Network Visibility Products

CATALOG
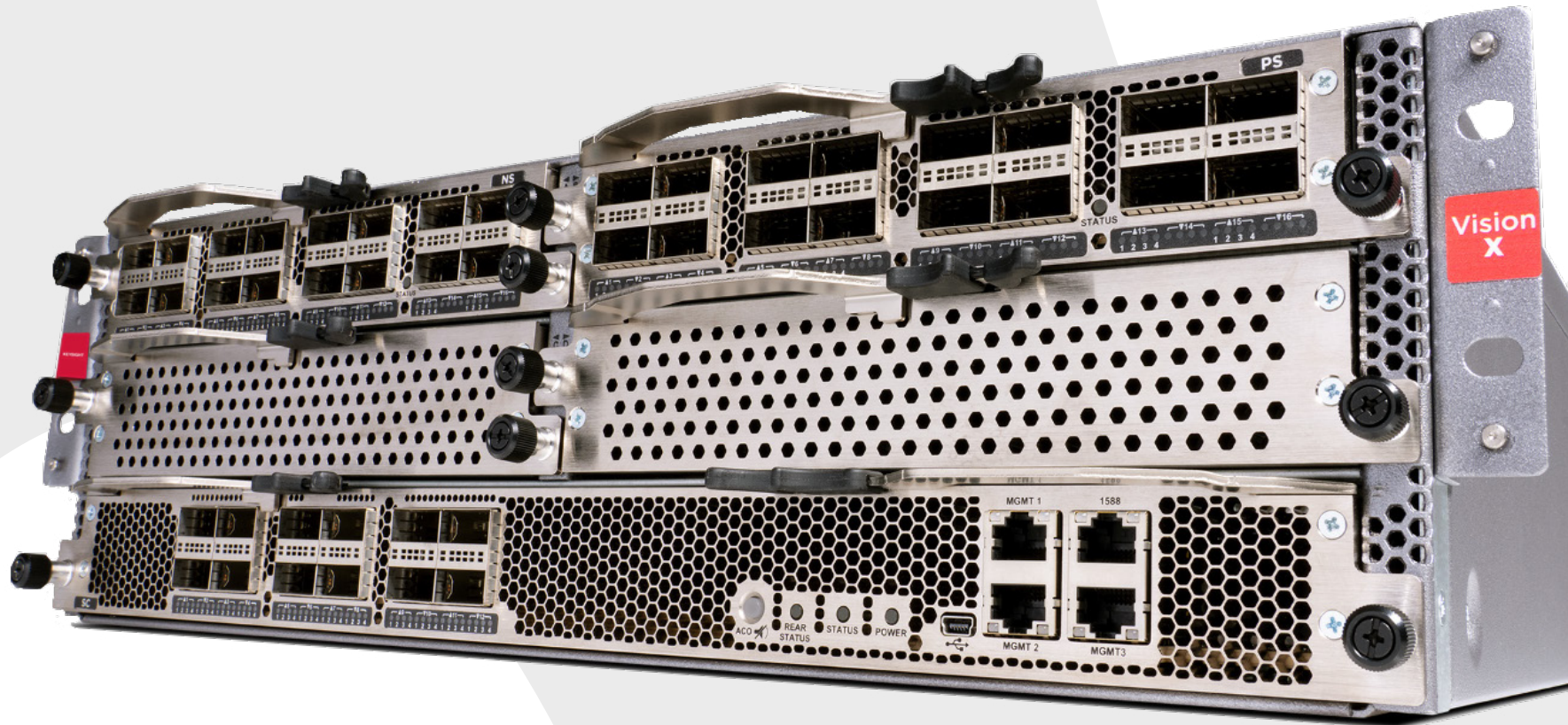
Contents

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.

Delivering dynamic network intelligence relies on network visibility, and Keysight provides a complete suite of products. Keysight Vision network packet brokers (NPBs) are at the core. They help you get the most out of your security and network monitoring tools by delivering filtered, streamlined traffic.

External bypass switches, such as the Keysight iBypass, enable high availability and inline failover to keep your network online. And taps provide a pure and unedited view into traffic on the network, forming the foundation of dynamic network intelligence.

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 and security tight.

