KEYSIGHT TECHNOLOGIES

Network Visibility Products Catalog

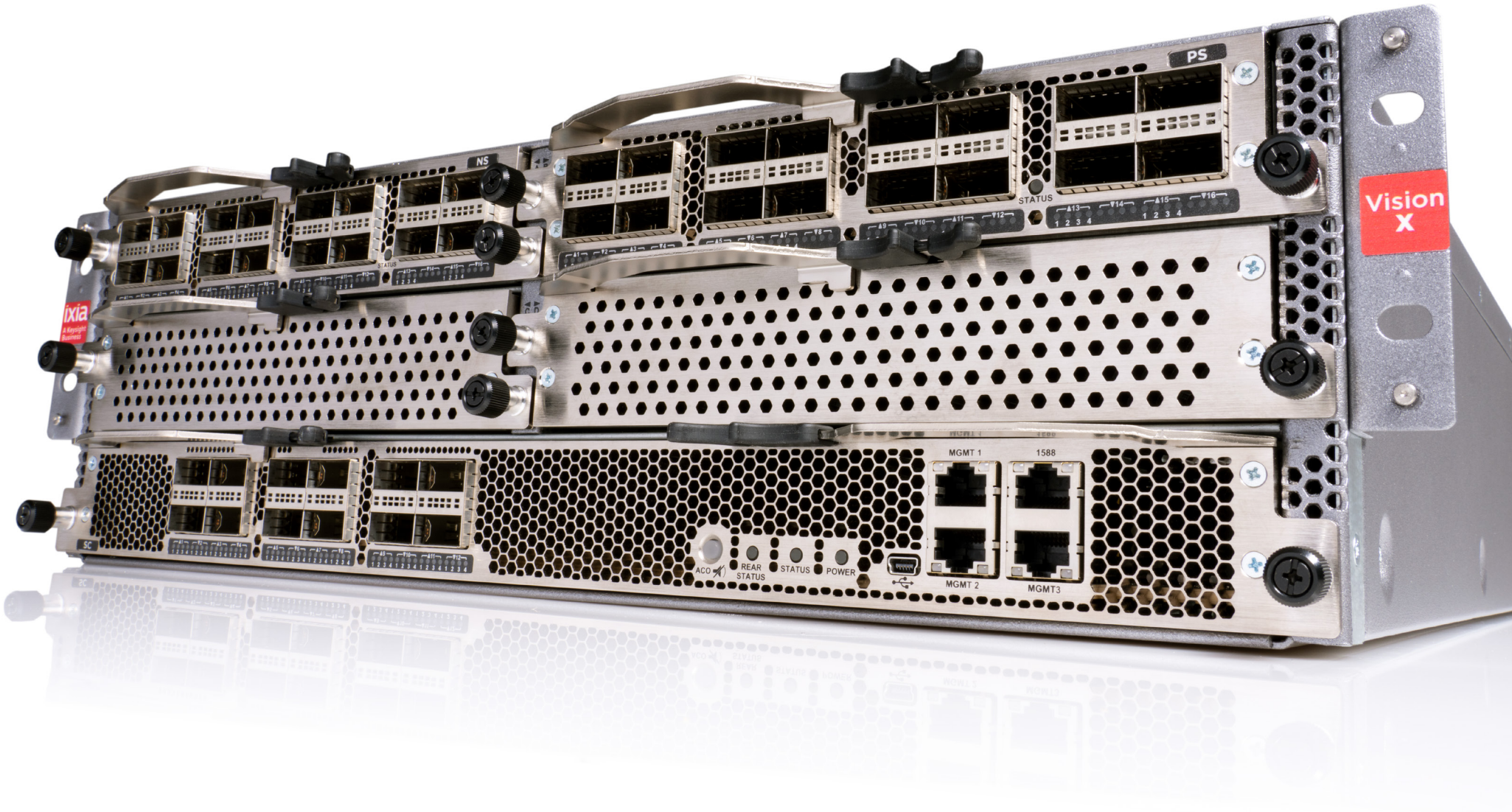


TABLE OF CONTENTS

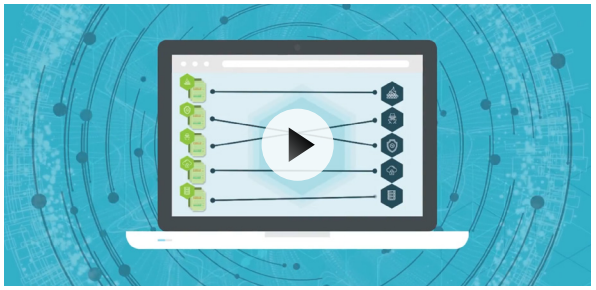
Connect and Secure the World with Dynamic Network Intelligence

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.

