WHITE PAPER

Chaos to Control: Validating Distributed, Disaggregated Digital Transformation

"If you can't measure it, you can't improve it." This quote could not find better applicability than in today's hyperconverged hybrid networks, evolving applications, and service infrastructures. Digital transformation is the essence of these rapidly evolving ecosystems and key to competitiveness for most enterprises today. Success and agility in such environments depend on the ability to measure and analyze how distributed, disaggregated network infrastructures, applications, and services perform before going live, as well as during their production life cycle.

Enterprises scarcely perform testing and validation, and usually do so before or immediately after the introduction of a network architecture, device, or service. Almost no testing occurs after the fact. This incomplete testing leaves doubts, uncertainty, and blind spots when it comes to performance and scale limits and potentially broken functionality, misconfigurations, and security gaps.

Nobody wants to face these issues deep in production phases and pay the price to fix them. Past research shows that early discovery of issues provides massive savings, with some finding that bugs discovered in development are 90 to 100 times less expensive to fix than when found in maintenance.

One of the fiercest enemies of today's networks and services is complexity. With evolution, complexity (exposed or hidden) builds at every step taken toward that new, next-generation, or cutting-edge piece of technology planned for adoption or development. Moreover, new methodologies such as continuous integration / continuous delivery (CI / CD) pipelines, development operations (DevOps), and

"If you can't measure it, you can't improve it."

A successful digital transformation journey should have *continuous improvement* as one of its core components.

Quantifiable and actionable data points are the cornerstone for achieving success throughout your network life cycle, from design to production.

80% of unplanned downtime is caused by human error

KEYSIGHT TECHNOLOGIES

development security operations (DevSecOps) are pushing the time to market to unprecedented levels. That speed puts increased pressure on test and validation aspirations. Research by Information Technology Intelligence Consulting (ITIC)[1] shows that human error causes 80% of unplanned downtime. Early testing could have found many of those problems.

In this white paper, you will discover essential strategies for ensuring high-performing networks, applications, and services through robust testing across the ecosystem life cycle.

The Only Constant Is Change

Change is all around us. It doesn't stop once the integration and transition phase of a new technology is complete. Today's reality is that the only constant is change.

Increasing traffic volumes pressure network infrastructures, the cyberthreat landscape is continuously evolving, and software patches and updates occur frequently. In the meantime, innovation demands make DevOps and DevSecOps models the new norm.

Within this realm, establishing a test and validation strategy that covers the network development life cycle is paramount. Although this seems to be a challenging endeavor, the alternative is more challenging to manage. Figure 1 summarizes the three main phases you need to consider when thinking about a test and validation strategy.

Establishing a test and validation strategy that covers the network development life cycle is paramount.

Figure 1. Enterprise network life cycle

In each of these three main phases, comprehensive testing can bring unique benefits and solve different problems, ultimately ensuring high-performing networks, devices, and services for a competitive edge in the digital transformation process. Table 1 shows an outline of these.

1. https://www.ibm.com/downloads/cas/YGLRKEEK

Table 1. Testing benefits

Network life cycle phases	Testing benefits
Proof of concepts, vendor bake-offs	• Make informed decisions on vendor and technology selection according to your requirements. • Rightsize your network, tools, and investments. • Derive an accurate total cost of ownership through real performance and capabilities testing.
Planning and design validation	• Tune and optimize your future networks and find the right balance of performance and security. • Introduce services with confidence. • Benchmark baseline performance and security efficacy to develop robust change management.
Production continuous validation	• Apply change management best practices. • Run continuous safe security assessments. • Perform service-level agreement (SLA) assessments. • Identify performance or functionalities deviations.

New Technologies Bring New Challenges

Cloud migration, SD-WAN, data center upgrades, advanced cybersecurity capabilities, Internet of Things (IoT), and application proliferation are examples of significant shifts in technology. Organizations are widely embracing these shifts as they evolve through digital transformation — which also brings significant technical challenges.

Companies spend a substantial amount of time, effort, and money to adopt and transition to new technologies. Testing and validation through different means and models is a principal component in this process and instrumental in making the transition with confidence and deriving quantifiable benefits.

