

Building a Foundation for Zero Trust Network Security



A Brief History of Keysight



1939–1998:
Hewlett-Packard years

A company founded on electronic measurement innovation

1999–2013:
Agilent Technologies years

Spun off from HP, Agilent became the World's Premier Measurement Company

In September 2013, it announced the spinoff of its electronic measurement business

2014+:
Keysight years

On November 1, Keysight became an independent company focused on the electronic measurement industry

2020

Keysight Technologies at a Glance

FY20 KEY STATISTICS

#1
Market Position¹

~30K
Total Customers²

100+
Countries Served

~\$20B
Market Cap^{3,4}

22
R&D Sites⁵

3,500+
Patents⁶

~13.9K
Employees

25%
Operating Margin^{3,7}

¹As per company estimate

²Includes indirect channel

³As of fiscal year end

⁴As per external sources

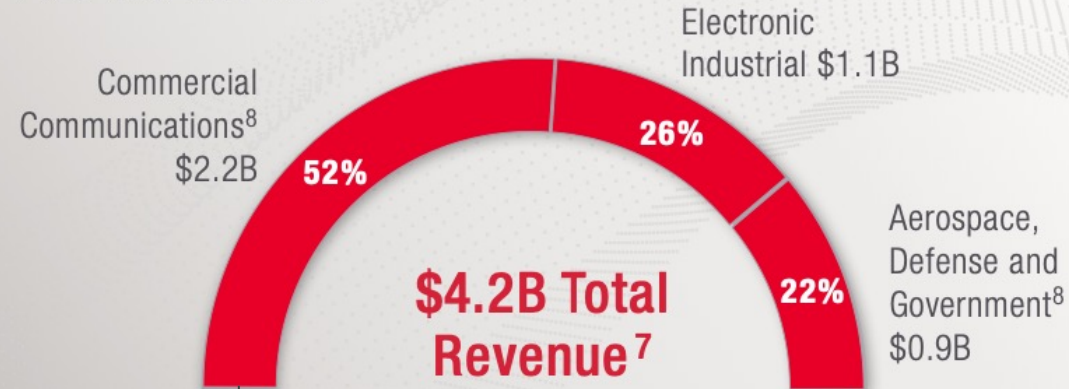
⁵Sites with > 50 R&D engineers

⁶Patents awarded to Keysight and Keysight's business under Agilent and HP as well as to companies acquired by Keysight

⁷Non-GAAP measure

⁸Communication Solutions Group: \$3.1B

FY20 REVENUE MIX



Enterprise Solutions
is part of
Commercial Communications



Keysight Enterprise Customer Focus

HEALTHCARE



SOLUTIONS FOR HEALTHCARE

Need to have visibility into data for use cases including: Compliance with HIPAA, HITRUST and other regulations

FINANCIAL



SOLUTIONS FOR FINANCE

Finance and capital market participants have specific requirements in terms of pre-deployment testing and post-deployment visibility solutions

RETAIL



SOLUTIONS FOR RETAIL, SLED, ENTERPRISE

Avoid unexpected outages, overloads, breaches, and performance issues.

INDUSTRIAL/OT



SOLUTIONS FOR INDUSTRIAL IOT

Fortifying ICS/SCADA networks is no longer optional. Protect your OT network with Keysight solution for complete visibility into your IT and OT networks

GOVERNMENT



SOLUTIONS FOR GOVERNMENT

Government agency personnel need actionable data so that they can mitigate security threats



What is Zero Trust?

What is Zero Trust?



Zero Trust Defined

Founded on the basis of a “Trust No One, Verify All” mindset, Zero Trust is a set of guiding principles that validates all users trying to access business resources regardless of who they are and where they’re from. Zero Trust turns the traditional network perimeter model on its head and converts it to a more data centric model with security controls every step of the way.

