

# LINKSHADOW AND KEYSIGHT DEEP INSIGHTS WITH DYNAMIC INTELLIGENCE

Being under the threat of a cybersecurity attack is the new norm nowadays. And to contain the growing rate of these attacks is the key challenge. Designed to manage threats in real-time with attacker behavior analytics, LinkShadow® is meant for organizations that are looking to enhance their defenses against advanced cyber-attacks, zero-day malware and ransomware, while simultaneously gaining rapid insight into the effectiveness of their existing security investments. With LinkShadow's unparalleled detection of even the most sophisticated threats, the chance of an attacker passing through your network is virtually nonexistent.

Ixia's Vision series of intelligent network packet brokers (NPBs) integrates with LinkShadow to provide a full visibility of network data and metadata, from across the hybrid enterprise, allowing LinkShadow to gain a bird's eye view into the whole organization to protect it from internal and external cyberattacks.





## INTEGRATION STORY: LINKSHADOW - KEYSIGHT

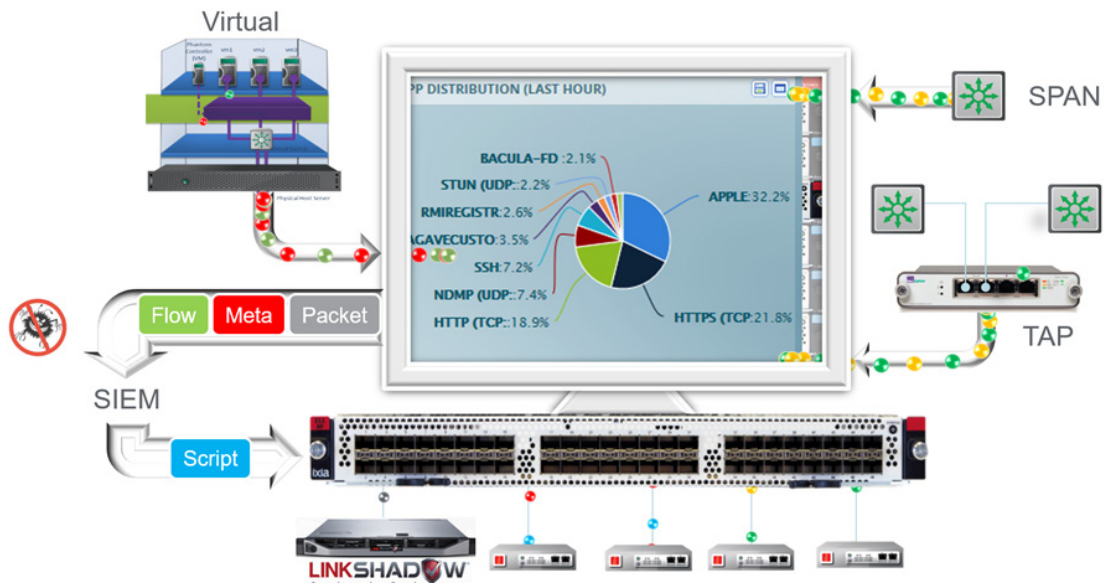
Security analysis processes are powered by accurate, real-time data from anywhere across the hybrid data center. Ixia's network visibility solutions equip LinkShadow with precisely the right Netflow and packet data, as well as time-saving metadata used to quickly identify potential threats. Ixia's Vision network packet brokers aggregate and filter traffic from taps and other network access points at line rate and deliver it to LinkShadow for fast, efficient analysis.

Ever wish you had the actual packets? The integrated solution features an API that allows analysts to configure Ixia packet brokers to automatically forward all relevant flow and packet data associated with specific alerts and anomalies to speed investigations.

**HOW IT WORKS:** Ixia visibility solutions provide packet and flow data from physical and virtual access points to LinkShadow and other security tools, simultaneously aggregating, filtering, and directing exactly the right metadata or packets to each tool. Based on LinkShadow alerts, packet captures can be automatically triggered to accelerate remediation.

## Joint Solution Highlights:

-  Deeper insights with dynamic network intelligence
-  Eliminating network blind spots
-  Increase LinkShadow's monitoring efficiency
-  Overcome SPAN and other network issues



## CHALLENGES OVERCOME BY THE INTEGRATION

Security team needs to be fortified against malicious activities that can be invisible in the logs and empowered with full visibility to guarantee optimum protection.

Integrated with IXIA, LinkShadow monitors Full Network Traffic passively, providing high-end visibility and birds-eye-view on all activities and empowers your defense system with Threat Hunting use-cases that helps detecting and identifying attacks not only at early stages, but the second it become suspicious.

LinkShadow uses advanced machine algorithms for analytics to build a mathematical model of users and entities on a network (UEBA), looking for anomalies, score it based on various factors to then send it for investigation seamlessly and without any human interaction.

LinkShadow also complies with MITRE ATT&CK, Cyber Kill Chain Framework and more to fully comprehend the threat landscape and make better use of the IoCs as part of the Intelligence Driven Defense, to document and track various techniques attackers use throughout the different stages of a cyberattack to infiltrate your network and exfiltrate data.

## HIGHLIGHTS INCLUDE:

- Internal and External Cyber-Threats Detection
- Hunt for threats across the network with speed, context, and efficiency
- Realtime traffic and attack visualization to seamlessly detect unknown communications
- 360 degrees view of an anomaly and relevant events associated with the anomaly being investigated
- Deep dive into suspected traffic every device connected to an infected endpoint