> **Companies spend a substantial amount of time, effort, and money to adopt and transition to new technologies, oftentimes without the confidence provided by quantifiable benefits.**

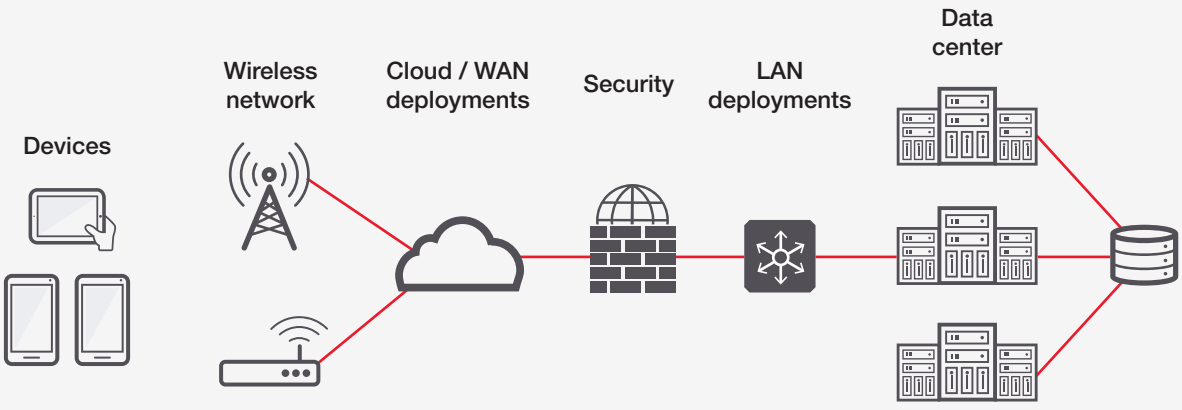


Figure 2. Distributed, disaggregated digital transformation leaves no network element untouched

Table 2 is a summary of the most important aspects to test when adopting modern technologies. While this list is not exhaustive, it does emphasize the primary concerns and challenges for the respective segment. This list comes from engagements with key leaders in each industry, including network equipment manufacturers, service providers, and enterprises.

Table 2. Summary of aspects to test for new technologies

Technology	Key challenges	Test insights
Cloud migration	• cloud spend • user experience • security	• rightsize cloud for performance and cost • configure elastic scaling policies • validate cloud security controls
SD-WAN	• benchmarks and policy calibration • routing capabilities • security and cloud access controls	• distributed workload and security characteristics • routing establishment and failure recovery • live assessments of SLA and user experience
Data center	• DC expansion — 100G, white-box switches • consolidation of SAN and LAN • micro-segmentation to handle increasing east-west traffic	• E2E fabric validation with real application and storage workload • failover and recovery • security posture validation
Cybersecurity	• new technologies (ML/AI, TLS 1.3) • complexity • moving targets (threats and solution updates)	• technology validation • optimizing overlapping security controls • proactive, continuous security validation
New applications and IoT proliferation	• new devices and applications • decentralization • increasing traffic volumes	• DPI capabilities to identify, authorize, and police • distributed assessments to understand the impact of device scale • performance and security

Solving Technology Challenges with Test Solutions

The sections above briefly present the high-level benefits of using testing and validation for different technologies and stages of the development life cycle. Let's take a closer look at the actionable insights testing brings on the unknowns of these new technologies.

> **Two of the top three cloud challenges relate to managing cloud spending and security.**

Solving cloud migration unknowns: Optimize cost, security, and QoE

While 84% of enterprises have a multi-cloud migration strategy, a survey conducted by Flexera[2] found that two of the top three cloud challenges relate to *managing cloud spending* and *security*.

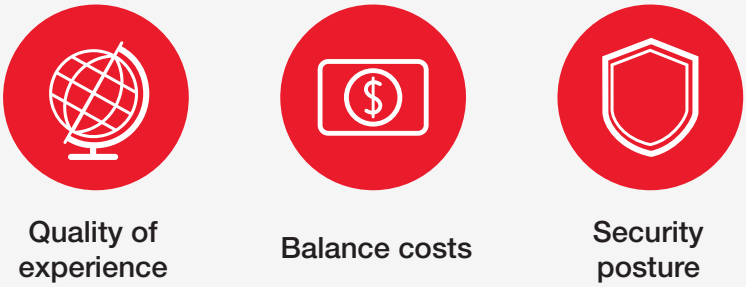


Figure 3. Cloud migration considerations

Cloud infrastructure and network elements include next-generation firewalls (NGFW), web application firewalls (WAF), application load balancers (ALB) / elastic load balancers (ELB), and web servers. One important unknown is how to properly size those elements to keep costs under control while ensuring optimal performance and user quality of experience (QoE). You need a test tool emulating your workloads and measuring the capabilities and performance of the provisioned cloud infrastructure to get the right metrics and data to make optimal cloud expenditures decisions.