GET A CRASH COURSE IN NETWORKING FUNDAMENTALS.
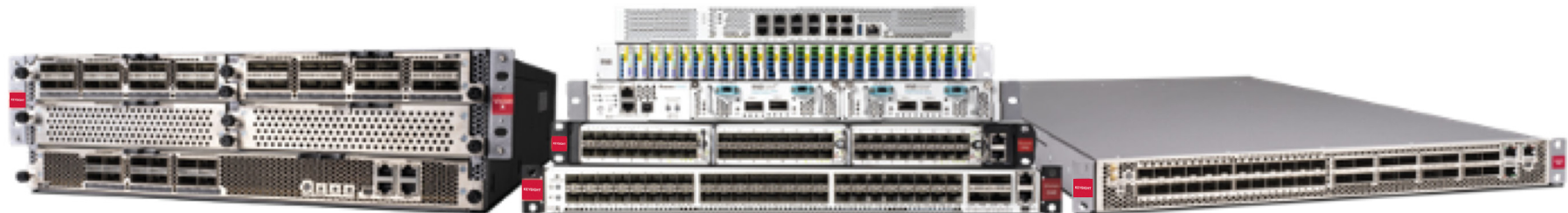
Network Packet Brokers: The Right Data for the Right Tools

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, Keysight 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).

Vision X NPB

Visibility for finance

Keysight TradeVision is a unique product for financial services organizations. It combines market-feed health monitoring with functionality that enables it to monitor 240 million trade / quote messages a second. That is 12 times more than the combined US equities and options markets. With lossless FPGA-based hardware acceleration, precision time-stamping, and tap aggregation capabilities, TradeVision reduces the time required to address potentially costly issues. Additional features include the following:

- Multicast gap detection.
- Advanced latency analytics.
- Micro-burst alerting.
- High-resolution traffic statistics.
- Simplified feed management.

Accredited security for US federal agencies

Government agencies, the military, and other security-conscious organizations require the highest standards of security integrity. That is why all our NPBs meet Common Criteria, FIPS 140–2, and DoDIN APL requirements. And the most recent certifications use a software module approach, which means they will always benefit from the latest software enhancements.

Want to know more?
Learn more about NPBs — what they do and why you need one.

What Is a Network Packet Broker
(AND WHY DO YOU NEED ONE)?

KEYSIGHT
TECHNOLOGIES
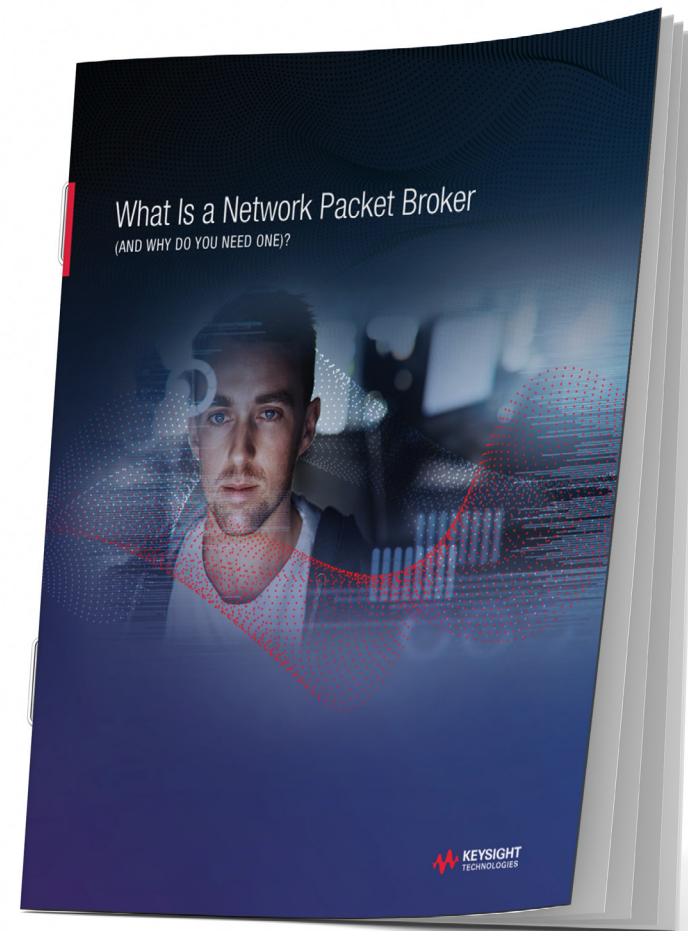
Advanced packet processing and intelligent context-aware filtering

Keysight's robust intelligent visibility feature stacks help you get the most out of Vision Series NPBs and your entire visibility and security platform These software stacks provide filtering based on L2 through L7. Each feature stack has a purpose-built design to ensure you get the best performance, whether in a physical data center or a private, hybrid, or public cloud.

NPB feature stacks offer dynamic network intelligence that extends and enhances the functionality of an NPB with advanced packet processing. See how we stack up.

NetStack

Provides the gold standard baseline for network visibility. It includes robust filtering, load balancing, aggregation, replication, and more, with three stages of filtering (ingress, dynamic, and egress) and a dynamic filter compiler.