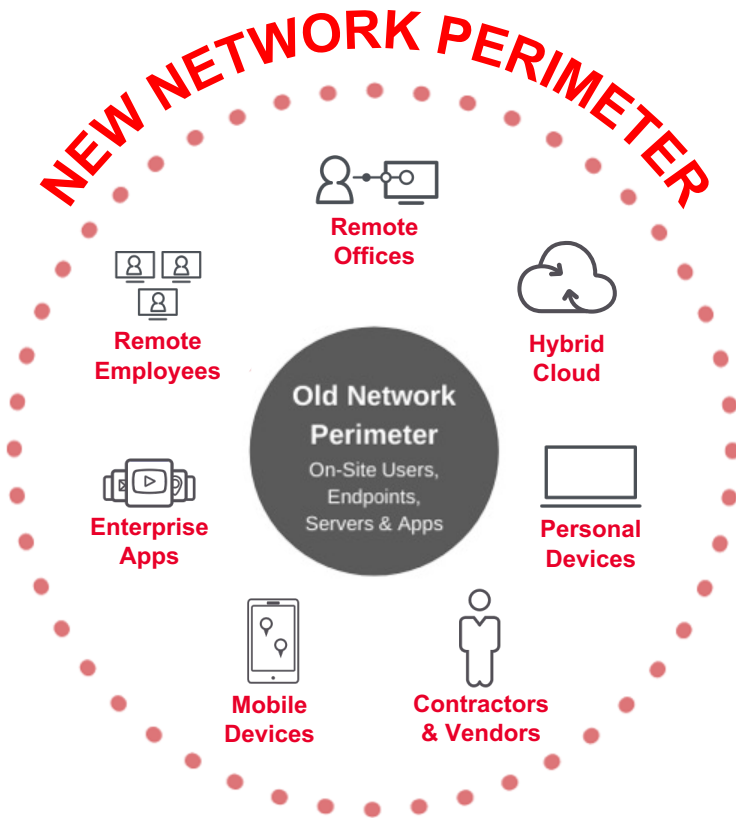


Zero Trust Justified

Various Zero Trust models are increasingly being adopted by enterprises and government security teams around the world. With perimeter security no longer effective by itself, new cloud models, the continued rise and sophistication of cyber attacks and current WFH initiatives, a Zero Trust architecture and corporate culture is needed now more than ever.

Security Challenges

NEW NETWORK LANDSCAPE = MORE THREATS



- ▶ Security teams aren't prepared for new adversaries and attacks.
- ▶ Legacy networks are hard to protect and ill-equipped for today's digital business.
- ▶ Security teams need better visibility and analytics to mitigate threats.
- ▶ Incident response capabilities continue to be weak.

Zero Trust is a Driving Force in Cybersecurity

TRUST NO ONE, VERIFY ALL

Zero trust is a strategic approach to security that centers on the concept of eliminating trust from an organization's network architecture. One can no longer assume that internal entities are trustworthy, that they can be directly managed to reduce security risk, or that checking them one time is enough. The zero-trust model of security prompts you to question your assumptions of trust at every access attempt. An effective model considers all resources to be external and continuously verifies trust before granting only the required access.

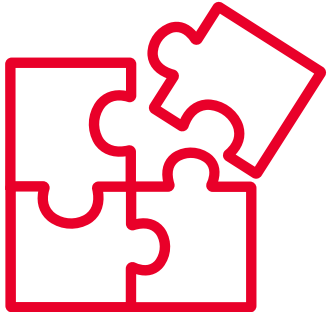
A zero-trust approach:

- ✓ Establishes trust in every access request, no matter where it comes from
- ✓ Secures access across your applications within new operational model
- ✓ Protects the business from advanced threats and impacts of breaches



Zero Trust is Not a Single Product

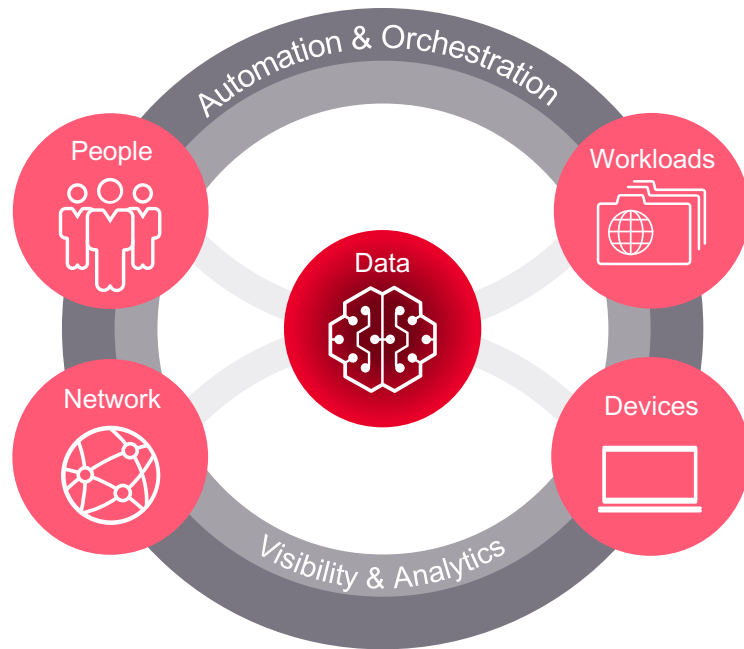
IT'S A COMBINATION OF SOLUTIONS FUELED BY A CULTURAL MINDSET



- ZERO TRUST IS A TEAM SPORT
- Zero Trust is built upon your existing ecosystem of solutions and products, and you must determine what other essentials are needed for your journey.
- Leverage and fine tune what you already have within a centralized framework
- Integration, heterogeneous support, and analytics are all critical capabilities to automate Zero Trust and make it easy to manage and deploy at scale.

Zero Trust Framework

COMPONENTS OF FORRESTER ZTX ARCHITECTURE



Network: The ability to segment, isolate and control the network

Data: Secure and manage the data, categorize and encrypt data both at rest and in transit

People: Secure the people using the network and business infrastructure

Workload: Secure cloud networks, apps, and other things used to make businesses operate