> **A test tool emulating your workloads and measuring the capabilities and performance of the provisioned cloud infrastructure is required to get the right metrics and data to make optimal cloud expenditure decisions.**

The cloud is supposed to give organizations almost unlimited scalability. However, linear scalability in cloud environments works only to a certain point before you hit underlying resource contention issues. Cloud architects need to understand the balance between scaling up and scaling out for a given workload, as this will enable them to configure their auto-scale policies correctly.

Also, performance issues may originate from complex interactions between subsystems that may include ELB, WAF, domain name system (DNS) service, and authentication. Therefore, you need a holistic approach to performance testing with realistic workloads that exercise all the subcomponents on the application delivery path.

2. https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey/

Cloud security brings even more uncertainties and unknowns. To realize cloud savings without compromising on security, you must exercise the unknowns that come with the elastic scalability, multitenancy, and high-availability characteristics of a cloud infrastructure. Considering today's cloud diversity, you need to test from multiple angles, for hybrid deployments, in a highly distributed fashion and have flexible automation for easy integration with CI / CD pipelines.

Solving SD-WAN unknowns: Network, service QoS, and security

Software-defined wide area network (SD-WAN) technology holds many promises. The fact that its apparent cost is just a fraction of traditional WAN deployments makes it one of the most widely adopted applications of software-defined networking (SDN) in enterprise networks. Modern SD-WAN solutions deliver more than just seamless WAN connectivity. They are evolving to deliver connectivity to multiple cloud providers, enforcing security policies across on-premises and cloud deployments, and orchestrating connectivity that spans multiple domains.

While transitioning to SD-WAN seems like an obvious strategy, if not done right, SD-WAN can bring more problems than benefits. To ensure the success of an SD-WAN implementation and provide the five nines of reliability required for business-critical applications, testing must be a key component in both pre- and post-deployment.

To ensure the success of an SD-WAN implementation and provide the five nines of reliability required for business-critical applications, testing must be a key component in both pre- and post-deployment.

In pre-deployment, you need test solutions that can emulate a fully scaled network, generate realistic workloads that represent enterprise applications, measure traffic characteristics, and ensure that security policies span the distributed network. Before rolling out a solution, you'll need to run performance benchmarks, SD-WAN policy calibration, and measurements of the QoE. Another aspect is emulating Layer 2/3 protocols and generating traffic at high scale to validate the routing capability of SD-WAN networks.

SLAs for network availability, latency, packet loss, and jitter are critical in a hybrid network, as the performance guarantees are not the same as in an MPLS-based WAN. Hence, it is important to be able to emulate user traffic in the different delivery points of SD-WAN architecture to validate end-to-end performance across these metrics. In addition to ensure user experience and performance across SD-WAN deployments, security policies for branch offices and the cloud need to be continuously assessed so organizations have a constant pulse on their security posture.

Solving new data center switching unknowns: Greater demands and challenges

Data center technologies are continuously evolving to address the perpetual demand for more speed, higher availability, increased capacity, and convergence.

The modern data center is a mixed offering of white-box, brite-box, and incumbent devices. Effectively managing these hardware resources in hybrid cloud environments is critical to success. Network operating systems (NOS) include both open source and commercial varieties. The disaggregated NOS provides a more open, cost-effective, and flexible alternative to traditional networking equipment. It speeds the adoption and use of white boxes in cloud data center infrastructure.

Spine-leaf fabrics are the fundamental underlay infrastructure connecting all physical and virtual resources. Today's data center needs to support massive north-south and east-west traffic, so fabric throughput needs to be benchmarked under many conditions with representative workloads. The data center also needs to provide redundancy with fast failover and always-on connectivity for all services running over it. Public cloud providers have adopted a simplified IP Clos architecture for the fabric. Is the NOS optimized for the underlying hardware mix, including white-box or specialized hardware? Does it meet the performance expectations for massive data throughput and latency? Can the fabric ensure that no traffic drops during failover? Does the failover convergence meet expectations? All of these are critical to the fabric performance.

