Network Performance and Security Products

CATALOG



KEYSIGHT

Table of Contents

3
Introduction

5
Threat Simulator

7
ThreatARMOR

10
Hawkeye

14
SSL VPN Assessment Service

Avoid Attacks and Maintain Peak Performance with Dynamic Network Intelligence

A lot is riding on your network. You need to connect your users, secure critical applications, and protect sensitive data. Network uptime, user experience, and security are more important than ever — but minimizing service disruptions and preventing attacks has never been more challenging:

- Distributed network applications, edge computing, and SD-WAN make it difficult to see everything at once.
- Dispersed employees increase your attack surface and make it harder to maintain consistent quality of service (QoS) — especially as more work from home.
- Misconfigured tools are constantly exploited by attackers and leave you blind to performance problems.

You need a source of truth. Keysight can help. As the world leader in application and threat intelligence, companies trust our solutions to deliver a combination of proactive insight and real-time analytics from every corner of their networks — spanning cloud, virtual, and on-premises infrastructure. Armed with this dynamic network intelligence, you will find it easier to prevent performance problems and avoid attacks.

Don't wait for costly surprises to threaten security or user experience. Discover our network performance and security products to see why 77 of the Fortune 100 depend on dynamic network intelligence.

What is dynamic network intelligence?

Download the eBook





Hack yourself before attackers do. See how Keysight Threat Simulator helps you identify and remediate vulnerabilities in your security operations.

Watch the on-demand webinar

Threat Simulator: Breach and Attack Simulation Platform

Security is never static. New threats are ever-present, and misconfigurations can compromise your network in an instant. While it may sound counterintuitive, you need to attack yourself — before someone else does. By safely simulating the entire kill chain on your production network, you can definitively measure risk, expose gaps, and course-correct with step-by-step remediations.

Built on 20+ years of leadership in threat intelligence and security testing, Keysight Threat Simulator makes it easy to continuously validate your defenses and prove you're safer than you were yesterday. With turnkey SIEM integrations and 24/7/365 updates from our Threat Intelligence database, Threat Simulator empowers your security operations (SecOps) team to take control of a rapidly changing attack surface.

Deployment	Licensing	Simulated attacks	Tool assessments	SIEM integrations	Update frequency	Product-specific remediations	Safe for production network	Automated assessments
Software-as-a-Service (SaaS)	Annual	Malware, spear phishing, cross-site scripting, data exfiltration, database exploits, advanced persistent threats, cryptojacking, and more	WAF, IDS, IPS, DLP, URL filtering, gateway antivirus, malware sandbox	IBM QRadar, Splunk	Continuous updates to attack library from Keysight Application and Threat Intelligence (ATI) Research Center	✓	✓	✓

Get a quote

Threat simulator

Get an at-a-glance view of your network's security posture with an intuitive product dashboard.

See exactly how secure you are at any given time.

Drill down on specifics to see which audits your security tools are passing, and which ones they are having trouble with.



ThreatARMOR: Threat Intelligence Gateway

Attackers are tenacious, but they aren't perfect. Many threats are preventable — yet breaches remain as prevalent as ever. SecOps teams work tirelessly to prevent attacks, but the sheer volume of SIEM alerts is immense, and you may often miss vital clues.

You need to reduce your attack surface — and that means stopping attackers from ever entering your network. That's why SecOps teams rely on ThreatARMOR to prevent malicious IP traffic from ever accessing their network in the first place. As bad actors continually circumvent firewall filters, threat intelligence gateways like ThreatARMOR give you a more resilient defense — drawing from a continuously-updated database of known attackers to block threats by location, not behavior.

Deployment	Licensing	Available speeds	Inbound IP blocking	Outbound IP blocking	Failsafe resiliency	Full line-rate performance	Proof of malicious activity	Technical support
On-premises (1RU)	Front panel LCD display, cloud-based controller	1 G, 10 G	Known-bad sites and untrusted locations	Botnet communication from infected internal systems	Built-in bypass mode and dual-redundant power supplies	✓	✓	✓

Get a quote

ThreatARMOR

Protection score shows you exactly how secure your network is. No analysis required.

See where threats are coming from — and block them at line rate.



Arm yourself with an industry-leading application and threat intelligence expertise

When it comes to security, you cannot afford to fall behind. ThreatARMOR and Threat Simulator are backed by Keysight's Application and Threat Intelligence (ATI) Research Center which is built on decades of industry-leading expertise. Our elite group of global security researchers keep your SecOps team updated with the latest known threats and exploits. Our database contains more than 50 million records, and millions of new threats are analyzed and cataloged each month.

Whether you're emulating the latest attacks or preventing emerging threats from gaining a foothold in your network, you can trust your team is a step ahead with Keysight ATI.

Discover how to protect your network with threat intelligence.

Download the white paper



Hawkeye:
Active Network Monitoring Platform

Your network team supports a broad range of applications (including unified communications (UC), VoIP, and video) — all with varying degrees of sensitivity to latency and loss. But when it comes to monitoring performance, passively waiting for live network data is not enough. If you want to find connectivity issues or performance problems before your subscribers do, you need to be proactive.

That's why organizations trust Hawkeye to make sure their network is ready for whatever comes next. With active network monitoring, you can minimize costly downtime by continuously testing, validating, and monitoring quality of service — from your centralized applications to your users on the network's edge.

Deployment	Licensing	Testing types, capabilities	KPIs	Alarms	API control	Synthetic test library	Machine learning	Real-time data, results	Automated schedule
On-premises (software-based platform)	Web-based controller with integrated metrics dashboard	Node-to-node, mesh, real service, application / web / Wi-Fi monitoring	Basic and advanced metrics	SNMP and email	SOAP API	✓	✓	✓	✓

Get a quote



Detect, diagnose, and remediate issues before they cause costly rework and leave a lasting impact.

Learn the essentials of an active monitoring strategy.

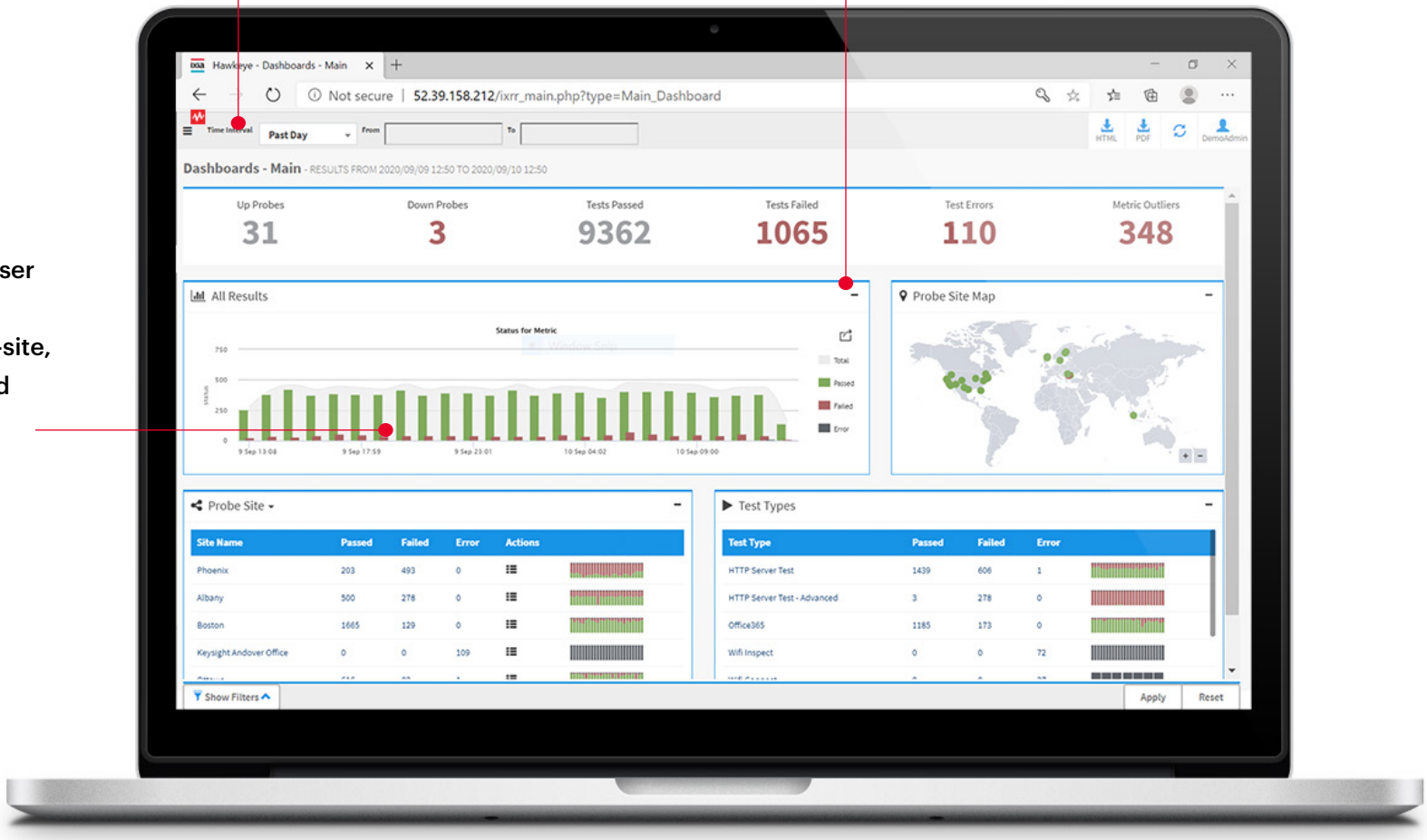
Get the guide

Hawkeye

An easy-to-use dashboard enables you to monitor performance from core to edge from a single pane of glass.

Pass / fail metrics deliver actionable insight.

Take control of the user experience. Monitor performance site-to-site, spot issues early, and troubleshoot faster.



Hawkeye endpoints: maximum coverage in a minimal footprint

You can't manage what you don't measure. When business depends on peak performance, blind spots are costly liabilities — slowing troubleshooting, lengthening outages, and undermining productivity when something goes wrong. You need to know what's happening everywhere, 24/7.

Hawkeye enables you to monitor user experience from your data center to your network's edge with a full suite of performance monitoring endpoints. Unlike purely Software-as-a-Service (SaaS)- solutions, you can easily deploy a full range of hardware- and software-based endpoints across your network — including network packet brokers, inline monitoring probes, and more.

Learn more about Hawkeye endpoints

Hawkeye endpoints	Typical application	Interface	Synthetic monitoring	Inline monitoring	Fail to wire	Packet capture, statistics, aggregation, filtering	NetFlow, deduplication	Local management	Remote provisioning
Virtual / Software (Docker, Cloud, Android, iOS, Microsoft Windows, Linux, Mac)	In conjunction with other endpoints	Ethernet, virtual, Wi-Fi, mobile, wireless	✓						✓
Vision E1S NPB	Large offices	4x 10 G (SFP+), 6x 1 G BASE-T, 2x 1 G BASE -T, 1x USB, 1x RJ45	✓			✓	✓	✓	✓
IxProbe	Branch locations or small offices	2x 1 G	✓	✓	✓			✓	✓
XRPI	Small offices	1x Wi-Fi, 1x FE, 2.4 GHz, 5 GHz, AC	✓						✓

SSL VPN
Gateway Assessment Service

A robust VPN infrastructure is a crucial part of any network architecture — even in the best of times. It is even more vital when a crisis hits, and business continuity depends on employees being able to work remotely. To prepare, not only do you need to provision enough VPN capacity for the usage surge, but you also need to validate that your network can smoothly support your critical applications at peak traffic loads.

Instead of hoping you have properly dimensioned and deployed your VPN gateways, why not let us help you? Rather than waiting for users to report connectivity issues, you can proactively validate your VPN capacity with a controlled, realistic performance test. With Keysight's gateway assessment service, you can identify bottlenecks, optimize your security policies, and rest assured your network is always prepared for the unexpected.

Testing as a service	Bandwidth-per-tunnel test	Usage capacity test	Connection time test	Throughput analysis	Live network impact	Average duration per assessment	Required information
✓	✓	✓	✓	✓	None	4 hours	SSL VPN address

Get a quote

SSL VPN gateway assessment service

Review the results of your VPN gateway assessment from a central dashboard.

How many users can your VPN gateway support? How much bandwidth per tunnel can it sustain? Get answers to these critical questions, and many more.





Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.

This information is subject to change without notice.
© Keysight Technologies, 2020 – 2023, Published in USA, January 9, 2023, 7120-1242.EN