INSURANCE INDUSTRY

Network Visibility and Cybersecurity Solutions

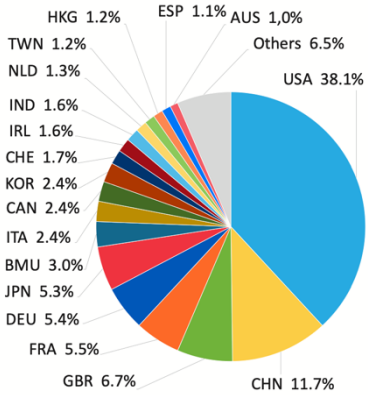
KEYSIGHT

BROCHURE

Table of Contents

Introduction

The global financial markets are made up of three distinct segments – Retail/Commercial Banking, Capital Markets and Insurance. Insurance is often considered the step child of the three segments, but is an enormous industry in its own right. According to the International Association of Insurance Supervisors (IAIS), the 2022 Global Insurance Market was $7.2 Trillion (USD) and growing at 8% per annum. Although the largest market is the USA, markets such as China, UK, France and Germany contribute significant revenues – see pie chart at right.



Though the insurance market continues to grow, consultancies such as PWC, KPMG, DELOITTE and EY all report considerable challenges in the insurance markets. The Covid pandemic and war in Ukraine have all added short term risk profiles, but longer term factors are all impacting the insurance market. Climate change is impacting risk in many areas. Technological change continues to open up both strategic threats but also business opportunities. And customers are increasingly tech savvy and demand new and ever more sophisticated products with what was historically considered impossible lead times. To add to even more pressure, we have the growth in InsurTech companies who threaten the established business models of many insurance companies.

According to PWC, successful insurance companies will be ones that:

- Are laser focused – they define a strategic direction and stick to it
- Commit enough resources to their strategy
- Get creative with insurance products
- Build strategic partnerships which allow the insurance companies to focus on core competencies and on enhancing technology

Therefore, a key part of success is the technology platform that not only allows the insurance company to successfully implement its strategy, but also minimizes risk, facilitates market access and channel development, and maximizes customer service.

According to PWC, the key elements of a successful strategic technology platform are:

- An end to end core processing system that efficiently issues policies, contracts, enables payments, keeps track of finances and allows the user to achieve scale
- A comprehensive digital data and integration capability
- One that supports customer/distributor/employee-facing systems
- An infrastructure that is fully integrated into a “Cloud First” strategy – to allow rapid scaling

This document highlights some of the areas that Keysight’s Visibility portfolio and associated products can assist insurance companies in the development and support of their strategic technology platform and gives some examples of real solutions provided to insurance companies around the world.

Deep Data Insights

Within any large insurance IT system, billions of packets are exchanged between end users, processes and virtual/physical servers. These packets are usually based on ethernet technologies and can travel a few feet within a data center equipment rack or thousands of miles across the world. Applications typically use just a subset of the information contained within the packets and may ignore information such as exact timing, IP address, MAC address (which indicates the exact hardware that originated the traffic) and protocols.

Keysight's network taps and packet brokers allow insurance companies direct access to packet level data. Such packet level data can be used to:

- Assist with tactical network management and fault finding - enabling higher availability of critical systems
- Assist with capacity planning – so enhancing end user experience
- Help detect malicious cyber attacks
- Provide an additional source of high value customer data

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.

Investing in reliable network monitoring and visibility solutions is critical for insurance companies to ensure the smooth functioning of their operations, maintain the trust of their customers, and comply with regulatory requirements.

Insurance companies are especially heavily reliant on their network infrastructure to conduct their day-to-day operations, including processing transactions, managing customers' accounts, and accessing critical financial data. Any disruption or downtime in theses network can result in significant financial loses, damage to their reputation, and loss of customer trust.

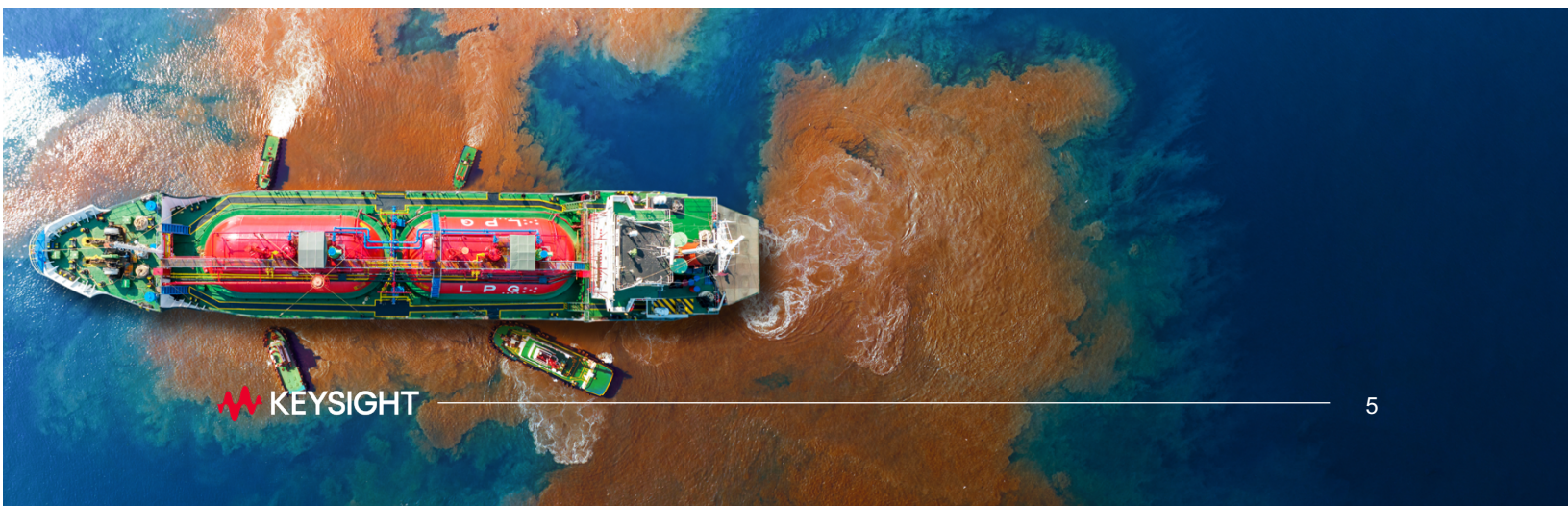
Network monitoring and visibility solutions provide insurance companies with real-time insights into their network performance, allowing them to detect and address issues before they escalate into major problems. By monitoring their network traffic, insurance companies can identify anomalies, potential security threats and performance bottlenecks that may impact their operations.