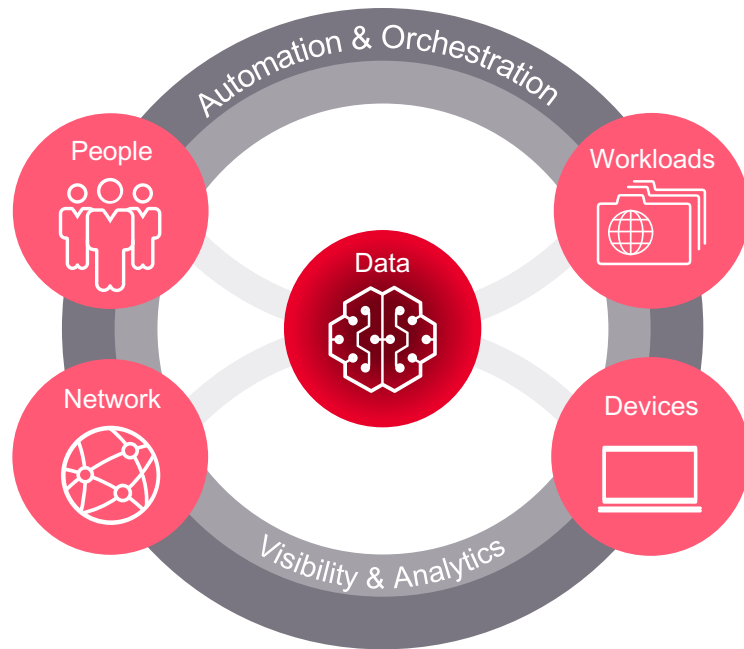
Devices: Isolate, secure, and control ALL devices accessing enterprise resources

Visibility and Analytics: Provides useful analytics and data points for correlation

Automation and Orchestration: Automate Zero Trust elements and provide more control of disparate systems

Zero Trust Framework

COMPONENTS OF FORRESTER ZTX ARCHITECTURE



Network: The ability to segment, isolate and control the network

Data: Secure and manage the data, categorize and encrypt data both at rest and in transit

People: Secure the people using the network and business infrastructure

Workload: Secure cloud networks, apps, and other things used to make businesses operate

Devices: Isolate, secure, and control ALL devices accessing enterprise resources

Visibility and Analytics: Provides useful analytics and data points for correlation

Automation and Orchestration: Automate Zero Trust elements and provide more control of disparate systems

Keysight Zero Trust Platform

FULL LIFECYCLE PROTECTION

As a leader in both network visibility and security testing, Keysight is uniquely qualified and positioned to provide a full lifecycle Zero Trust platform that has you covered from the second you go live. We allow you to design the best security architecture to meets your needs, while at the same time enabling you with the power to validate that design continuously ensuring that your security posture is constantly evolving. Security is not a singular event, it's a full lifecycle that continuously adapts to its environment giving you the best possible protection against advanced cyber threats.

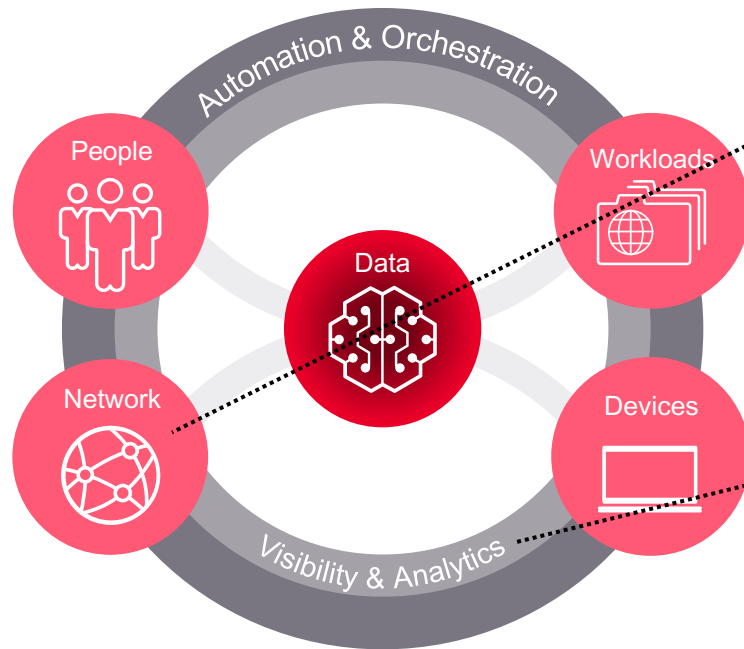




Part 1: Zero Trust Visibility

Zero Trust Framework

COMPONENTS OF FORRESTER ZTX ARCHITECTURE



Network

- Goal – Segment, isolate & secure the network
- Challenge – How to deploy security controls on internal (E-W) segments without impacting network availability
- Solution – Keysight Bypass Switches (+Technology Partner Solutions)
- Benefit – Deploy and maintain internal firewalls with impacting network uptime

Visibility and Analytics

- Goal – Illuminate and secure every nook and cranny of the extended enterprise environment
- Challenge – Network threat analytics detects attacks that logs miss. But accessing needed network data can be challenging.
- Solution – Keysight Visibility Fabric (+Tech Partner Solutions)
- Benefit – Complete and scalable hybrid cloud visibility for security tools, including decryption

Keysight Visibility Challenges

Scalability

- Internal E-W traffic is 80% of enterprises traffic
- 40/100G links can overwhelm tools
- Large number of links to monitor with limited tools budgets

Complexity

- SSL encryption is ZTA best practice, but creates blind spots
- VM-to-VM virtual traffic blind spots
- Multi-cloud deployments