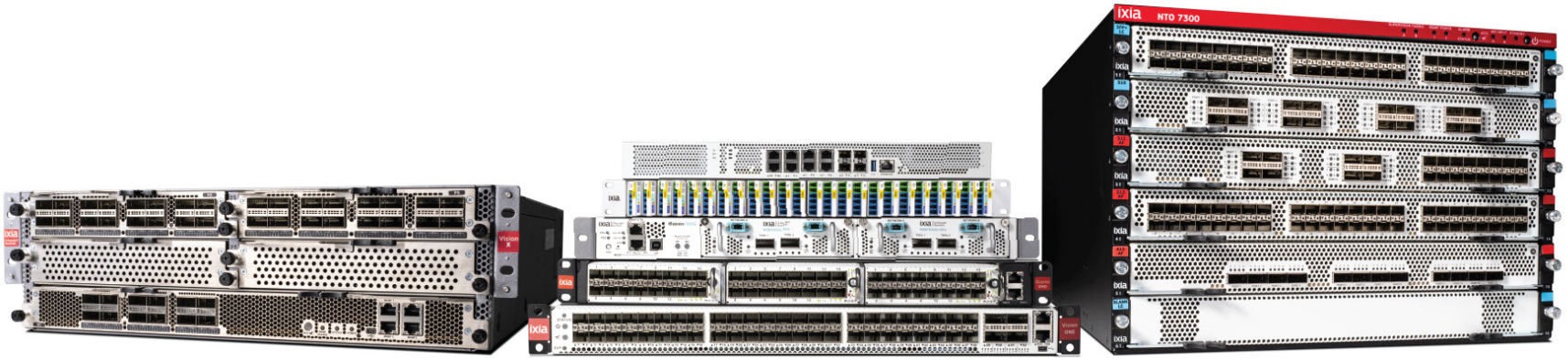
Keysight can help. Customers rely on our solutions to deliver rich data about network traffic, applications, and users across any networking environment. This deep insight is what we call dynamic network intelligence. It helps you continuously innovate, meet aggressive service-level agreements, and keep 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.



Watch the video series



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)

Learn more

Vision X NPB

VISIBILITY FOR FINANCE

TradeVision is a unique product for financial services organizations. It combines market-feed health monitoring with best-in-class functionality that enables it to monitor 240 million trade/quote messages a second. That's 12 times more than the entire US equities and options markets combined. 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:

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

ACCREDITED SECURITY FOR US FEDERAL AGENCIES

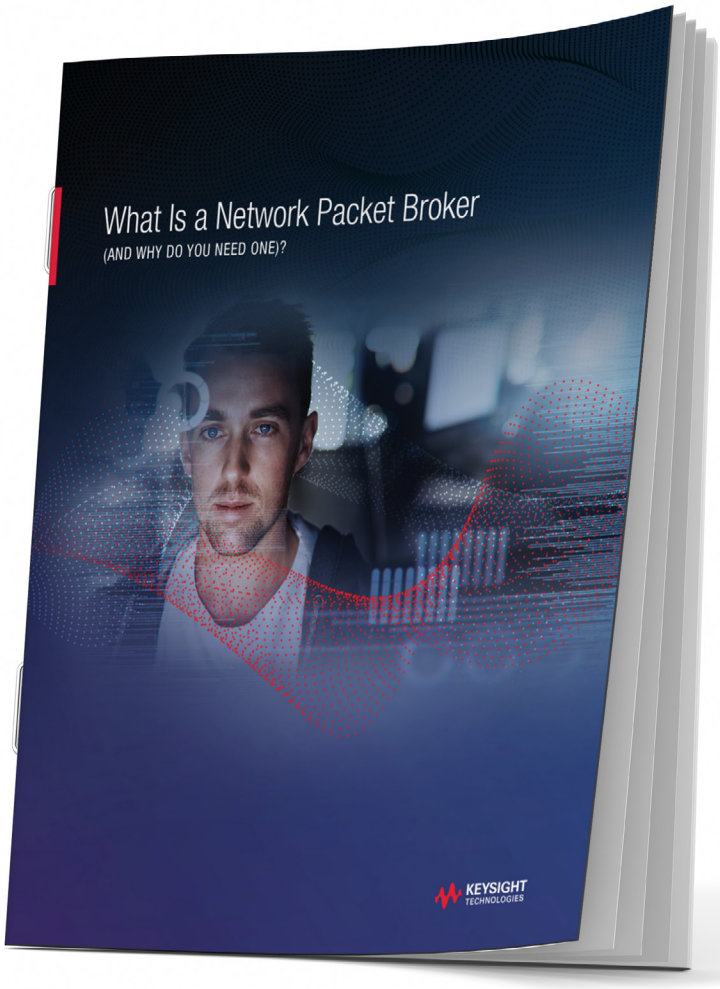
Government agencies, military, and other security-conscious organizations require the highest standards of security integrity. That's why all of our NPBs are Common Criteria, FIPS 140–2 and DoDIN APL listed. And, the most recent certifications utilize a software module approach, which means they will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

Learn more

WANT TO KNOW MORE?

Learn more about NPBs — what they do, and why you need one.

Download brochure



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 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 timestamping 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. Supports inline and out-of-band SSL / TLS decryption and threat intelligence. Data Masking Plus meets Health Insurance Portability and Accountability Act, Payment Card Industry, and other regulatory compliance requirements. Achieve greater visibility by decrypting traffic so you can 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 allows 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.

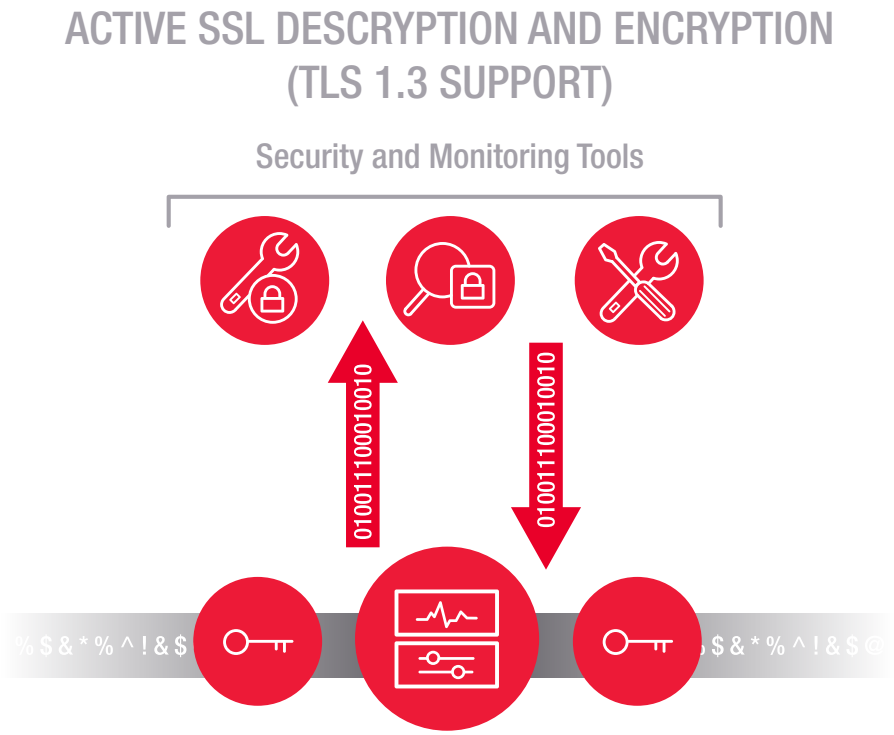
MobileStack: Offers visibility intelligence for the mobile carrier evolved packet core with General Packet Radio Service Tunneling Protocol, or GPRS Tunneling Protocol (GTP). MobileStack provides Session Initiation Protocol correlation and load balancing, subscriber-specific filtering, subscriber allow lists, 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 and is designed to support 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 millisecond resolution, microburst detection, feed health, 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.