In addition, network monitoring solutions help your corporation comply with regulatory requirements related to data privacy, security and availability. These solutions enable insurance companies to collect and analyze network data, which can be used to address compliance with regulatory requirements.

Keysight can help. Over 50 insurance companies in 17 countries rely on our solutions to deliver rich data about network traffic, applications, and users across any networking environment. Keysight's optical and copper taps, plus Vision network packet brokers (NPBs) are at the core. They help insurance companies get the most out of the security and network monitoring tools by delivering filtered, streamlined traffic. Taps provide a pure and unedited view into traffic on the network, forming the foundation of dynamic network intelligence. Once a tap has an unadulterated copy of a packet it can be processes within a NPB and directed to the correct tool or data storage area.

To add additional resiliency to NPBs or to network management or standalone tools, they can be supplemented by bypass switches. Bypass switches can detect tool failure or be manually switched to pass traffic around downstream tools.

Together, Keysight's network visibility products enable you, and all your network tools, to be more efficient and effective so you can keep performance high, security tight and help provide a deep insight into user behavior.



Network Taps: The Foundation of Dynamic Network Intelligent

Network taps, and the pure, unfiltered visibility into network traffic they provide, are the foundation of dynamic network intelligence. Unlike SPAN ports or port mirroring, taps provide a view of all traffic — including malformed traffic and errors that typically would get dropped. This true visibility facilitates troubleshooting, as well as security and forensics.

Keysight offers the broadest selection of taps for any network, including Flex Tap optical taps, Flex Tap Secure+ enhanced security taps, copper taps, and aggregation taps

Keysight taps offer these key features:

- Plug and play
- No IP addresses
- Secure and un-hackable
- Copper and fiber
- Speeds up to 400 Gbps
- Support for single mode, multi mode and BiDi optics

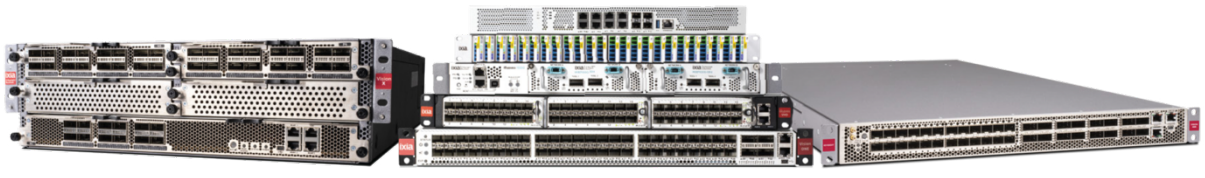
Network Packet Brokers: The Right Data for the Right Tools

NPBs are central to providing dynamic network intelligence throughout your network. Using application-aware traffic filtering, decryption, and deduplication, NPBs enable your security and monitoring tools to be more efficient and effective by ensuring that each tool gets the right data — nothing more, nothing less.

Furthermore, unlike many competitive offerings, many of Keysight's NPBs offer hardware acceleration enabled by field-programmable gate arrays (FPGAs). This functionality is a key consideration for any visibility deployment supporting mission-critical security or network monitoring because it allows the application of features and filters at line rate without lost traffic, blind spots, or dropped packets. Because partial visibility isn't good enough.

Keysight NPBs offer these key features:

- Zero-loss architecture
- Load balancing for multiple monitoring or security tools
- Centralized decryption, including advanced TLS 1.3
- Dynamic filter compiler reduces operational complexity
- Easy-to-use graphical user interface (GUI)
- Interface speeds from 100Mbps to 400Gbps



Case Study 1

Global Insurance Company provides packet data to its security tools

Problem: One of the top ten global insurance companies, based in Europe, wanted to ensure that copies of all critical traffic in their major data centers was sent to security tools. The company wanted to select relevant traffic from hundreds of links, filter it and then feed to a multitude of tools.

Solution: Keysight worked with the end customer and came up with a three tier design based around:

- Optical Taps – Flex Taps
- E100 NPBs
- Vision X NPBs

The optical taps provide copies of all traffic flowing on a particular network link within a major data center. By using the Flex Tap optical taps the customer could use different models for multi-mode BiDi and single mode links all within the same rack mount chassis.

The E100 NPBs provide an aggregation layer which concentrates the traffic from hundreds of taps within a data center. The E100s then feed the Vision X NPBs which do sophisticated filtering of traffic before it is sent on to the relevant tools.

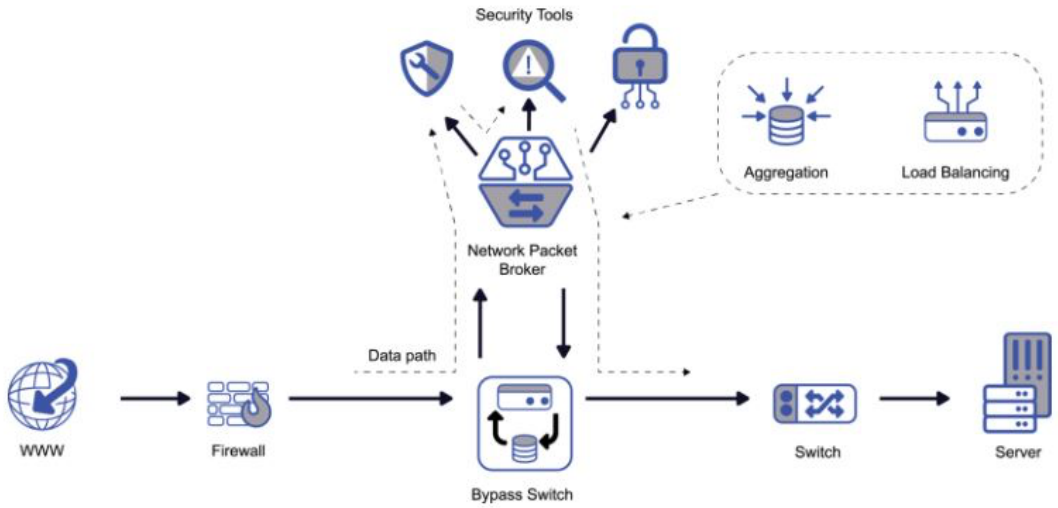
To manage the large number of NPBs per data center the IFC-CM management tool is used to provide a single “pane of glass” visualization of the arrangement of the packet brokers and to help with software upgrades etc.

The key benefits of the solution are:

- Cybersecurity and network management tools have access to every packet on their network for forensic and real time analysis
- Use of optical taps means that there is no danger of critical tool traffic being dropped by switch ports.

Increase Security Tool Uptime

IPS and WAF solutions can remove up to 80% or more of incoming security threats, before they ever enter your network. **External bypass switches and packet brokers** optimize the flow of data to those security tools as well as ensure continuous monitoring with the fastest possible recovery using a high availability configuration.



Keysight offers a wide range of external bypass switches. External bypass switches are preferred bypass switches embedded with an NPB as they offer true independent bypass capabilities. An external bypass and packet broker combination create an opportunity to realize the following benefits:

- Reduce security alerts – Keep security tools from being overwhelmed and help staff focus on high-priority alerts using advanced filtering capabilities
- Ensure continuous inspection – High availability deployments and traffic load balancing enable security tools to deliver robust threat detection
- Maximize tool efficiency – Chain inline security tools together to increase tool efficiency
- Protect network availability during deployment, upgrade, and maintenance of security solutions – an external bypass in front of inline security tools lets you route traffic around any device you need to take offline
- Deploy cyber resilient technology – Use equipment heartbeat messaging to create a self-healing architecture that can adapt during infrastructure failures and recover afterwards
- Deploy centralized decryption – Use a packet broker to decrypt once and pass the data to multiple security tools before re-encrypting legitimate data for passage downstream

Keysight provide a range of bypass switches that operate at speeds from 100 Mbps to 100 Gbps. They include such features as Active-Standby failure over, fail-to-wire in the event of power failure and automatic detection of tool failure by the use of programable heartbeats.

Bypass switches can be combined with inline configured NPBs or deployed in stand alone configuration. For maximum availability and risk mitigation the bypass switches are totally independent of the NPBs and can be configured to bypass the hardware in the event of not only a tool failure but even if an NPB fails.

Case Study 2

APAC Insurance Company increases availability of its security tools

Problem: The Keysight client is a leading insurance company in Asia-Pacific with operations across the region. With a strong technology platform the company relies on its network to provide digital insurance services to its customers who use both internet and mobile platforms. Given the criticality of its infrastructure it is imperative that its security tools do not degrade the availability of its eCommerce platforms. How then to have high product availability, but at the same time still being able to cope with scheduled and un-scheduled downtime of multiple security tools?

Solution: Keysight worked with the end customer and their preferred VAR to propose a solution based around iBypass DUO (Keysight's market leading optical bypass switch) and a number of Vision E40 NPBs. In total over 100 iBypass/Vision E40s have been deployed for this customer deployment.

The iBypass DUO are configured in an Active/Standby mode and pass internet traffic via the NPBs to the security tools. If the iBypass DUO detects failure of a primary security tool (via its inbuilt heartbeat capabilities) traffic will be directed to a secondary tool. Alternatively the iBypass DUO can be switched manually to allow for downtime of the primary tool – for software upgrades or other reasons.

In addition, a number of Vision E100 NPBs are used to collect traffic 'out of band' and feed multiple copies of traffic to additional security and monitoring tools.

Key benefits of the solution:

- Higher security tool availability
- Load sharing of security tools
- Easier swapping out of tools for configuration changes and software upgrades

Detect the Encrypted Trojan Horses

Organizations encrypt internet traffic to protect themselves and their users — in particular, to protect sensitive information such as credit card numbers, passwords, social security numbers, etc. As of early 2023 over 95% of web sites run the encrypted HTTPS protocol, with more than half using the advanced NTTPS/2 version. This encryption helps prevent identity theft, security breaches, and data leaks. However, much like a Trojan horse, encryption can also be the way malware and other threats are inserted into networks. The use of encryption therefore is a double edged sword. Encryption protects the data that users of insurance companies applications transfer across the internet, but it also allows malicious parties to hide data transfer of sensitive material from within an organization to the outside. By encrypting the outbound (and inbound) traffic, attackers can make the detection of compromised systems that much more difficult to detect and counter.

To defeat such encryption, Keysight recommends the decryption of all traffic passing to and from the internet. There are two basic approaches:

- Use inbuilt tools within each security tool to decrypt the traffic
- Decrypt the traffic once and feed the decrypted traffic to multiple tools

Inbuilt Tools

Using the inbuilt decryption capability within each security tool is a valid approach, but has a number of negatives:

- Decrypting the latest encryption standards (TLS with ephemeral keys) can take up to 60-80% of a tool's capacity

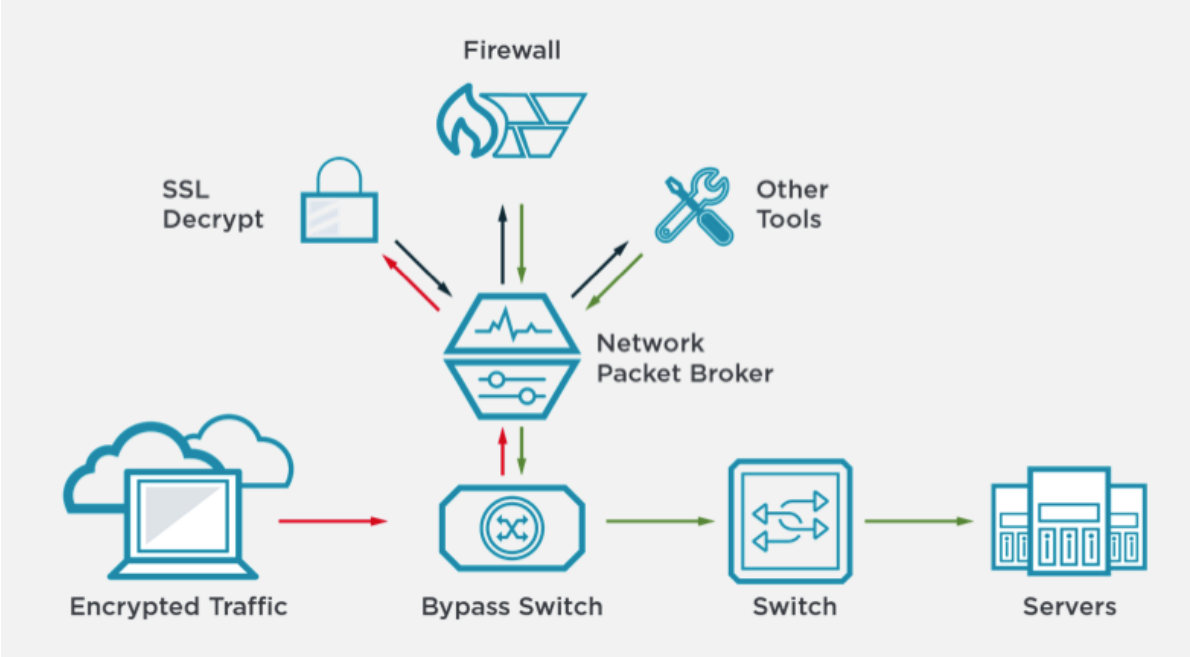
- Some tools simply do not have the capability to decrypt encrypted traffic flows – certainly at high data rates
- Setting up in line decryption capabilities is a complex and time consuming task. Why do this multiple times when a single solution is possible?

Decrypt Once, Inspect Multiple Times

The Vision X Network Packet Broker has a powerful inbuilt processor which allows it to decrypt inline encrypted traffic. Using Vision X's decryption capabilities allows insurance companies to decrypt traffic bound to/from the internet just once and then feed the decrypted 'clear text' traffic to multiple security tools. By offloading decryption insurance companies can:

- Maximize their ROI in security and monitoring tools
- Improve the performance of these tools
- Increase their capability to scale
- Have complete visibility into encrypted traffic, even if based on ephemeral keys

The following diagram shows a simplified view of a Keysight NPB being used in line to decrypt traffic.



Example of a visibility architecture using inline SSL decryption

Help Migrate To and Secure Cloud Infrastructure

As mentioned in the introduction, insurance companies who wish to be successful must embrace public cloud infrastructure. Although moving mission critical applications to public cloud services offers a number of benefits, it also raises a number of concerns. Key amongst these are:

- How do you have full visibility of traffic moving between applications, as you do in the physical world by using taps and network packet brokers?
- How do I test that zero trust models are working within the cloud when I can't see the traffic?
- How do my security tools in the cloud really scale?

To help insurance companies answer such questions, Keysight offers a range of visibility and test tools. Two key products are:

- CloudLens
- CyPerf

CloudLens

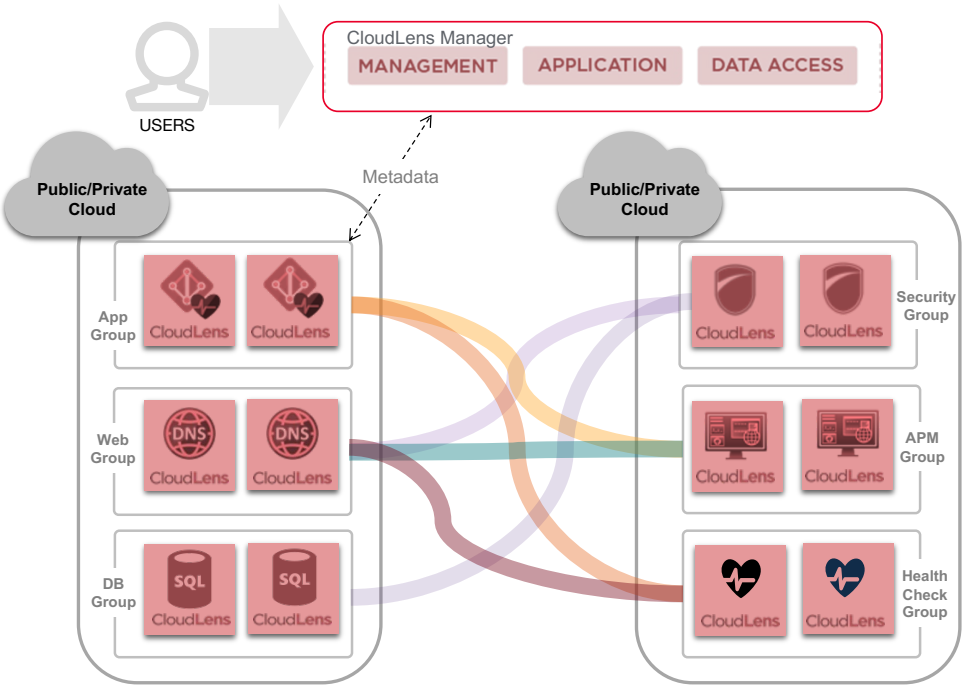
Keysight CloudLens provides a complete cloud-based visibility solution for virtual network traffic. With CloudLens you can mirror data, filter and forward traffic between virtual machines, containers or Kubernetes Pods, and tools. It includes two core capabilities. First, an ability to virtually tap (vTap) or capture, filter and forward a copy of network traffic directly to either tools or a network packet broker. Second, it can operate as a virtualized network packet broker, allowing aggregation, filtering, deduplication of virtual network traffic all within the cloud.

vTap's Integrated filtering reduces vSwitch, vNet, VPC and LAN bandwidth consumption by filtering at the vTap point (source), providing a multi-layer L2-L4 filtering engine allowing for filtering based on IP address, subnet, protocols, port numbers, and/or individual workloads.

There are several different variants of CloudLens which can operate in Private, Public or Hybrid environments.

Within public cloud environments, the complete virtual tap ecosystem includes the following components:

- CloudLens Manager, deployed as a virtual appliance or within a Kubernetes Cluster, provides capture and filter management, and monitoring.
- CloudLens Sensor vTaps, installed in the virtual workloads to monitor traffic, within AWS, Azure, GCP for example, are the sources of the traffic to mirror. The sensors includes some filtering options and then forwards the tapped traffic via GRE, VxLAN or Encrypted tunnel to aggregation points. The sensors can send traffic over any interface available in the virtual workload.



In addition to tapping capabilities, CloudLens supports packet processing within a private or public cloud environment allowing virtual network traffic aggregation, filtering, deduplication, NetFlow generation, and access to Keysight's application intelligence capabilities without the need of a physical packet broker.

Keysight's CloudLens virtual packet processing is delivered through a dedicated virtual machine and is an intermediate component in the virtual visibility architecture that "sits" between vTap points and performance and monitoring tools to which can do the following:

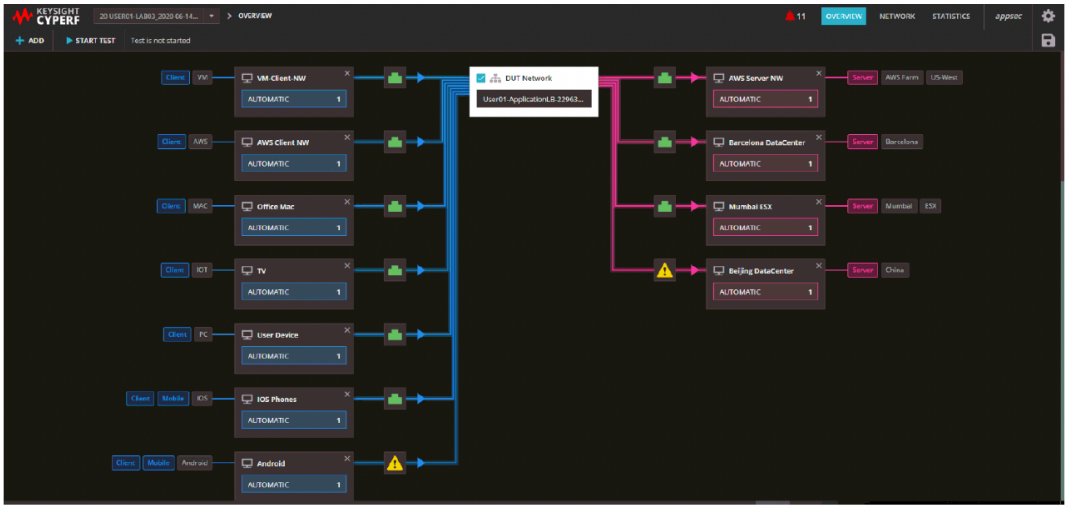
- Terminate/Strip GRE, VxLAN, Geneve and VLAN
- Aggregate network packets
- Re-Assemble network packets

- Filter and deduplicate traffic
- Duplicate and forward traffic
- Load-Balancing

CyPerf

CyPerf is the industry's first scalable, cloud-native software subscription network test solution for zero trust. It deploys lightweight test agents across various private and public cloud environments, delivering insights into user experience, security posture, and performance bottlenecks. By realistically emulating application traffic, user behavior, and threat vectors at scale, CyPerf measures and validates the performance of dynamic distributed networks, security devices, and services for more confident deployments and ongoing monitoring.