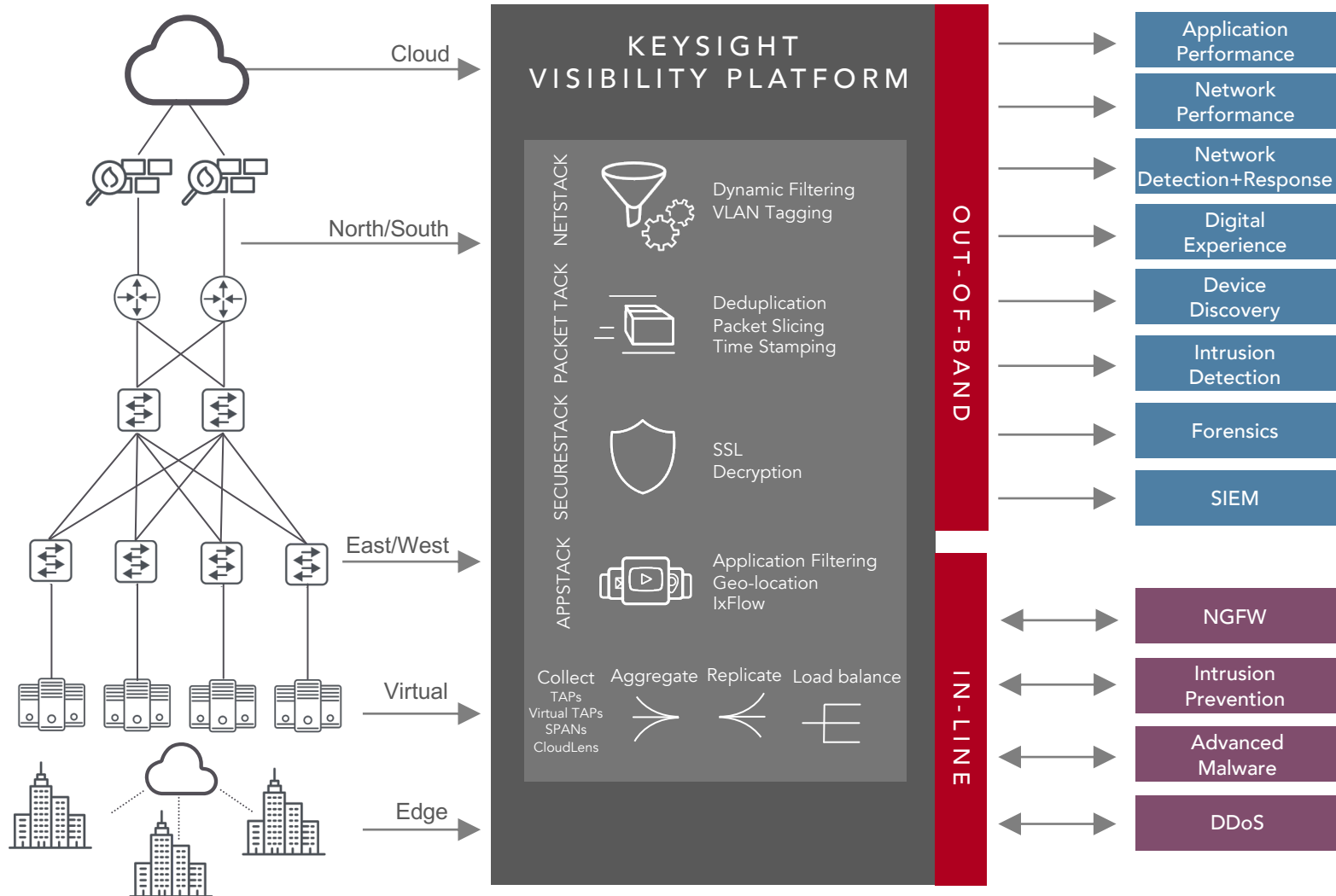
Network Visibility



Why is it still important?

- Even though perimeter security alone is insufficient, you still need to know what's going across it
- You need asset discovery to know what devices you have in your environment, managed or unmanaged
- You need internal security controls within your network segments
- You need to decrypt SSL traffic for full visibility
- You need to be able to correlate all these findings together for a holistic view
- Threat Intelligence sharing accelerates detection and resolution