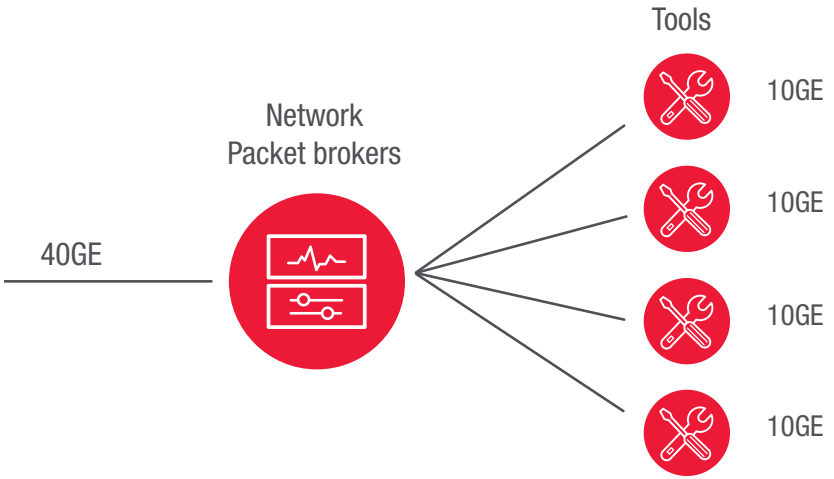
STOP HACKERS WITH SECURE TRAFFIC PROCESSING AND SSL / TLS DECRYPTION

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.

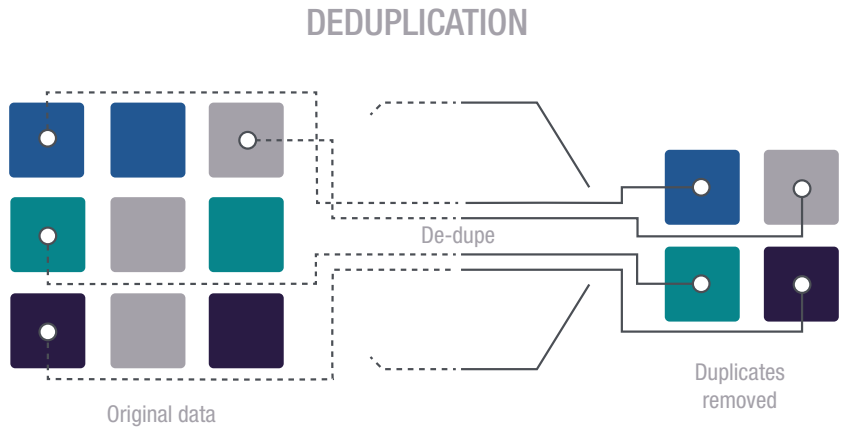


REDUCE COSTS AND EXTEND THE LIFE OF TOOLS WITH LOAD BALANCING

Vision NPBs with NetStack perform aggregation and load balancing, breaking data down 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 budget for more expensive tools that support higher data rates.



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



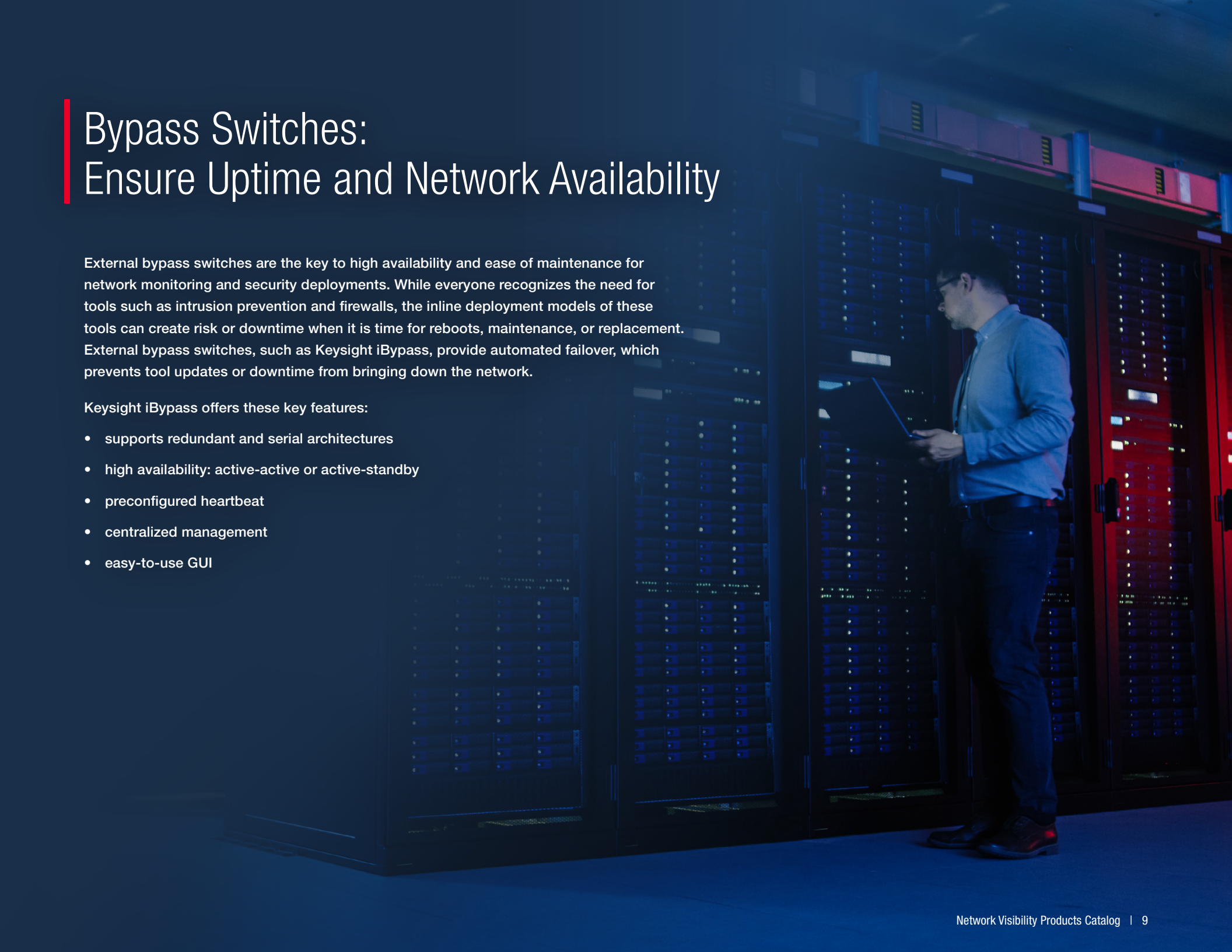
Product	Vision X	Vision ONE	Vision 7816	Vision Edge 100	Vision Edge 40	Vision Edge 10S	Vision Edge 1S	Vision Edge OS	TradeVision
Description	High-performance, high-density, modular, scalable 3RU chassis for 10 / 25 / 40 / 50 / 100G networks	Full-featured, turnkey 10 / 40G visibility in a 1RU form factor	Scalable, high-density, 2RU chassis supporting 10 / 25 / 50 / 100G networks	Cost-effective, high-density rack-level visibility for 10 / 25 / 40 / 50 / 100G	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	Market-feed monitoring and tap aggregation for financial markets
Zero-packet-loss architecture	✓	✓	✓	✓	✓	✓	-	✓	✓
Dynamic filter compiler	✓	✓	✓	✓	✓	✓	-	✓	✓
System Height (RU)	3	1	2	1	1	1	1	Switch dependent	1
AC redundant power supply (hot swap)	✓	✓	✓	✓	✓	✓	✓	Switch dependent	✓
DC redundant power supply (hot swap)	✓	✓	✓	✓	✓	✓	-	Switch dependent	✓
Max backplane capacity (Gbps)	6400	640	6400	3200	720	480	12	Switch dependent	640
Max number of 1G ports	0	64	0	0	48	48	10	Switch dependent	64
Max number of 10G ports	108	64	128	128	72	48	4	Switch dependent	64
Max number of 25G ports	108	0	128	128	0	0	0	Switch dependent	0
Max number of 40G ports	76	16	64	32	18	0	0	Switch dependent	16
Max number of 50G ports	108	0	128	64	0	0	0	Switch dependent	0
Max number of 100G ports	60	0	64	32	0	0	0	Switch dependent	0
	GET A QUOTE	GET A QUOTE	LEARN MORE	GET A QUOTE	GET A QUOTE	GET A QUOTE	GET A QUOTE	GET A QUOTE	GET A QUOTE

