

# Trellix + Keysight:

Scalable threat prevention

# The Joint Solution

Your business relies on reliable connection to the Internet, but with today's complex threat landscape, access isn't as simple as it should be. Trellix's Threat Prevention Platform stops cyber-attacks that traditional and next-generation firewalls, Intrusion Prevention Systems (IPS), anti-virus, and web gateways may miss.

Trellix's Threat Prevention Platform protects against zero-day Web exploits and multi-protocol callbacks. Combining the platform with Keysight's VisionOne creates a scalable and fault-tolerant solution that lets businesses maintain security and performance while meeting increasing demand.

- Easily scale deployments while lowering TCO
- Protects against zero-day, advanced targeted attacks
- Cuts off outbound malware transmissions across multiple protocols
- Integrates with EX Series to stop blended attacks
- Add a PX series appliance for network forensics capabilities and accelerated actionable insight



## The Trellix Threat Prevention Platform Keeps Sensitive Data Safe

Trellix's NX and Network Threat Prevention Platform appliances deliver a turnkey system that can be deployed inline at Internet egress points to block inbound exploits and outbound multi-protocol callbacks. Highlights include:

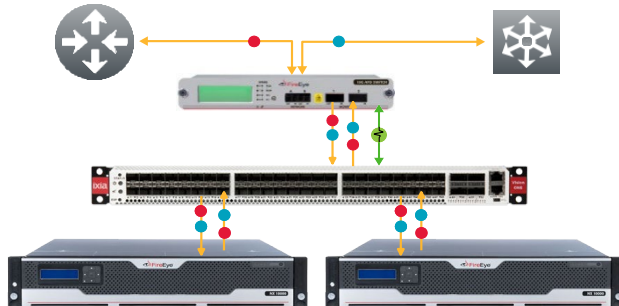
- Employing patented Multi-Vector Execution (MVX) to accurately confirm zero-day attacks, create real-time protections, and capture dynamic callback destinations
- Dynamic analysis of zero-day attacks within a full-featured virtual analysis environment yields real-time malware security content to protect the local network and share with subscribers of the Trellix Dynamic Threat Intelligence (DTI) cloud
- Signaling to incident response mechanisms such as SIEM
- TCP resets for out-of-band blocking of TCP, UDP, or HTTP connections
- Keysight's VisionOne prevents overburdening of tools

Keysight's VisionOne is built specifically to prevent overburdening by distributing traffic to multiple monitoring tools. This allows deployments to scale with demand while maintaining security. Tool health is monitored using Heartbeat packets, allowing traffic to be proactively redirected to available or spare tools in case of failure.

VisionOne works with Trellix NX Appliances and AFO Bypass Switches (OEMed from Keysight) to optimize inline deployment. Bypass switches feature advanced Heartbeat and Link Fault Detect capabilities allow monitoring of Keysight's xBalancer's state information.

Switches send heartbeat packets to VisionOne to identify link anomalies and power failures. Upon detecting a change, the bypass switch immediately re-routes traffic using Keysight's Fast Path™ technology. Once VisionOne is brought back online, traffic automatically resumes.

This joint solution from Trellix and Keysight increases ROI and network reliability with intelligent security automation, advanced load-balancing for the greatest efficiencies, and assurance that security solutions will scale as needs continue to grow.



**How it Works:** Two network ports on the Trellix AFO bypass switch connect inline to upstream and downstream network devices, while 2 monitor ports connect to the Keysight xBalancer. The Trellix appliances provide inline network conditions, while the AFO continually verifies that VisionOne is in operation.

## Features and Benefits

- Next-generation load-balancing without compromising reliability
- Protects against zero-day, advanced targeted attacks: Solution detects and stops advanced targeted attacks using malicious images, PDFs, Flash, or ZIP/ RAR/TNEF archives
- Thwarts malware: Inline or out-of-band, helps deter data exfiltration, botnet activities, and advanced persistent threats communicating across HTTP, FTP, IRC, and others
- Integrates with Trellix's EX Series to stop blended attacks
- Dynamically generates malware intelligence: Captures details such as callback coordinates and communication characteristics to protect locally and share globally through the cloud

## About Trellix

Trellix's purpose-built, virtual machine-based security platform provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber-attacks. These highly sophisticated cyber-attacks easily circumvent traditional signature-based defenses such as next-generation firewalls, IPS, anti-virus, and gateways. The Trellix Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. Trellix's virtual execution engine and dynamic threat intelligence combine to identify and block cyber-attacks in real time. Trellix has more than 2,200 customers across more than 60 countries.

## About Keysight

Keysight delivers a powerful combination of innovative solutions and trusted insight to support network and security infrastructures from concept to operation. Whether you are preparing a product for launch, deploying a service or application, or managing performance in operation, we offer an extensive array of solutions for testing, visibility, and security—all in one place.

Our solutions are used worldwide to validate network functions, test the integrity of security infrastructures, and deliver an end-to-end view of the network. The result: stronger networks, better performance, increased security resilience, happier customers, and maximum ROI.

For more information on Keysight Technologies' products, applications, or services, please visit: [www.keysight.com](http://www.keysight.com)



This information is subject to change without notice. © Keysight Technologies, 2022, Published in USA, August 17, 2022, 7019-0367.EN