> **VXLAN and EVPN are critical overlay network technologies. Organizations need to validate maximum VXLAN tunnels, EVPN VXLAN scale and performance, virtual machine mobility, multihoming, and traffic load balancing.**

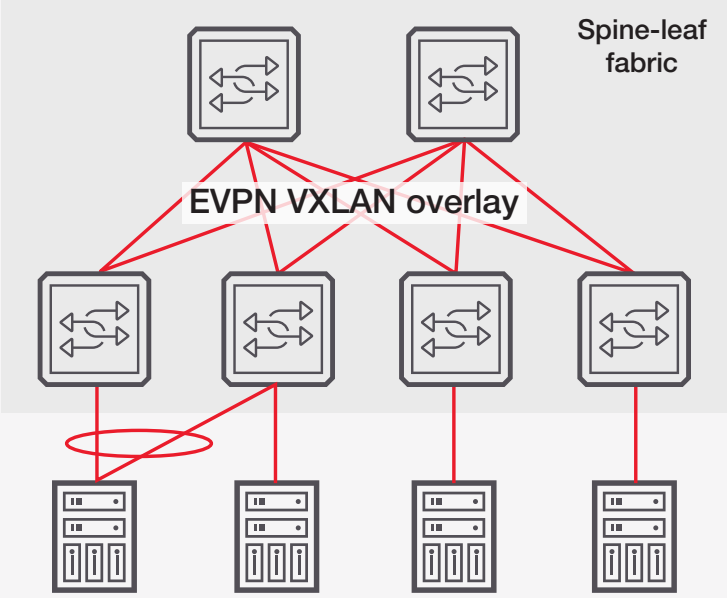


Figure 4. Spine and leaf fabrics underlay infrastructure to connect all physical and virtual resources

In addition to a robust underlay network, you need an overlay network to provide network segmentation with multitenancy support for a large number of users. Resource placement should be flexible to support fast service provisioning and sustain peak workloads. These require intelligence for effective orchestration. Virtual extensible LAN (VXLAN) and Ethernet virtual private network (EVPN) are critical overlay network technologies. Organizations need to validate maximum VXLAN tunnels, EVPN VXLAN scale and performance, virtual machine mobility, multihoming, and traffic load balancing.

Storage traffic takes a huge proportion of any data center traffic load. Many data centers are moving away from dedicated storage networks and adopting Ethernet for their storage infrastructure. Lossless Ethernet is the key for a converged compute and storage network. Non-volatile memory express (NVMe) over remote direct memory access (RDMA) over converged Ethernet version 2 (RoCEv2) with priority flow control (PFC) and explicit congestion notification (ECN) is an important technique to ensure lossless Ethernet. The switch fabric needs to be stress-tested with storage workloads to measure throughput, latency, and input / output performance.

Enterprises are using micro-segmentation to switch from a monolithic structure. Micro-segmentation segregates the data center by smaller and similar workloads and creates individual security plans and measures for each. This technique is an efficient way to protect data from threats such as lateral movements or other exploits or malware that are relevant in east-west traffic.

Quantifiable data is critical to guiding the selection of technology that best matches your needs and rightsizing that investment — before launching a data center (or segment) into production or bringing a network device into the picture. You can achieve this by running a battery of tests:

- Use real-life, high-volume, application, and storage workloads to make sure individual network devices, as well as the end-to-end network infrastructure, can handle the required volumes with high quality.
- Validate data center perimeter security under your specific configuration by simulating legitimate traffic combined with a broad set of attacks like malware, exploits, distributed denial-of-service, brute-force, and web application attacks.

Solving cybersecurity unknowns: Maximize security investment and manage complexity

Enterprise cybersecurity leaders have a lot of challenges on their hands: higher compliance burdens, evolving threats, lack of skilled resources and talent retention, adopting and transitioning to new technologies. One of the key issues is that too many cybersecurity point solutions don't always work well together. Additionally, even with all the investment, security personnel lack hard data on their network security posture. In reality, these expensive and complex security solutions do not always guarantee a more secure network, especially when users have a limited understanding of their real capabilities, performance, and efficacy.

To maximize security investments and manage complexity, consider the following key points:

- Understand the actual cost per protected megabyte of candidate security solutions before making purchasing decisions.
- Make sure that new security solutions do not excessively overlap with your existing security architecture and that their production integration is successful.
- Regularly check against the baseline (especially for change management) to identify any potential deviation before wasting resources on wrong assumptions.

The required testing strategy to cover at least the above points perfectly fits the three main phases of continuous testing throughout the network life cycles. When it comes to security, the strategy should encompass the following:

- Perform vendor selection *after* head-to-head performance, functionality, and security efficacy comparison tests. To get a relevant security efficacy score on each device, conduct such tests using traffic that represents your particular enterprise along with security attacks for the respective environment. For example, a financial application mix might have different results for different vendor devices than an enterprise application mix.
- Validate your solution / technology pre-deployment to ensure proper characterization before production prime time. But you also need end-to-end tests to pinpoint overlapping security controls and to confirm successful solution and technology integration.
- Baseline your network performance and use automation for confident change or update rollouts. Also, use continuous security posture assessment using realistic attack and breach simulations to get actionable security insights and know whether your security is working.