PacketStack

Provides intelligent packet filtering, manipulation, and transport with deduplication that removes duplicate packets at full line rate with no loss. Other capabilities include header (protocol) stripping, packet trimming, time-stamping, data masking, and burst protection.

With PacketStack, you can do the following:

- Protect and extend the life of monitoring tools so they operate more effectively.

- Boost tool performance by retaining only needed header bytes and trimming payload to a user-configurable length.

- Hide personally identifiable information, such as credit card and Social Security numbers, before sending data to analysis tools.

- Monitor tools to measure latency, with nanosecond resolution and accuracy, by time-stamping all packets for time-sensitive applications.

- Terminate L2GRE or ERSPAN tunnels from vTap and deliver plain Ethernet traffic to your tools.

- Strip new or proprietary protocols like L3GRE, Jmirror, PBB-TE, LISP, VSL, OTV, and PPPoE using generic header stripping.

SecureStack

Optimizes handling for secure traffic and supports inline and out-of-band SSL / TLS decryption. Data Masking Plus meets Health Insurance Portability and Accountability Act, Payment Card Industry, and other regulatory compliance requirements. Achieve greater visibility by decrypting traffic to quickly detect hidden malware and prevent data loss or security tool bottlenecks.

AppStack

Provides context-aware, signature-based application-layer filtering with accurate and fast application identification, geolocation and tagging, patented signature detection, and optional RegEx

filtering. A simple point-and-click management interface enables you to select application traffic types of interest and filter traffic to tools. AppStack improves monitoring platforms by adding a richer set of geographical, application, and device information.

MobileStack

Offers visibility intelligence for the mobile carrier evolved packet core with General Packet Radio Service Tunneling Protocol, or GPRS Tunneling Protocol (GTP). MobileStack provides Session Initiation Protocol correlation and load balancing, subscriber-specific filtering, subscriber allowlists, and subscriber sampling. MobileStack on Vision X can correlate up to 512 million subscriber sessions and 1,600 GB of user plane traffic per chassis supports 5G performance.

TradeStack

Offers the financial capital markets a simplified market feed data management tool that removes the hassle of configuring, analyzing, and managing market feed data. Features include high-resolution traffic stats down to 0.1 ms resolution, microburst detection, feed health, latency measurement, and gap detection.

With Keysight's modular NPB stacks, you can add only the capabilities and features you need, when you need them. Equipping your NPBs with a full stack of software solutions ensures that your network visibility architecture will evolve and scale to support current and future needs.

Stop hackers with secure traffic processing and SSL / TLS decryption

To prevent blind spots, you need to see all network traffic — both decrypted and encrypted. But the same encryption used to protect your data can be a dual-edged sword. Cybercriminals can attack your network by concealing ransomware and malware within encrypted data, much like a Trojan horse. Beat hackers at their own game by offloading the process-intensive task of SSL / TLS decryption to a Vision Series NPB with SecureStack. Doing so will improve the efficiency of your tools without overloading or impacting their performance.

Active SSL decryption and encryption (TLS 1.3 support)

Security and monitoring tools
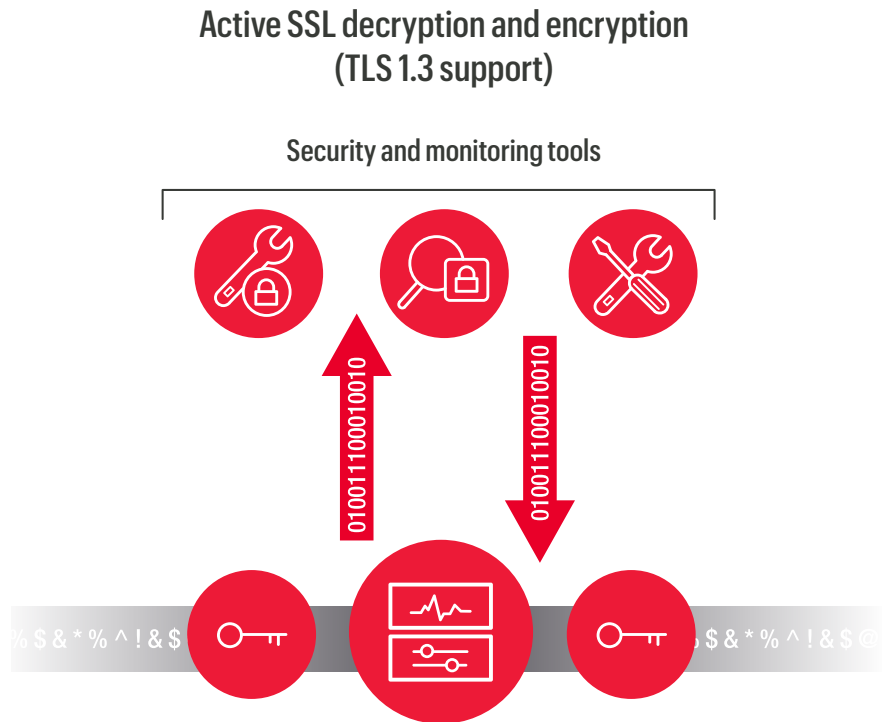
Reduce costs and extend the life of tools with load balancing