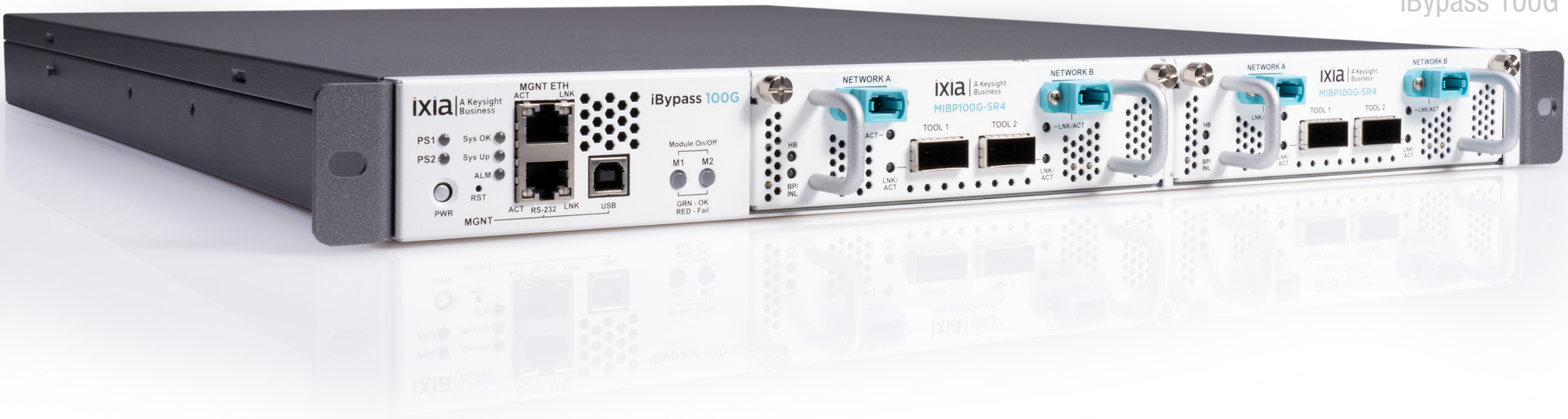
Bypass Switches: Ensure Uptime and Network Availability

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, the inline deployment models of these tools 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:

- supports redundant and serial architectures
- high availability: active-active or active-standby
- preconfigured heartbeat
- centralized management
- easy-to-use GUI





Learn more about Keysight bypass switches

Product	iBypass 100G	iBypass DUO	iBypass VHD	iBypass HD	iBypass 4 Copper
Description	Single-segment 100G intelligent bypass	High-density bypass with redundant management	Very-high-density, 12-segment intelligent bypass	High-density, 8 segment intelligent bypass	Single-segment intelligent bypass for copper networks
Speed	100/40G	1G / 10G	1G / 10G	10 / 100 / 1G	10 / 100 / 1G
Media type	Fiber	Fiber	SFP+ / SFP	Copper or fiber	Copper
Networks per device	1 or 2 segments	1 or 2 segments	12 segments	8 segments	1 segment
High availability	Active-active / active-standby	Active-active / active-standby	Active-active / active-standby	Active-standby	-
Configurable	✓	✓	✓	✓	✓
Link fault detection	LFD	LFD / LFDC	LFD / LFDC	LFD	LFD / LFDC
	GET A QUOTE	GET A QUOTE	GET A QUOTE	GET A QUOTE	GET A QUOTE

AN OLD BYPASS SWITCH CAN BE A LIABILITY. LEARN WHY AN UPGRADE IS WORTH THE INVESTMENT.

Download the product brief

Network Taps: The Foundation of Dynamic Network Intelligence

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, aggregation taps, and industrial Tough Taps.

