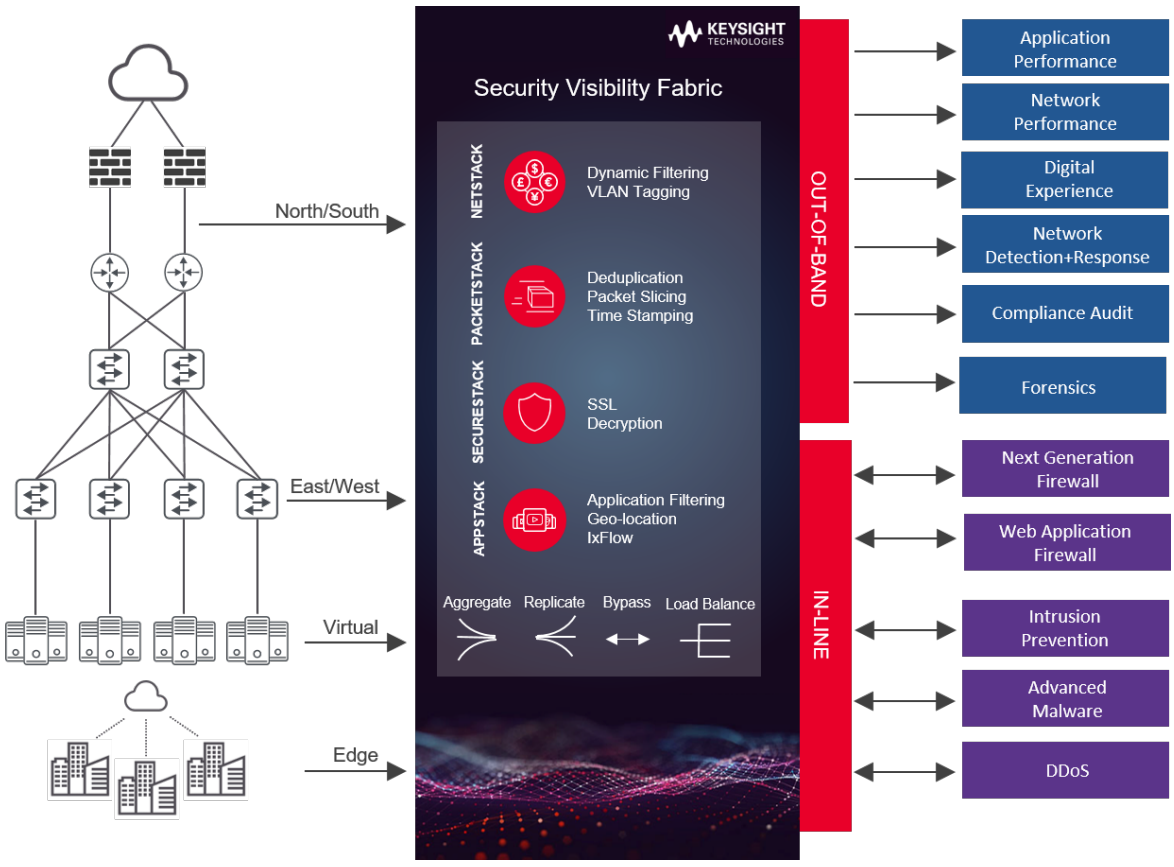
# Keysight Security Visibility Fabric Protects Network Availability

The network operations team expressed concern about the risk of downtime associated with adding yet another inline security device. To address this concern, the Keysight Security Visibility Fabric increased the company's security resilience and eliminated single points of failure each security appliance represented when deployed inline. The Keysight solution deploys bypass switches in front of every inline device to continually assess their readiness and, if necessary, route traffic around any device that is not operating properly. This simple architectural change prevents any inline security device that becomes overwhelmed or simply fails—including firewalls, intrusion prevention systems (IPS) or web application firewalls (WAF)—from causing a wider network outage.

# Intelligent Filtering Increases Efficiency and Effectiveness

To build in intelligence and flexibility, Keysight combines bypass switches with intelligent network packet brokers (NPBs) at key points to collect, aggregate, and inspect network traffic. This approach lets the healthcare provider see everything on their network, look within encrypted SSL traffic, and forward only relevant traffic to each security monitoring and detection tool. NPB intelligent filtering, combined with load balancing, reduces the traffic flowing to each security tool, increasing efficiency, and limiting data volumes each tool must reliably handle. The features most important to the team were:

- hardware based solution provides full line-rate processing with nanosecond latency
- 100% reliable packet forwarding, with no dropped packets circumventing security inspection
- intuitive drag-and-drop GUI lets security administrators work more quickly and productively
- role-based access control to satisfy demands of HIPAA



# Visibility to Face Ever-Evolving Threats

The organization's complex security architecture made it difficult to get a comprehensive view of the traffic entering and moving across the company's internal networks. Keysight's Security Visibility Fabric provided them with visibility across each segment of the network and also simplified maintenance and configuration, to let the security team focus on threat detection and elimination. The NPB centralized interface supports both inline and out-of-band tools, to make it easier to document the movement of patient records from one location to another, as HIPAA requires.

# Fast Failover Wins the Day

The healthcare provider required vendors to perform a failover test to measure just how fast the network could be restored from a security tool failure event. Keysight's redundant bypass switches and NPBs in active-active mode provided the fastest recovery time among the solutions tested. A competitive solution—only available in Active-Standby mode—took nearly double the time and convinced the team that Keysight's Security Fabric was the only real choice.

# Future Flexibility and Scalability

This architecture enables administrators to safely deploy new solutions, add scale to handle increasing traffic, upgrade tools, or take a device offline for troubleshooting—all without impacting the flow of network traffic or waiting for planned downtime.