

Payment Processing Company Works with Keysight and Trellix to Decrypt Traffic and Maintain Compliance

HIGHLIGHTS**Industry:** Finance**Customer:** Payment Processing company based in Puerto Rico and serving the LATAM region**Challenge:** Adding decryption capabilities needed to detect threats and maintain compliance without deploying an agent-based solution.**Solution:** Upgrading existing monitoring solution to modern Trellix IPS solution and using Keysight Vision 400 network packet brokers to perform decryption prior to sending data to Trellix for inspection

A prominent payment processing company serving Latin America chose a Keysight network visibility platform and Intrusion Prevention Systems (IPS) from Trellix to decrypt traffic in primary data centers. The upgrade improves the company's threat detection capabilities and meets financial industry data privacy regulations that mandate decryption.

Compliance Calls for Full Visibility

With up to 90% of all traffic traversing networks encrypted, financial services providers cannot risk letting data pass to and through security tools uninspected. The Puerto Rico-based company sought a scalable, secure, and future-ready solution to avoid missing dangerous threats, failing cybersecurity audits, and incurring steep fines for non-compliance.

To perform decryption, the company's existing McAfee monitoring tools would have needed to install agents directly onto workstations, some of which could not accommodate agents. Decryption also needed to take place inline to support the exchange of ephemeral keys used in the Diffie Hellman method of cryptography.

The company wished to avoid the operational overhead and third-party risk associated with agent-based monitoring. The CISO reached out to Cortelco, a trusted integration partner, to come up with a viable alternative.

Cortelco Designs a Solution Based on Keysight and Trellix

Cortelco, also a long-time Keysight channel partner, devised an innovative plan for upgrading the company's three primary data centers. Since McAfee had since joined forces with Trellix, the process began with migrating the old monitoring technology to modern Trellix IPS solutions.

Instead of deploying agents, the Vision 400 handles decryption directly onboard the packet broker before load-balancing traffic to monitoring tools for analysis. This agentless approach meets various compliance requirements for data security and can also improve monitoring infrastructure performance by removing unwanted traffic from the network – duplicates, unnecessary headers, etc. – altogether.

Keysight Adds Resilience to Bypass Downtime

Along with the packet brokers, the company deployed Keysight intelligent bypass switches to bolster network resilience. iBypass complements Vision packet brokers by regulating the flow of traffic between the Vision 400s and Trellix IPS devices and monitoring for network, device, and power failures. In the event of an outage, iBypass re-routes traffic to other available links and tools to avoid downtime until issues get resolved.

Joint Solution Benefits

The addition of decryption capabilities to its visibility and monitoring infrastructure equips the payment processing company:

- Inspect all network traffic for malware and other threats hidden inside encrypted packet
- Support its implementation of Diffie Hellman cryptography
- Optimize investments in monitoring while evolving its data center infrastructures throughout the region
- Avoid downtime during network upgrades and day-to-day operations

Visit [GetNetworkVisibility.com](https://www.keysight.com/GetNetworkVisibility) 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.

This information is subject to change without notice. © Keysight Technologies, 2026, Published in USA, January 6, 2026, 3126-1003.EN