Keysight taps offer these key features:

- plug and play
- no IP address
- secure and unhackable
- copper and fiber
- speeds up to 400 Gbps

Learn more about Keysight taps

LEARN MORE ABOUT TAPS AND WHY THEY ARE CRITICAL TO NETWORK VISIBILITY.

Download the solution brief

Flex Tap

Product	Flex Tap	Flex Tap Secure+	Patch Tap	Copper Tap	Tap Aggregators
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
Speeds	1G to 400G	1G to 400G	1G to 100G	10 / 100 / 1000 Mbps copper	10 / 100 / 1000 Mbps copper
Port types	LC and MTP	LC	LC	RJ45	RJ45
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 • bend-insensitive • multi-mode 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 ports and monitored ports enhances security by preventing malicious injections into the monitoring network. • wide flexibility and coverage	• monitors full-duplex traffic with a single NIC • aggregates both directions into a single monitoring link • works as a standard tap or aggregation tap
	GET A QUOTE	GET A QUOTE	GET A QUOTE	GET A QUOTE	GET A QUOTE

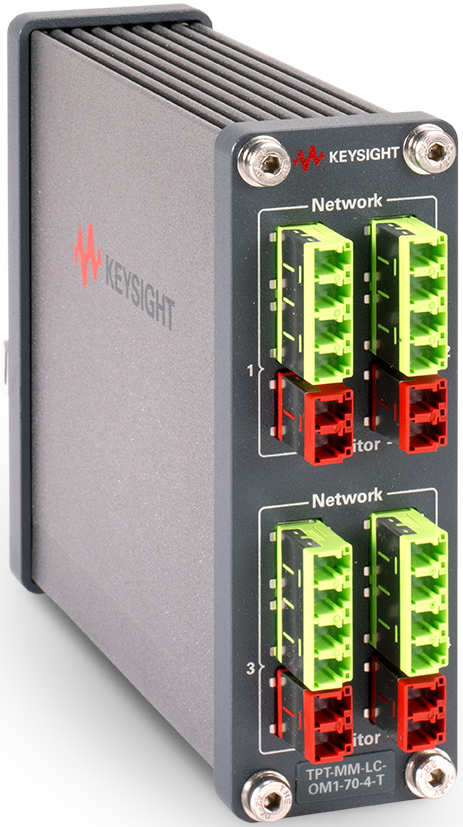
TOUGH TAPS FOR INDUSTRIAL ENVIRONMENTS

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 has 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 Fiber Flex Tough Taps collect and archive network traffic. They are optimized for "run to fail" fiber networks with both old and new fiber modes found in remote substations. These taps are TAA compliant, and you can deploy them at any inline connection on the network.

Fiber Flex Tough Tap



Copper Tough Tap

Product	Copper Tough Taps	Fiber Flex Tough Taps
Description	Industrial active copper taps	Industrial multi-mode, modular, passive fiber taps
Speeds	10 / 100 / 1000 Mbps copper	1G to 400G
Port types	RJ45	LC
Certifications, 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 cannot be hacked • 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	• No power required • Secured by design — with no management interface or IP address, it cannot be hacked • Passes all traffic (including errors) from all layers • Compact — 4 taps in one module • Completely passive, optical device • OM1, OM5 multi-mode models in 70 / 30 split ratio • Can be deployed at any inline network connection • DIN rail mountable • Same form factor as Copper Tough Tap • Color-coded LC connectors
	LEARN MORE	LEARN MORE

Ixia Fabric Controller Centralized Manager: Single-Pane-of-Glass Network Visibility

Networks are growing increasingly complex, as is the task of extracting dynamic network intelligence information from them. Having a visibility fabric consisting of NPBs, bypass switches, and taps is a good start. What comes next is managing and coordinating all these systems. That is where Keysight's Ixia Fabric Controller Centralized Manager (IFC CM) comes in.

IFC CM enables you to manage 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 with other network management systems via northbound interfaces.

Keysight IFC CM offers these key features:

- single-pane-of-glass management
- device auto-discovery
- SSO and zero-touch provisioning
- physical or virtual form factors
- high availability with floating primary / backup IP
- RADIUS, TACACS+, and LDAP authentication

Get a quote