Even with all the investment, security personnel lack hard data on their network security posture. In reality, expensive and complex security solutions do not always guarantee a more secure network, especially when users have a limited understanding of their real capabilities, performance, and efficacy.

Solving IoT and new application unknowns: Identification, performance, and scale

IoT has fundamentally changed the way we live, work, and play. Billions of IoT devices already exist, with hundreds more, ranging from consumer products to devices and sensors used for mission-critical applications, coming online each second. As a direct effect, existing and new application dynamics increase significantly, resulting in greater stress on the performance, capacity, and security of existing networks. Below are the most important scenarios enterprises need to consider when adopting IoT as part of their digital transformation to limit risk on their networks and increase their operational efficiency and bottom line.

The first consideration is on the connectivity side. Most IoT devices use Wi-Fi for connectivity. However, most Wi-Fi networks are at best qualified only for coverage, with basic element and interoperability testing. This woefully inadequate test strategy exposes companies to the risk of their business applications failing in the field. What you need is a comprehensive test tool that can emulate real-world IoT traffic to validate the entire Wi-Fi ecosystem. It should deliver powerful independent Wi-Fi benchmarking, as well as functional, soak, and stability testing for wireless local area networks (WLANs).

> **Most IoT devices use Wi-Fi for connectivity. However, most Wi-Fi networks are at best qualified only for coverage, with basic element and interoperability testing. This exposes companies to the risk of their business applications failing in the field.**

Subsequently, at the application and security layer, companies must use a test solution that is powerful enough to measure and harden the application performance of networks and security devices while confronted with IoT-specific workflows. A best practices checklist of items to cover should include the following:

- Emulate IoT endpoints at scale, running specific protocols and applications to evaluate the capacity and performance of the network infrastructure and how this potentially impacts the QoE of business-critical applications.
- Evaluate the capabilities of existing security devices to identify IoT traffic and apply corresponding security profiles.
- Simulate IoT-specific attacks, including botnet traffic, brute-force attacks, exploits, and malware, along with legitimate traffic to understand the efficacy of existing or potential security solutions.

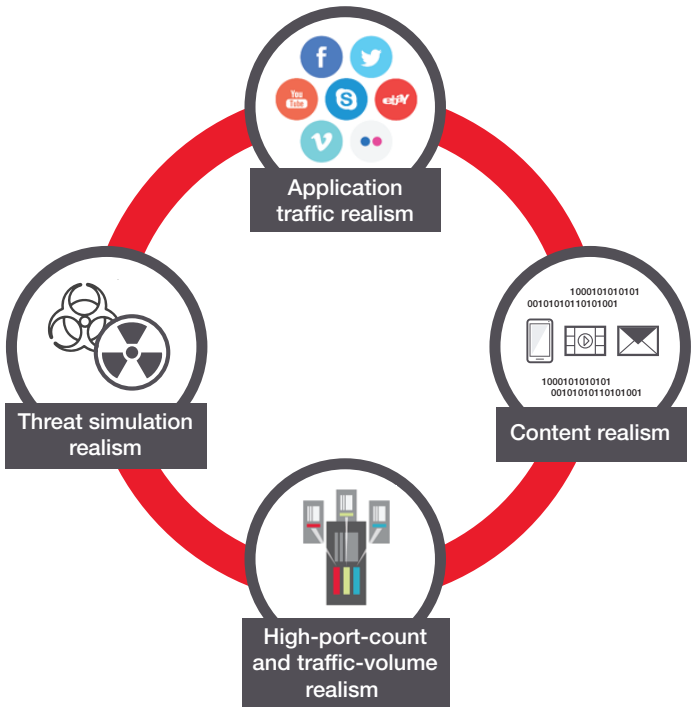
Testing with Keysight: Realism in the Lab and Live

We have established that, as organizations move through their digital transformation, there are a lot of unknowns. Testing and verifying each step of the network life cycle gives organizations tremendous confidence in their choices and decisions. It also reduces operational and downtime costs by uncovering bugs and issues early in development — rather than identifying the issues in production.