Vision NPBs with NetStack perform aggregation and load balancing, breaking data into lower-rate streams to send to the proper tools. Spreading 40 Gbps of traffic across multiple 10 Gbps tools, for example, extends the life of your 10 Gbps tools until you have the budget for more expensive tools that support higher data rates.

Tools

Network packet brokers

40GE

10GE
10GE
10GE
10GE
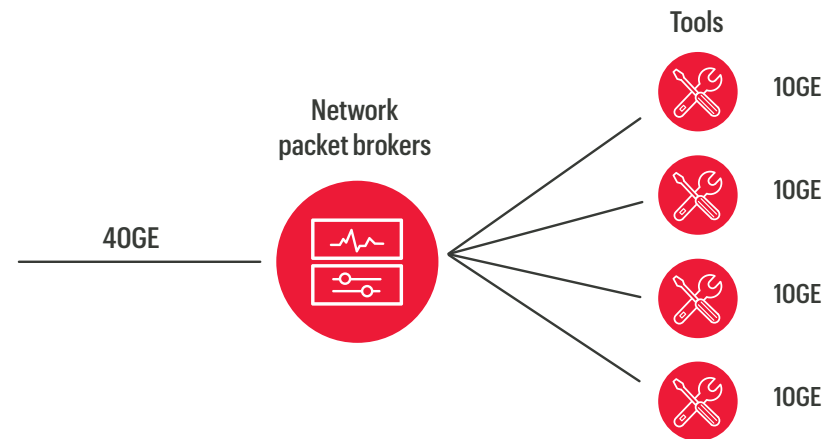
Deduplication increases the efficiency of monitoring and security tools by 35% to 50% by reducing the amount of filtered data sent to tools

Deduplication

Dedupe

Original data

Duplicates removed
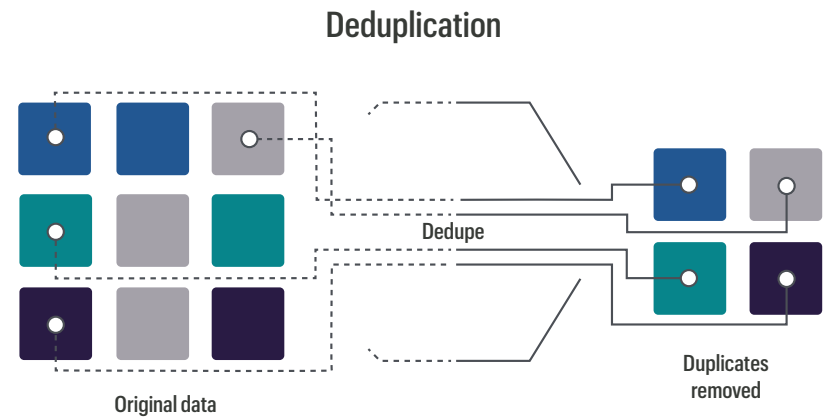
NextGen network packet broker: Vision 400 and E400S
Scale your visibility to 400G speed

Keysight Vision 400 and Vision E400S are the next-generation network visibility solutions. With comprehensive feature sets, they meet the ever-evolving visibility needs of your production network for up to 400 Gbps network speeds.
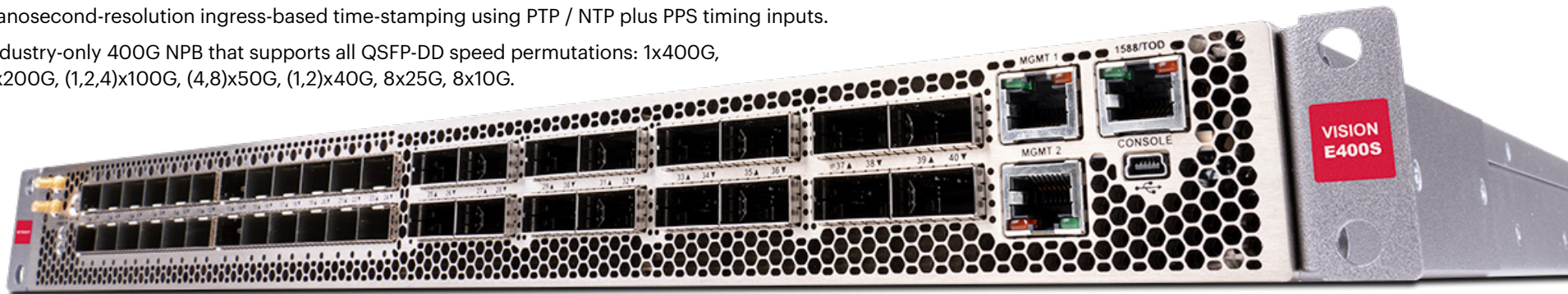
Highly compact and 1RU in size, their front panels provide 24 QSFP56 and 16 QSFP-DD ports. Each QSFP-DD can break out to many smaller speed ports (200G, 100G, 40G, 50 / 25 / 10G) via fan-out cables. They are the only NPBs that support all possible permutations of speeds, increasing the chance of interoperating with legacy devices while maximizing design flexibility.

The reprogrammable nature of the silicon enables fast implementation of a new parser or header-stripping option of any new protocols, well-known or proprietary. New load balance (LB) options support load balancing per port group. In addition to traditional session-aware load balancing, new options allow asymmetric LB, weighted LB, random LB, and LB using tunneled IP header.

The Vision 400 contains a high-performance FPGA, which provides additional PacketStack capabilities beyond the E400S's, such as line rate deduplication, packet trimming, and burst protection.

Highlights

- Compact 1RU NPB that supports 10 / 25 / 40 / 50 / 100 / 200 / 400G port speeds.
- P4 and Tofino-based programmable silicon.
- Full-duplex, non-blocking, and line rate L2 forwarding of 9.2 Tbps.
- Nanosecond-resolution ingress-based time-stamping using PTP / NTP plus PPS timing inputs.
- Industry-only 400G NPB that supports all QSFP-DD speed permutations: 1x400G, 2x200G, (1,2,4)x100G, (4,8)x50G, (1,2)x40G, 8x25G, 8x10G.

Vision E400S

Product	Vision 400	Vision X	Vision ONE	Vision E400S	Vision 7816	Vision Edge 100
Description	Scalable 1RU chassis that supports intelligent visibility stacks for 10 / 25 / 40 / 50 / 100 / 200 / 400G networks	High-performance, high-density, modular, scalable 3RU chassis for 10 / 25 / 40 / 50 / 100G networks	Full-featured, turnkey 10 / 40G visibility in a 1RU form factor	Scalable 1RU chassis for 10 / 25 / 40 / 50 / 100 / 200 / 400G networks	Scalable, high-density, 2RU chassis supporting 10 / 25 / 50 / 100G networks	Cost-effective, high-density rack-level visibility for 10 / 25 / 40 / 50 / 100G
Zero-packet-loss architecture	✓	✓	✓	✓	✓	✓
Dynamic filter compiler	✓	✓	✓	✓	✓	✓
System height (RU)	1	3	1	1	2	1
Advanced packet processing	✓	✓	✓	✓	—	—
Port ingress time-stamping	✓	—	—	—	—	—
AC redundant power supply (hot swap)	✓	✓	✓	✓	✓	✓
DC redundant power supply (hot swap)	✓	✓	✓	✓	✓	✓
Max backplane capacity (Gbps)	9200	6400	640	9200	6400	3200
Max number of 1G ports	0	0	64	0	0	0
Max number of 10G ports	152	108	64	152	128	128
Max number of 25G ports	152	108	0	152	128	128
Max number of 40G ports	32	76	16	32	64	32
Max number of 50G ports	152	108	0	152	128	64
Max number of 100G ports	64	60	0	64	64	32
Max number of 400G ports	16	0	0	16	0	0
Get a quote >	Get a quote >	Get a quote >	Get a quote >	Get a quote >	Get a quote >

Product	Vision Edge 40	Vision Edge 10S	Vision Edge 1S	Vision Edge OS	Vision T1000	TradeVision
Description	Cost-effective rack-level visibility for 1 / 10 / 40G	Ideal for remote site deployments supporting 1 / 10G networks	Compact, cost-effective visibility for branch sites	Disaggregated visibility OS for open switch hardware	Tough NPB designed for harsh environments -40 C to +85 C op. temp.	Market-feed monitoring and tap aggregation for financial markets
Zero-packet-loss architecture	✓	✓	—	✓	—	✓
Dynamic filter compiler	✓	✓	—	✓	—	✓
System height (RU)	1	1	1	(switch dependent)	1	1
Advanced packet processing	—	—	—	—	—	—
Port ingress time-stamping	✓	—	—	(switch dependent)	—	—
AC redundant power supply (hot swap)	✓	✓	✓	(switch dependent)	✓	✓
DC redundant power supply (hot swap)	✓	✓	—	(switch dependent)	✓	✓
Max backplane capacity (Gbps)	720	480	12	(switch dependent)	12	640
Max number of 1G ports	48	48	10	(switch dependent)	26	64
Max number of 10G ports	72	48	4	(switch dependent)	—	64
Max number of 25G ports	0	0	0	(switch dependent)	—	0
Max number of 40G ports	18	0	0	(switch dependent)	—	16
Max number of 50G ports	0	0	0	(switch dependent)	—	0
Max number of 100G ports	0	0	0	(switch dependent)	—	0
Max number of 400G ports	0	0	0	(switch dependent)		
	Get a quote >	Get a quote >	Get a quote >	Get a quote >	Get a quote >	Get a quote >

↓ (icon) Switch dependent

Bypass Switches: Ensure Uptime and Network Availability

External bypass switches are the key to high availability and ease of maintenance for network monitoring and security deployments. While everyone recognizes the need for tools such as intrusion prevention and firewalls, their inline deployment models can create risk or downtime when it is time for reboots, maintenance, or replacement. External bypass switches, such as Keysight iBypass, provide automated failover, which prevents tool updates or downtime from bringing down the network.

Keysight iBypass offers these key features:

- Redundant and serial architecture support.
- High availability: active-active or active-standby.
- Preconfigured heartbeat.
- Centralized management.
- Easy-to-use GUI.

iBypass 100G

Product	iBypass 100G	iBypass DUO	iBypass VHD	iBypass 4 Copper
Description	Single-segment 100G intelligent bypass	High-density bypass with redundant management	Very-high-density, 12-segment intelligent bypass	Single-segment intelligent bypass for copper networks
Speed	100/40G	1G / 10G	1G / 10G	10 / 100 / 1G
Media type	Fiber	Fiber	SFP+ / SFP	Copper
Networks per device	1 or 2 segments	1 or 2 segments	12 segments	1 segments
High availability	Active-active / active-standby	Active-active / active-standby	Active-active / active-standby	—
Configurable	✓	✓	✓	✓
Link fault detection	LFD	LFD / LFDC	LFD / LFDC	LFD / LFDC
	Get a quote >	Get a quote >	Get a quote >	Get a quote >

Which iBypass belongs in your network?

Buying Guide—Which iBypass
Belongs in your Network?

KEYSIGHT
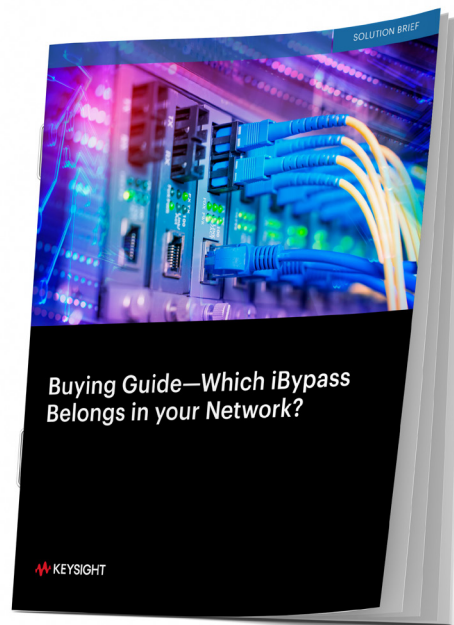
Network Taps:
The Foundation of Dynamic Network Intelligent

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, 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, aggregation taps, and industrial Tough Taps.

Keysight taps offer these key features:

- Provides plug-and-play simplicity.
- Requires no IP address.
- Provides unhackable security.
- Comes in copper and fiber.
- Supports speeds up to 400 Gbps.

Learn more about taps and why they
are critical to network visibility.

Flex Tap

Product	Flex Tap	Flex Tap Secure +	Patch Tap	Copper Tap	Tap aggregators	iLink Aggregator II
Description	Modular, passive fiber taps	Modular, passive fiber taps with optical diode	Low-latency, passive fiber taps	Active copper taps	Active copper taps with aggregation mode	Multiple (x8) copper taps with aggregation[1]
Speed	1G to 400G	1G to 400G	1G to 100G	10 / 100 / 1000 Mbps copper	10 / 100 / 1000 Mbps copper	10 / 100 / 1000 Mbps copper + 4 x SFP+ for aggregation ports
Port type	LC and MTP	LC	LC	RJ45	RJ45	RJ45 / SFP+
Unique features	• 40 / 100G BiDi PSM4, SR4, SR10, and QSFP+ 40G-LX4 • Multiple split ratios and fibers • OM3, OM4, and OS2	• Advanced security prevents accidental or intentional light or data injection • Ideal for lawful intercept, government, military, and other high-security deployments	• Low latency down to < 8nSec • Bend-insensitive • Multimode OM4 • Single-mode OS2	• Independent auto-negotiate (tap low-speed networks and send data to higher-speed tools) • Physical air-gapped monitor ports — data • Diode between tool and monitor ports • Fail-to-wire capability	• Monitors full-duplex traffic with a single NIC • Aggregates both directions into a single monitoring link • Works as a standard or aggregation tap • Offers fail-to-wire capability	• Cost-effective tap aggregator designed to combine traffic from multiple taps • Supports low-medium speeds that high-performance NPB often do not support • Inbuilt taps have fail-to-wire capability
	Get a quote >	**Get a quote >**	**Get a quote >**	**Get a quote >**	**Get a quote >**	**Get a quote >**

1.   Also available as a 16-port SPAN aggregator. 16 x 10 / 100 / 1G input ports and 4 x 10G SFP+ monitor / any-to-any.

Tough taps for industrial environments

Built from the ground up, Keysight Tough Taps are the industry's first ruggedized network taps designed for harsh environments. They meet extended temperature ranges, withstand shock and vibration, and have optimized copper and fiber 10 / 100, 1G, and 10G ports. Tough Taps are certified for Institute of Electrical and Electronics Engineers (IEEE) standards, including IEEE 1613 for safety and IEC 61850 for communication protocols for intelligent electrical devices.

The Copper Tough Taps offer out-of-band monitoring for security and performance tools and duplicate all packets for full visibility. For extra uptime protection, these taps have redundant terminal block power connectors. If the primary power source fails, the tap automatically switches to the backup power source. If both input power sources fail, the tap will still pass traffic between its network ports (fail-open).

The Flex Tough Taps collect and archive network traffic. Optimized for run-to-fail fiber networks with old and new fiber modes found in remote substations, these taps are TAA-compliant. You can deploy them at any inline connection on the network.

Flex Tough Tap

Copper Tough Tap

Product	Copper Tough Taps	Flex Tough Taps
Description	Industrial active copper taps	Industrial multimode, modular, passive fiber taps
Speeds	10 / 100 / 1000 Mbps copper	1G to 400G
Port types	RJ45	LC
Certification, standards, and compliance	TAA; IEC 61000-4-2,3,4,5,6,8,11; IEC 60068-2-6; IEEE-1613; UL 508 Listed; UL 60950-1; EN60950-1; CE; IEC 61850	TAA; CE; RoHS 10
Unique features	• Supports Power over Ethernet (PoE) • Auto speed negotiation • Secured by design — with no management interface or IP address, it is unhackable • Physical air-gapped monitor ports — data diode between tool ports and monitored ports prevents malicious injections from monitoring network • Silent operation • DIN rail mountable • Fan-less • Operating temperature range -40 C to +85 C	• No power required • Secured by design — with no management interface or IP address, it is unhackable • Passes all traffic (including errors) from all layers • Compact — 4 taps in one module • Completely passive, optical device • OM1, OM5 multimode models in 70 / 30 split ratio • Deploy at any inline network connection • DIN rail mountable • Same form factor as Copper Tough Tap • Operating temperature range -40 C to +85 C
	Learn more >	**Learn more >**

Cloud Visibility

CloudLens powers better security, visibility, and performance monitoring for the cloud

Keysight CloudLens, the public, private, and hybrid cloud visibility platform, enables packet capture, filtering, and analysis to provide dynamic network intelligence in any cloud environment. With its unique cloud-native architecture, CloudLens is a natural fit for cloud-only and cloud-first strategies, along with organizations that use multi-cloud or hybrid environments.

When network security and performance matter most, organizations trust CloudLens to shed light on their most vulnerable blind spots.

CloudLens offers these key features:

- Captures and forwards full packets and NetFlow from virtual machines, containers, or inter-Pod network traffic to tools.
- Operates as a virtualized network packet broker, allowing aggregation, filtering, and deduplication of virtual network traffic all within the cloud.
- Auto-scales elastically, on-demand with cloud instances.
- Is multi-platform capable, cloud service provider- and platform-agnostic.

Visibility Central Management: Manage Many NPBs Through a Single Pane of Glass

Networks are growing increasingly complex, as is the task of extracting dynamic network intelligence information from them. A visibility fabric consisting of NPBs, bypass switches, and taps provides a good foundation for your network. Then you need to manage and coordinate all these systems. That is where Keysight Visibility Central Management comes in.

Centralized management enables you to oversee hundreds of devices with monitoring, scheduled configuration changes, and bulk software upgrades. You can import or export configurations, run scripts, view bandwidth utilization, and more. Additionally, you can customize dashboards and integrate them with other network management systems via northbound interfaces.