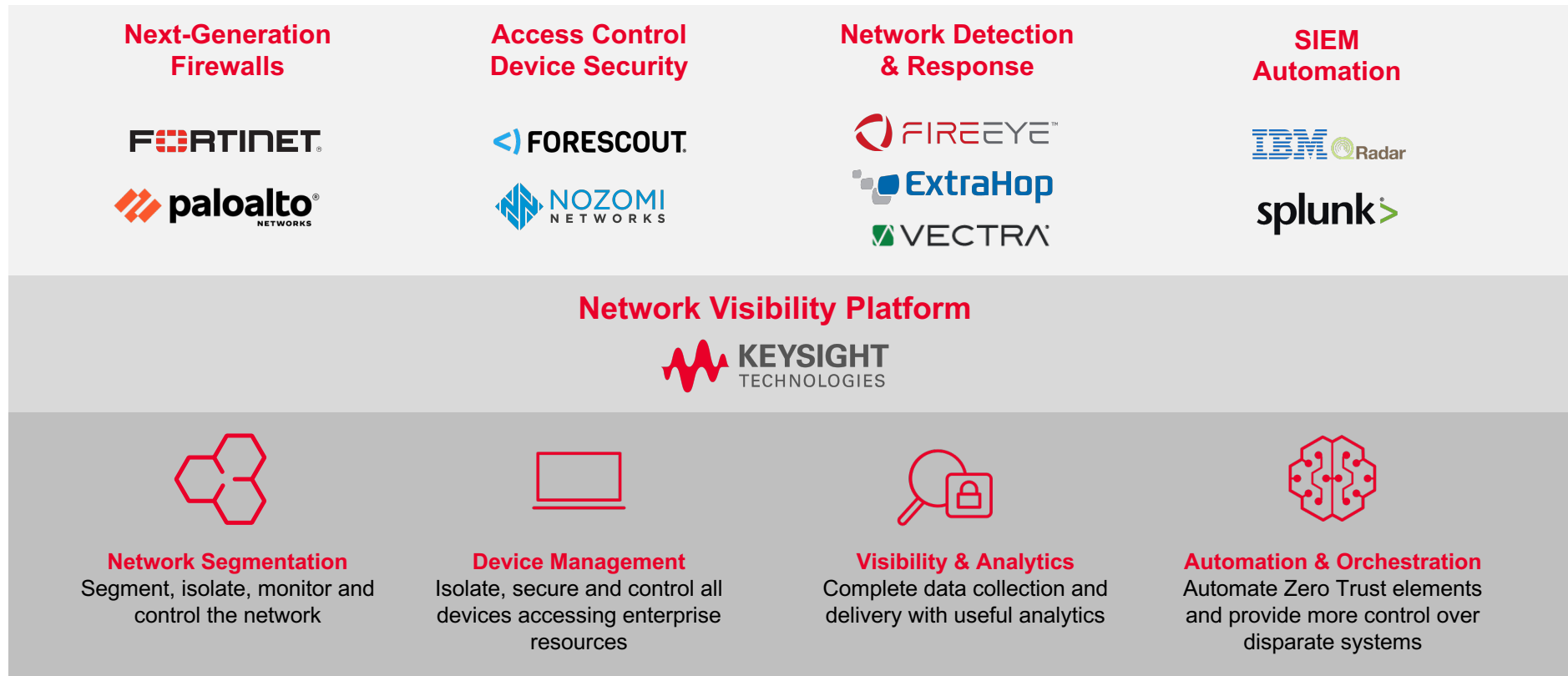
Keysight Visibility Platform



Keysight Partner Ecosystem

HIGH LEVEL BUILDING BLOCKS OF ZERO TRUST

The Keysight Zero Trust architecture is composed of numerous elements that are design to interoperate and work seamlessly with one another. When deployed and configured correctly as a unified system, all of the various security tools and processes bring a new meaning to the term, Better Together.



Keysight Zero Trust: Visibility & Analytics

OVERCOMING ACCESS TO NETWORK TRAFFIC



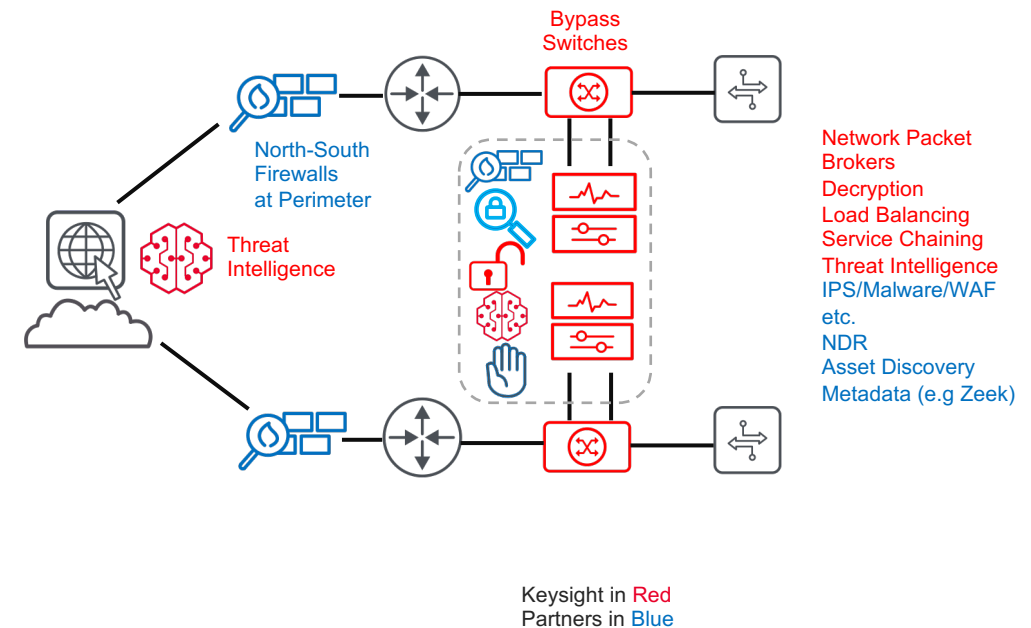
Visibility Fuels Analysis

You can't combat a threat you can't see or understand. Tools such as traditional security information event management (SIEM); more-advanced security analytics platforms like those from Splunk, IBM, etc; security user behavior analytics (SUBA); and network analysis and visibility (NAV) enable security pros to know and comprehend what's taking place in the network. This focus area of the extended Zero Trust ecosystem helps with the ability of a tool, platform, or system to empower the security analyst to accurately observe threats that are present and orient defenses more intelligently.

Keysight Zero Trust: Visibility & Analytics

SECURITY SERVICE CHAINING AT THE BORDER

- **Deployment Challenges**
 - General access to data by ALL security tools can be a challenge when access points are already taken
 - Network analytics tools often detect threats that logs miss
 - Resiliency is required at the network border
 - Performance for advanced functions (e.g. ssl decryption, personal information masking)
 - Sharing of traffic is required (most Enterprises maintain multiple security tools)
- **Solution**
 - Keysight Visibility Platform enables access to network traffic, to be shared for all tools (out-of-band and in-line)
 - Keysight Network Packet Broker provides advanced functions like load balancing, de-duplication and advanced data filtering



Keysight Zero Trust: Network Segmentation

PREVENTING LATERAL MOVEMENT ATTACKS



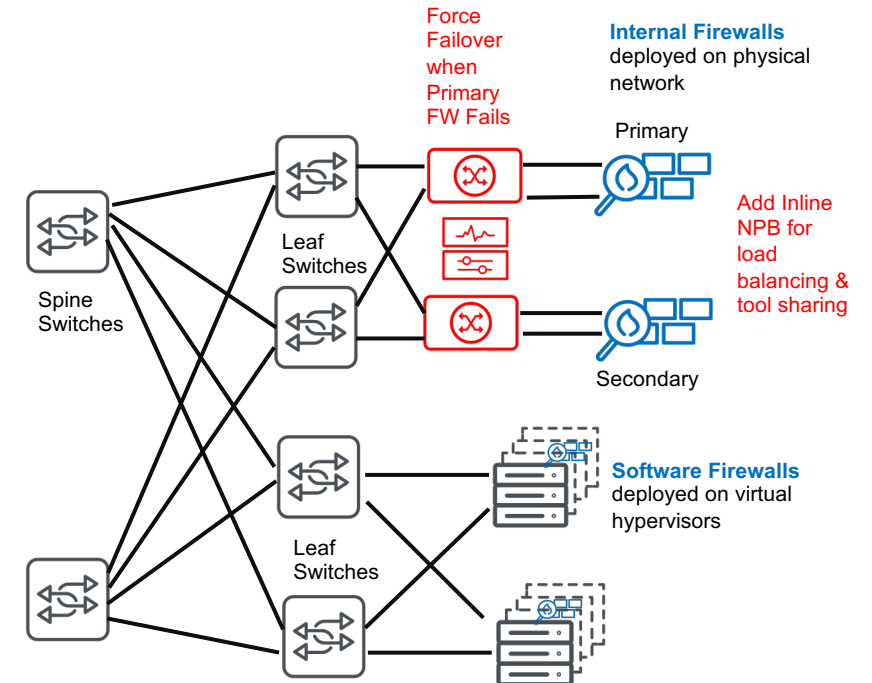
Segmentation is Key

Zero Trust is strategically focused on preventing lateral movement of attackers within a cyber kill chain. Architecturally, Zero Trust mandates that you segment across environments in order to isolate threats and limit the impact of breaches. The understanding you gained from mapping helps you decide where and what to segment – and is necessary for effective segmentation design.

Keysight Zero Trust: Network Segmentation

SECURITY CONTROLS FOR INTERNAL PROTECTION

- **Deployment Challenges**
 - NGFWs need to scale to internal network speeds (previously deployed at slower external gateways only)
 - Software solutions are on the rise, but hardware solutions provide the most scale.
 - Resiliency is more important than ever (for internal networks availability is primary consideration)
 - Performance for advanced functions (e.g. decryption, personal information masking)
 - Sharing of traffic is required (most Enterprises maintain multiple security tools)
- **Solution**
 - Keysight Bypass Switch with heartbeat health checking ensures availability
 - Keysight Network Packet Broker provides load balancing, traffic sharing, and advanced traffic processing



Keysight in Red
Partners in Blue

Visibility Benefits

DATA SECURITY STARTS WITH DATA VISIBILITY



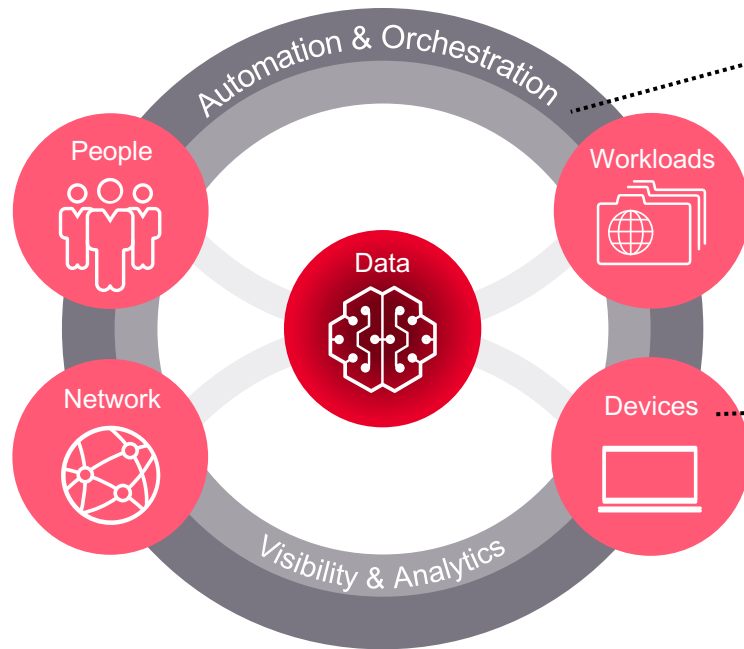
- Better security - tools work best with all the data they need. Missed packets are missed threats
- Eliminate virtual and multi-cloud blind spots
- Encryption – enable data to be encrypted, without blinding security tools
- Scale – help NetOps & SecOps teams keep up with exploding traffic volumes
- Cost savings – payback is usually under two years due to reduction in tools needed



Part 2: Zero Trust Validation

Zero Trust Framework

COMPONENTS OF FORRESTER ZTX ARCHITECTURE



Automation & Orchestration

- Goal – Automate Zero Trust controls & processes
- Challenge – Verifying security controls and policies on a consistent schedule as updates and patches are implemented
- Solution – Keysight Threat Simulator
- Benefit – Tests your network against the Zero Trust framework & provide recommendations

Devices

- Goal – Secure all network devices accessing enterprise resources
- Challenge – Not all devices have the correct access privileges and enterprise endpoint software required
- Solution – Keysight Threat Simulator
- Benefit – Validates effectiveness of security controls across endpoints and ensures EPS is up to date



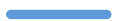


Zero Trust Validation

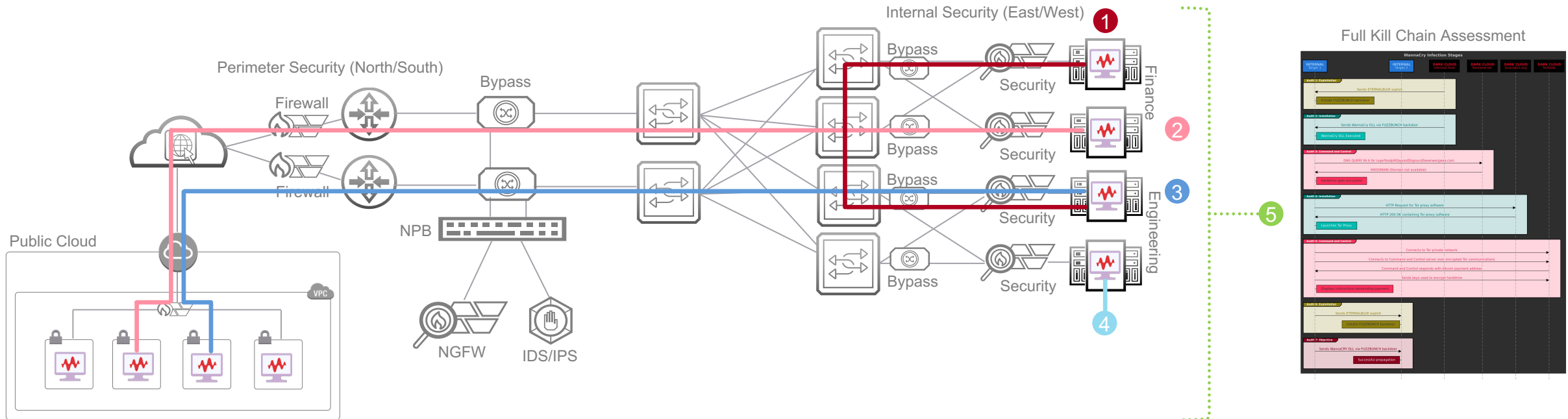
TYPES OF TESTS THREAT SIMULATOR CAN PERFORM

Zero Trust Component	What Does Threat Simulator Do?
Networks	Segmentation: Zero trust supports the use of micro-segmentation in the network. Threat Sim tries to scan and find machines that it can communicate with from the machine it's running on, that belong to different network segments. If Threat Sim successfully performed cross-segment communication, we recommend checking firewall rules and logs. This is relevant to the Visibility component as well.
	Tunneling: One Threat Sim agent tries to tunnel traffic using other agents. If it succeeds, that means that the network policies are too permissive. We recommend restricting them in such a way that unknown tunneling traffic will not be allowed.
Devices	Exploitable Machines: Threat Sim tries to exploit machines to breach them and propagate in the network. If Threat Sim has successfully exploited endpoints, we recommend checking IDS/IPS logs to see activity recognized and see which endpoints were compromised and remedy the reasons the endpoints are vulnerable.
	Endpoint Security: Threat Sim checks if there is an active endpoint security software in place. If Threat Sim doesn't find ANY active endpoint security processes, we recommend installing and activating an anti-virus software on endpoints. If Threat Sim found active endpoint security processes, we recommend checking their logs to see if they recognized Threat Sim as a security concern.
Visibility & Analytics	Malicious Activity Timeline: Zero Trust attempts to empower the analyst. Threat Sim performs all sorts of malicious-looking actions, like scanning and attempting exploitation. If you have good Visibility of your network, you should be able to see all the events in your SOC logs and alerts.

Zero Trust Validation

THREAT SIMULATOR IN ACTION

Networks		1. Segmentation: Cross segment malicious communication using malicious traffic
		2. Tunneling: Unauthorized tunneling between segments
Devices		3. Exploitable Machines: Breach attempts on endpoints using simulated attacks
		4. Endpoint Security: Validates if anti-virus software is present and active
Visibility & Analytics		5. Malicious Activity Timeline: Generates attack timeline, enables validation of log accuracy thru SIEM



Keysight Threat Simulator

AUTOMATED, SAFE, AND CONTINUOUS ASSESSMENT

Attack Yourself Quickly, Safely, & Securely

- Deploy and run in a matter of minutes.
- Simulate the kill chain with real-world malware & techniques
- Agents hosted in Dark Cloud ensure safety

Remediate and Optimize Rapidly

- Best-in-class step-by-step recommendations close gaps
- Maximize existing products without extra cost

Analyze Detection and Blocking Capabilities

- Be confident in detection and blocking rules, even after changes

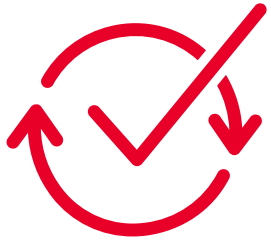
Get In Front of New Attacks with Continuous Audits

- Minimize risk from config. changes, new threats, etc.



Validation Benefits

TESTING IS NOT A SINGULAR EVENT



- Measure the cybersecurity effectiveness of live networks... all the time
- Improve the security you have before investing in more
- Remediate easily with fast results
- Quickly identify misconfigurations and policy gaps
- Analyze detection & blocking capabilities

Why Keysight Zero Trust

IF ZERO TRUST IS YOUR STRATEGY, THEN KEYSIGHT IS YOUR PLATFORM



Complete Lifecycle Protection

Keysight Zero Trust offers an effective solution set that is designed to secure all access to the network and applications, from any user and device from any location, while continuously testing the efficacy of the architecture and its policies. Our complimentary suite of products are designed to seamlessly interoperate with your entire infrastructure while maintaining your investments in other solutions.



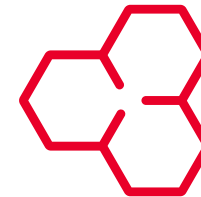
Zero Trust for Visibility

Secures access across your applications within new operational model



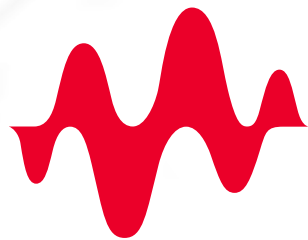
Zero Trust for Devices

Establishes trust in every access request, no matter where it comes from



Zero Trust for Networks

Protects your business from advanced threats and impacts of breaches



KEYSIGHT
TECHNOLOGIES

4.50221

Zero Trust Campaign

- Campaign-in-a-box
 - Messaging
 - Customer Slides
 - Whitepaper
 - Keysight Zero Trust Architecture using Visibility and Test
 - Solution briefs from Tech Partners (Palo Alto, Fortinet, Forescout)
 - Webinars in Q3 (Fortinet, FireEye)
 - Channel Training
 - New Website
 - Video
 - Blog
 - Email Template (Customizable)

Zero Trust
CAMPAIGN-IN-A-BOX
Go-To-Market with Solutions for Enterprise IT

Building a Foundation for Zero Trust

Table of Contents

Introduction.....	2
Campaign Messaging.....	2
Customer Presentation.....	4
Zero Trust Whitepaper.....	5
Technology Partner Solution Briefs.....	6
Product Catalogs.....	7
Other Resources.....	7

KEYSIGHT TECHNOLOGIES

Find us at www.keysight.com Page 1

Industry's leading security preference designs that Though your customers are all scalable and can

ed in one of the ou in touch with ilable.

Expandable Next Generation Firewall Security

Perimeter and Internal Security Protection

Forescout Securing IoT Devices The Moment They Connect

Find us at www.keysight.com Page 6

KEYSIGHT TECHNOLOGIES MAY 2021

Building a Foundation for Zero Trust

Zero Trust: What is it and why is it important?

Founded on the basis of a "Trust No One, Verify All" mindset, Zero Trust is a set of guiding principles that validates all users trying to access business resources regardless of who they are and where they are from. Zero Trust turns the traditional network perimeter model on its head and converts it to a data centric model with security controls at every step.

As networks continue to evolve and we continue to see an acceleration of digitization and a remote workforce, the Zero Trust model of security is increasingly being adopted by enterprise and government security teams worldwide.

Keysight Zero Trust Platform

As a leader in both network visibility and security testing, Keysight is uniquely positioned to provide a full lifecycle security platform that has you covered from the second you go live. We empower you to design the best security architecture for your environment, while at the same time enabling you with the insight to validate the effectiveness of that design so you can fine tune and adjust for better protection. Security is not a singular event. Our common cyber adversaries constantly evolve their attack methods. Your security posture should constantly evolve as well.

Scalable Network Monitoring • High Resiliency • Decryption & Multi-cloud

Attack Simulation • Continuous Monitoring • Policy Effectiveness

ZERO TRUST SECURITY