CyPerf emulates real user and application behavior, customizable applications and attacks to replicate a real-world environment. It delivers new heights in realism by generating both legitimate and malicious traffic across a complex set of proxies, software-defined wide-area networking (SD-WAN) devices, identity providers (IdP), secure access service edge (SASE) nodes, virtual private network (VPN) tunnels, transport layer security (TLS) inspection devices, elastic load balancers, containerized devices, and web application firewalls.



CyPerf screen showcasing multiple agents simulating geographically distributed clients and servers

Cyperf key capabilities include:

- High realism
- Native authentication
- High scalability
- Support for both lab and live production network testing
- Auto-scaling
- Modern, easy to use UI supporting multi-user authentication

Branch Office IT Quality

Over the last ten years the role of the insurance branch office as not so much evolved as revolutionized. Customers no longer want to travel to a local office or insurance broker to buy insurance, they prefer to transact via either a PC over the internet or from a mobile device. However, at the same time the offerings from insurance companies have become ever more sophisticated and complex. The range of insurance cover possible to both consumer and corporate customers can seem overwhelming. In these environments the role of face to face meetings still has value and in fact can be seen as a competitive advantage to either the insurance company themselves or their network of insurance brokers that they support. On-Line/Mobile access provides the generic ordering for the vast majority of insurance transactions, but face to face meetings are still key for more complex and higher value transactions

In these new branch offices, which may seem more like a high end coffee bar, than a dull corporate office, the role of IT is critical to not just the ability of the customer or employee to access tools and transact purchases, but in some senses it reflects the value of the brand itself. Going into an insurance branch office and finding out that you cannot access the internet or that connections keep dropping out does not instill confidence in the quality of the insurance provider.

Given the new role of the branch office, and the increasing sophistication of the telecommunications infrastructure deployed at branches, it is more important than ever that corporate IT departments are proactively monitoring the performance of their branch environments. It is no longer acceptable to wait for internal staff (or even customers) to report networking or connectivity issues. IT teams need to proactively monitor the branch networking infrastructure and rapidly react to issues. In addition they must be able to demonstrate to the internal business customers how they are providing the world class connectivity on a day by day basis.

Hawkeye

Take control of insurance branch user experience with active / synthetic network performance monitoring

To help you proactively monitor your branch network environment Keysight provides an active network monitoring tool known as Hawkeye. Hawkeye is an ideal tool to continuously manage performance and connectivity across your network. Hawkeye makes it simple for you to monitor remote sites access to cloud services and more — all from a single tool.

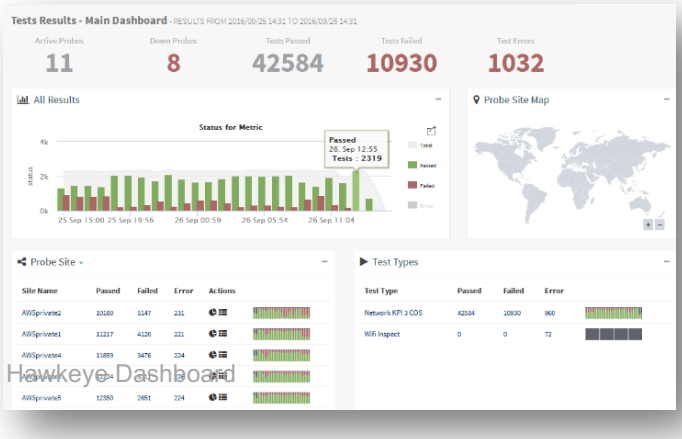
Whether you're measuring remote user experience over voice applications, branch office users on Wi-Fi, or general connectivity to your SaaS applications, it's easy to monitor, manage, and maintain peak performance. With Hawkeye, you can do all this and more:

Hawkeye offers these key features:

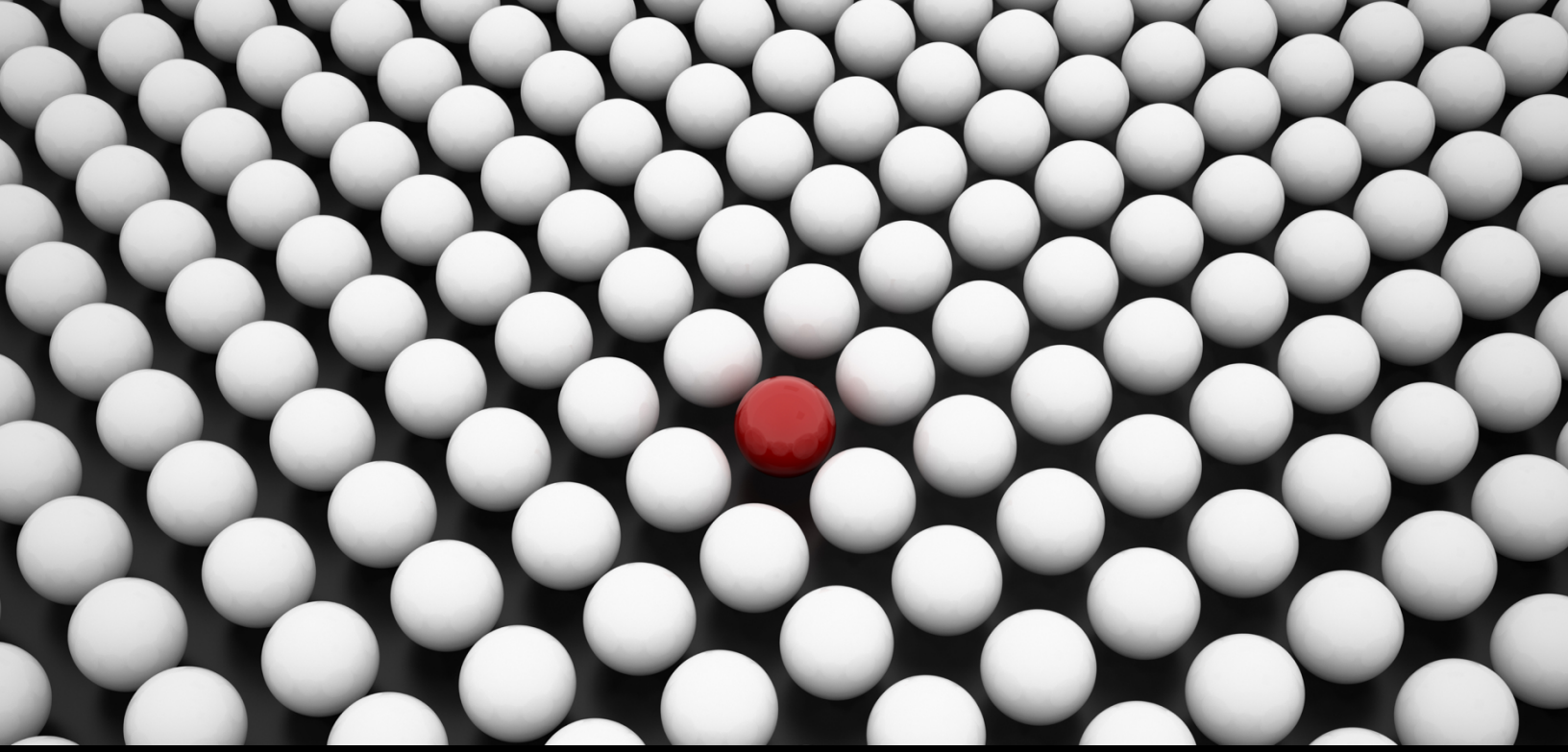
- A robust library of pre-defined QoS tests
- Monitor voice, video, and unified communication tools with turnkey integrations
- See all your performance data in a single interface
- Set custom alarms
- WiFi 6 and wireline monitoring
- Software (Linux, Windows, Mac) and wide choice of hardware platforms such as Vision 10S, XR3000, IxTap and IxProbe

IxTap Hawkeye Endpoint

- Speeds from 100M to 10G
- Wide range of inbuilt test types including:
  - Speed test from site to site with advanced configuration on traffic profiling
  - Advanced Bandwidth availability or verification with bit blasting or TCP-based testing
  - Class of service (COS) implementation validation with oversubscription scenarios
  - IP network SLA verification (one-way delay, jitter, loss)
  - Unified communications tests (Teams, Zoom) and Office 365 applications
  - Real-time streaming verification
  - Mean opinion score (MOS) for voice – G711, G729, AMR …
  - User experience tests (downloading web pages, etc.)
  - DNS response time
  - Netflix, YouTube, and Dash/Adaptive streaming test



Hawkeye Dashboard



Detect and Protect Against Time Anomalies

TimeKeeper provides time synchronization and time anomaly alerts

With an ever-growing dependence on accurate time, systems and processes are increasingly vulnerable to accidental or deliberate attacks on timing infrastructure. Organizations such as the US Government's Cybersecurity & Infrastructure Security Agency (CISA) are strongly advising that users of time harden their timing infrastructure and take steps to detect timing anomalies and react to them. Many internal systems and security processes rely on correct and unambiguous time. Disruption of timing signals such as GNSS, NTP or PTP can lead to failure of critical IT systems. Accurate time is also necessary to correlate the timing of security breaches.

TimeKeeper is a software product that is installed on servers and replaces standard timing daemons. It provides enterprises, service providers and governments with the ability to synchronize system clocks with multiple time sources available over the public internet or via GNSS time signals such as GPS or GALILEO. In addition to synchronization it also detects and alerts on timing anomalies. TimeKeeper is installed in over 100 financial institutions as well as multiple government deployments around the world.

TimeKeeper offers these key features:

- Simultaneous support of NTP and PTP time sources
- TrustedTime multisource failover
- Full alerting and easy to understand web-based time error graphs
- Choice of GUI or CLI management
- Optional long term audit tracking for financial markets
- Linux or Windows Server support
- TimeKeeper Server can serve time and manage hundreds of clients

Protect Against Cyber Own Goals

Problem: Security is Hard, Misconfigurations are Common, and Breaches are Rampant

With a multitude of emerging threats from inside and outside your network, the risk of a security breach has never been higher. All those risk factors are combined with a big human element that assumes everything has been setup and configured properly to get the best outcomes from each security tool. Organizations typically respond by throwing more money at the problem — acquiring additional security controls while increasing management complexity and complicating visibility for teams such as SecOps that are pressed to provide results and ROI.

To ensure a strong defense, organizations need to embrace an offensive approach that employs up-to-date threat intelligence to continuously verify their enterprise-wide security controls are working as expected and are optimized for maximum protection. Did John misconfigure the firewall on the midnight shift on Sunday night? Did Jane accidently install an obsolete version of the threat signatures on the IDS system when she did the update? To answer these questions Keysight have developed Threat Simulator.

Keysight Threat Simulator™ is a breach and attack simulation platform that provides insurance company security teams with insights into the effectiveness of their security posture and actionable intelligence to improve it. Keysight Threat Simulator comprises three core components:

- A user-friendly web-based interface makes it easy to configure and run security assessment scenarios, identify drifts in your security posture and retrieve actionable remediations.

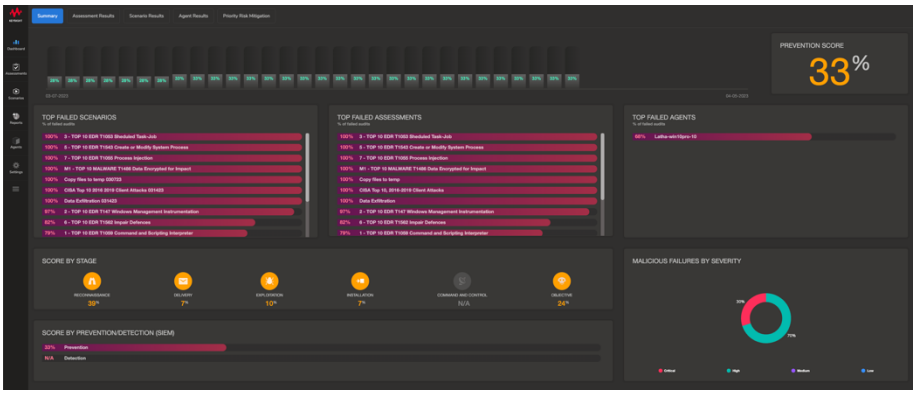
- A “dark cloud” entity that spins up agents on demand to simulate threat actors in the public domain (e.g.: malicious websites, external hackers, C&C).

- Agents that are deployed on your Enterprise network; available in Docker-container format, they act as simulator “targets” or “attackers” inside your network, enabling safe, yet realistic, attack and breach simulation scenarios (inside-to-outside, outside- to-inside and lateral movement).

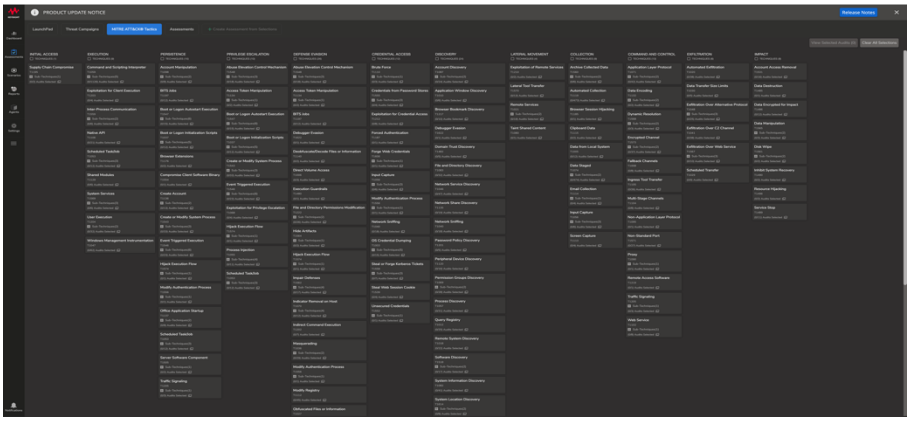
Key highlights are:

- Safe and cost-effective way to measure and validate the effectiveness of your production security tools.
- Patented recommendation engine provides clear, actionable insights on how to remediate identified gaps.
- Enables you to perform automated breach and attack simulations on a regular basis.
- Eliminates the assumptions that security controls are deployed and configured correctly.
- Active validation of all phases of the Attack Life Cycle.
- Support for MITRE ATT&CK® attack profiles and tactics

Example Threat Simulator screens:



Dashboard



MITRE ATT&CK® attacks

Digital Customer Experience

Eggplant

Steve Jobs once said - **“You’ve got to start with the customer experience and work backward towards the technology, not the other way around.”**

In an era where buying patterns have fundamentally changed and insurance customers are more digitally savvy than ever, delivering a seamless digital experience that delights every time is the only way to win.

While the definition of customer varies by specific part of the insurance industry, all users are united by their high expectations for quality digital offerings and services. For example:

- Consumers navigating a healthcare insurance site demand intuitive, easy-to-access content
- Retail customers availing of mobile apps or self-checkout kiosks will switch to a competitor if these systems experience performance issues or fail to impress them
- Uses of insurance aggregation sites expect them to display information (extracted via APIs) from any relevant insurance providers

Across these and other applications, the need to deliver a high-quality digital experience regardless of device, operating system or user is of paramount importance. Keysight’s Eggplant Software is a new way of testing end user applications. It is focused on the experience as seen by the customer and is focused on the user experience of retail sites – it can halve the time to test new retail sites and new functionality.

Eggplant gives insurance companies’ testing teams the power to delight their customers — and their boardrooms — by delivering technology that provides an engaging experience while simultaneously driving positive business outcomes. Or, to put it another way, we help organizations follow Steve Jobs’ advice. And what company wouldn’t want to do that?

About Keysight Technologies

Keysight Technologies, Inc. (NYSE: KEYS) is a leading technology company that helps enterprises, financial institutions, service providers, and governments accelerate innovation to connect and secure the world. Keysight's solutions optimize networks and bring electronic products to market faster and at a lower cost with offerings from design simulation, to prototype validation, to manufacturing test, to optimization and monitoring of networks and cloud environments.

Keysight generated revenues of $5.4B in fiscal year 2022. Keysight has over 30,000 customers in over 100 countries. 15,000 staff are employed at major R&D facilities around the world.

More information is available at www.keysight.com

Keysight has been widely recognized for excellence

by the cybersecurity industry:

Winner – Most Innovative, Breach & Attack Simulation, Global Infosec Awards, 2022

Security Solution of the Year – Glotel Awards 2020

New Product-Service of the Year | Security Software 2020 (Bronze Winner)

InterOp Best of Show 2020 (Runner-Up)

Hot Company in Breach and Attack Simulation – InfoSec Awards 2021

Finalist – Best Security Innovation in a SaaS Product – Cloud Awards 2021