The following characteristics are paramount to ensuring meaningful results that deliver the right insights. Keep them in mind as you plan and define the validation criteria for your application and content-aware intelligent devices, networks, and solutions:

- Application traffic realism – The workloads and traffic mixes that you choose to simulate as you benchmark networks and security appliances need to represent what you expect to see in your production networks. Getting this mix right will result in benchmarking that represents your particular network, rather than relying on data sheets, which vendors construct under assumed, ideal conditions.
- Content realism – Ensure that the payloads in your workload simulation contain realistic, dynamic content, as this will relevantly exercise the deep packet inspection (DPI), content rules, and data leakage prevention capabilities of your security solutions. Also, fake static content compared to real dynamic content has a profound impact on the CPU and memory performance of security devices. Fake content can also unfairly show a device in a poor light because a string of zeros in a payload might cause an intrusion prevention system engine to think there is something suspicious, increasing application latency and decreasing overall performance.
- Threat simulation realism – It is difficult to effectively measure your security posture as security threats arrive with unprecedented diversity, volume, and velocity. Therefore, to truly validate security effectiveness and efficacy, you need threat simulation that can emulate a diversified and realistic library of techniques, threats vectors, and kill chain modeling combined with legitimate user and application behavior.

Testing and verifying each step of the network life cycle gives organizations tremendous confidence in their choices and decisions. It also reduces operational and downtime costs by uncovering bugs and issues early in development—rather than identifying the issues in production.



- High-port-count and traffic-volume realism – With mass deployment in modern data centers, 100GE technologies have come to maturity, and market trends indicate steady growth for the next few years. To address the need for higher scale at a manageable cost, merchant silicon is significantly driving down the cost per bit of switched data in the network. You'll need affordable options to get one-to-one port-count testing for white boxes and massive-volume testing to realistically emulate the data center.

Keysight Technologies is the only solution on the market that can deliver this realism, in conjunction with high-performance simulation. By creating and applying the realism of your unique networks and traffic workloads, Keysight enables your IT organization to quickly evaluate how specific technologies, architectures, and transformation plans will deliver performance, user experience, and security, optimizing operational and downtime costs.

The right products to solve the challenges of today and tomorrow

Using the right tools to solve new challenges is critical to success. Keysight helps the world's leading companies move from chaos to control as they undergo their distributed, disaggregated digital transformation. We help solve the challenges described in this paper by offering a robust portfolio of proven test solutions.

Table 3. Keysight test solutions

Test challenge	Test solution
Continuous validation of enterprise-wide security posture lets enterprise SecOps teams identify opportunities to remediate security gaps and monitor for environment drifts in production networks.	Threat Simulator
Distributed agent-based application performance and security simulation lets enterprises validate elastic, distributed, hybrid pre- and post-production networks and devices.	CyPerf
Large-scale application performance and security simulation lets enterprises validate on-premises, preproduction networks and devices.	BreakingPoint
Large-scale application performance simulation lets enterprises validate QoE for on-premises pre-deployment networks and devices.	IxLoad
Large-scale network infrastructure protocol and traffic simulation lets enterprises validate routing and switching, data center migrations, and software-defined networking.	IxNetwork

The market leader and your trusted test partner

Keysight is the world's leading electronic measurement company, transforming today's measurement experience through innovative, unique solutions. Keysight, together with its Ixia product line, provides end-to-end solutions to design, test, and secure networks, devices, and services. Keysight solutions span the stack (Layers 1–7), from edge devices to network performance and security, and the product life cycle, from design creation to manufacturing and beyond. Enterprises and organizations gain faster time to market, optimized application performance, and higher-quality deployments, ensuring that their networks are resilient.

Keysight provides the tools that can realistically exercise all these vectors. It also offers the possibility to connect with a trusted partner to design, build, and operate the networks and services that facilitate a competitive edge.

Keysight, together with its Ixia product line, provides end-to-end solutions to design, test, and secure networks, devices, and services. Testing that replicates your network in action.

Conclusions

Performance, functionality, QoE, and security efficacy are all key components that you need to validate regardless of the embraced technology, selected network design, or even development phase. In the chaos of your distributed, disaggregated digital transformation, getting all these components right is a real balancing act that you can master only through a systematic and robust test strategy and with a trusted partner.

Your ability to validate with real-world traffic across the stack — spanning networking protocols, services, applications, and cybersecurity — offers a competitive advantage. That is true whether you are conducting proof of concepts, planning and design validation, or continuously testing into production.

Keysight's network, applications, and security test products ensure that your test results are meaningful and deliver the right insights. We do this by offering the industry's highest-performance testing with the most realistic application workloads and traffic mixes, dynamic payloads, threat simulation, evasions, and legitimate traffic. It is testing that replicates your network in action.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES