CASE STUDY

SOOSAN INT and Keysight Help National Data Center Centralize Security Orchestration and Ensure Resilience

KEYSIGHT

Overview

As the organization responsible for managing the national IT infrastructure and Government Data Center, maintaining continuous network availability is paramount. However, the data center's security architecture had become increasingly complex due to the deployment of a diverse array of inline security solutions.

To achieve this, they deployed a powerful joint architecture combining Keysight Network Packet Brokers (NPBs) with SOOSAN INT's ePrism SSL VA. This integration streamlined their complex network configuration into a unified platform, ensuring high-speed traffic is decrypted, load-balanced, and precisely delivered to security tools without compromising service availability.

Highlights

Industry: Government

Customer: South Korean government organization responsible for managing national IT infrasturcture

Challenge: Systematizing complex security architectures involving multiple inline security tools and ensuring the resilience of critical infrastructure against failures

Solution: Implement SOOSAN INT ePrism SSL VA to provide dedicated, high-capacity TLS/SSL decryption and Keysight Network Packet Brokers (NPBs) to aggregate, load balance, and ensure fail-safe distribution of traffic

The Challenge

The organization sought to decouple these tools from the network path to ensure resilience (bypass) while simultaneously optimizing their performance. They needed a solution that could intelligently filter traffic — sending only relevant packets to specific tools — and load balance high-throughput data to prevent bottlenecks.

To achieve modernization, the decision-making team required a unified platform capable of delivering:

- Simplified management of complex multi-tool environments (WAF, IPS, IDS, APT) using network packet brokers
- Operational optimization through intelligent load balancing and precision traffic filtering
- High-availability resilience ensuring zero network impact during device failure or maintenance
- High-capacity TLS/SSL processing capable of handling encrypted traffic at scale
- Seamless integration via robust API support

> "Keysight's network packet brokers simplified our complex security architecture by ensuring that only necessary traffic reaches our WAF, IPS, and APT tools," said the Head of IT at the Data Center. "Paired with ePrism SSL VA for high-speed decryption, this joint solution delivers the resilience and optimized performance required for critical national infrastructure."

Together, SOOSAN INT, Keysight, and the customer team designed a unified, scalable visibility platform able to simplify encrypted traffic management and optimize traffic flow to security tools.

The Solution: A Modern Joint Solution from SOOSAN INT and Keysight

To modernize their security architecture, the government data center selected Keysight for its proven stability, scalable architecture, and ability to ensure high availability across complex networks. The team required a solution that could orchestrate traffic for a diverse range of inline tools—including WAF, IPS, APT, and packet analysis systems—without inducing latency or points of failure.

ePrism SSL VA was selected to handle the compute-intensive demands of high-capacity TLS/SSL decryption, ensuring comprehensive threat visibility. As the market-leading SSL visibility solution in South Korea, ePrism is recognized for its exceptional throughput and seamless compatibility with a vast ecosystem of third-party security tools. Critically, the team valued ePrism's support for NPB Health Checks — overcoming a common stability challenge that frequently impacts other SSL solutions when integrated into complex inline chains.

Keysight's Network Visibility Platform delivers full-featured network visibility capabilities, including:

- High-performance traffic aggregation
- Intelligent filtering and deduplication
- Efficient forwarding of traffic to ePrism SSL VA and other go-to security tools

What's Next?

The joint network visibility architecture from SOOSAN INT and Keysight is engineered to meet future demands head-on. As TLS/SSL traffic volumes grow, the solution supports seamless scalability — allowing the organization to simply add ePrism appliances to the Keysight network packet broker fabric. Furthermore, the bank is positioned to unlock deeper visibility intelligence by deploying Keysight's AppStack and SecureStack software suites, enabling advanced analysis and rapid threat detection.

About Keysight Technologies

Connect and Secure the World with Dynamic Network Intelligence

The need for always-on networks is pervasive, and expectations are high when it comes to keeping them connected and secure. As technologies advance, edge computing, cloud environments, sophisticated security threats, increasing bandwidth requirements, and demanding compliance regulations make it challenging to extract actionable insight from your network. Keysight can help. Customers rely on our solutions to deliver rich data about network traffic, applications, and users across any networking environment. This deep insight is what we call dynamic network intelligence. It helps you continuously innovate, meet aggressive service level agreements, and keep applications running smoothly and securely.

Visit GetNetworkVisibility.com for the latest from Keysight on insights for optimizing network monitoring, security, and analysis.

For more info, contact: 1-888-438-4942 or visibilitysales@keysight.com

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.

KEYSIGHT

This information is subject to change without notice. © Keysight Technologies, 2026, Published in USA, January 23, 2026, 3126-1053.EN