Keysight centralized management offers these key features:

- Single-pane-of-glass management.
- Device auto-discovery.
- Single-sign-on and zero-touch provisioning.
- Physical or virtual form factors.
- High availability with floating primary / backup IP.
- RADIUS, TACACS+, and LDAP authentication.

Hawkeye

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

As an active monitoring platform, Keysight Hawkeye can help you continuously manage performance and connectivity across your network. Hawkeye makes it simple to monitor remote sites, data centers, cloud services, and more — all from a single tool.

Whether you are measuring remote user experience over voice applications, branch office users on Wi-Fi, or general connectivity to your software-as-a-service 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 quality-of-service tests.
- Voice, video, and unified communication tools monitoring with turnkey integrations.
- The ability to see all your performance data in a single interface and set custom alarms.
- Wi-Fi 6 and wireline monitoring.
- A wide choice of hardware platforms, such as Vision 10S, XR3000, IxTap, and IxProbe.
- Speeds from 100M to 10G.
- Software versions.

Hawkeye Monitor Console
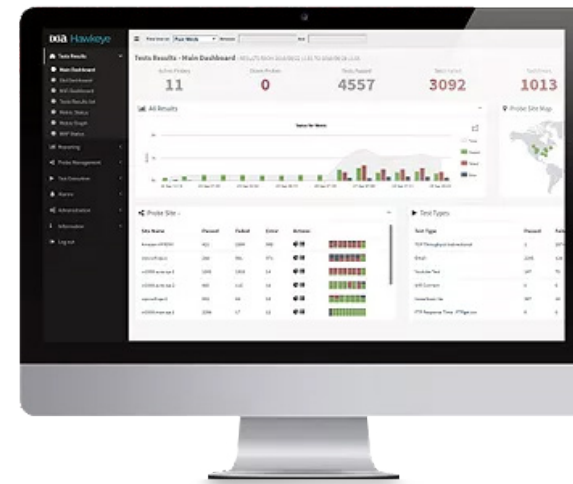
Hawkeye Endpoints

TimeKeeper

Intelligent end-to-end software driven clock synchronization

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 and Infrastructure Security Agency strongly advise that users of time services harden their timing infrastructure and take steps to detect and react to timing anomalies. Many internal systems and security processes rely on correct and unambiguous time. Disruption of timing signals such as global navigation satellite system (GNSS), Network Time Protocol, or Precision Time Protocol can disrupt critical systems.

Keysight TimeKeeper software, installed on servers, replaces standard timing daemons. It enables enterprises, service providers, and governments 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 detects and alerts on timing anomalies. More than 100 financial institutions and multiple governments worldwide have installed TimeKeeper.

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.
- Ability to serve time and manage hundreds of clients with TimeKeeper Server.

Visibility Support Programs

Flexible support options

Highlights of our global visibility support options include the following:

- Rapid response and problem resolution.
- Technology life cycle expertise throughout ramp-up, configuration, debugging, and new feature and services rollout.
- Full-service hardware repair and rapid interchange of field-replaceable modules.
- Recommendation of new releases and features that support changing business needs.
- Immediate access to the latest software releases, including new features, enhancements, and patches.
- Fast, easy online access to an extensive library of white papers, black books, product documentation, and license management.
- Daily software scans for proactive visibility and fix resolution for popular and zero-day common vulnerability exposures.
- Three optional support levels.

Support agreement features	Basic[1]	Essential	Enterprise 24/7
Response time	1 – 2 business days	2 business hours	2 clock hours
Live support (business hours)	✓	✓	✓
After-hours live support	—	—	24x7x365
After-hours software / hardware upgrades and debug	—	—	24x7x365
Repair service	Return and repair[2]	Advanced hardware replacement	Advanced hardware replacement
Advanced hardware replacement[3]	First 90 days after new product shipment	✓	✓
Expedited hardware shipment from regional inventory[4]	—	✓	✓
Phone, email, customer portal access (business hours)	✓	✓	✓
After-hours phone, email, customer portal	—	—	24x7x365
Software upgrades and bug fix patches[5]	✓	✓	✓
Resource library 24/7	✓	✓	✓
Customer satisfaction health checks	✓	✓	✓
Dedicated support advocate for escalation and QBR[6]	—	—	✓

1. Purchase includes 12-month basic support after product shipment.
2. Requires seven to 10 business days to repair equipment.
3. Replacement hardware shipped in one to two business days.
4. Only available in select countries. Please contact your local Keysight representative.
5. New feature software upgrades, service pack enhancements, bug fix patches, and emergency hot fixes.
6. At your request, and up to once per calendar quarter, a director-level support advocate for escalation will meet with you for a quarterly business review. You will discuss existing and closed technical support cases and updates on any open actions, and you may share your insight into areas where we can improve.

KEYSIGHT