SOLUTION BRIEF

Testing Performance and Security in Distributed Networks With CyPerf

Networks continue to change rapidly as traditional premise-based networks evolve to distributed cloud and hybrid environments. These complex networks use edge computing and centralized resources that bring applications closer to users and the source of data. Legacy networks with clearly defined perimeters are somewhat easy to defend. However, modern networks have no defined perimeter to secure and often employ zero trust security policies that use identity, not perimeter-based access. This transformation brings many major unknowns to the performance, scalability, and threat protection of network and security architectures.

Testing today's complex and dynamic networks the same way as legacy networks is no longer feasible — a new paradigm is necessary.

CyPerf sets a new standard as the world's first instantly scalable test solution for zero trust in distributed cloud networks.

What is Zero Trust?

Zero trust is not a single product, technology, platform, or feature but rather an overarching cybersecurity strategy or a framework of policies, best practices, and guidelines. A zero-trust framework is critical for securing and managing the growing complexity and digital transformation of modern networks. Zero trust is based on a model that never trusts and always verifies.

Traditional network security assumes that once users are inside a network say via protected VPN there is an implied trust. This implicit trust allows for lateral movement once inside the network, not only by legitimate users but also by hackers and other malicious traffic that have the intent to cause harm.

Zero trust secures an organization by eliminating the outdated idea of implicit trust. With zero trust, there is no lateral movement within networks because without exception, every network and application request undergo continuous validation and authentication.

Even though zero trust and a secure sockets layer (SSL) VPN are on opposite sides of the security spectrum, they are not exclusive. Organizations can still use SSL VPN. It is more of a transport technology with the added benefits of providing confidentiality, integrity, and authentication. Zero trust brings multiple benefits to an organization's security posture, closing some of the existing gaps inherent in other models while drastically reducing the attack surface.

The Test Challenges of Modern Networks

Network equipment manufacturers (NEMs) who provide enterprises, government entities, and service providers with their underlying network infrastructure face new challenges as they pivot from delivering primarily premise-based hardware or "big iron" products to more cloud-based applications and services. They must have the right tools to validate and prove their products perform at scale in distributed cloud and hybrid environments — especially those using zero trust security. Enterprise IT teams also need a process for testing distributed cloud environments using different methods and tools than what they use for traditional networks and data centers.

Traditional legacy networks with a defined perimeter have few network ingress / egress points and are more straightforward to validate. Distributed cloud and hybrid networks with advanced traffic patterns, complex application mixes, zero trust parameters, no defined perimeter, and numerous ingress / egress points make testing more difficult. As the world moves to more cost-effective and elastic off-premises networking and storage, measuring the unknowns becomes even more challenging.

When considering switching to a zero-trust model, you must ask yourself several questions to ensure you're choosing a solution to fit your needs. These perimeter-less, elastic, dynamic networks require a completely new testing paradigm. Are you delivering high-quality access to users, devices, and cloud services anywhere in your distributed, disaggregated networks? Is your cybersecurity infrastructure strong enough to limit exposure across your on- and off-premise networking? Are your security policies dynamically adjusting to your auto-scale events?

Introducing Keysight CyPerf

CyPerf is the industry's first scalable, cloud-native network test solution for zero trust. It deploys lightweight test agents across various physical and cloud environments, delivering insights into user experience, security posture, and performance bottlenecks. By realistically emulating authentic application traffic, user behavior, and threat vectors at scale, CyPerf measures and validates the performance of dynamic distributed networks, security devices, and services for more confident deployments.

Realistic Testing That Replicates Your Distributed Networks in Action

CyPerf emulates real user and application behavior, customizable applications and attacks to replicate a real-world environment. It delivers new heights in realism by generating both legitimate and malicious traffic across a complex set of proxies, software-defined wide-area networking (SD-WAN) devices, identity providers (IdP), secure access service edge (SASE) nodes, virtual private network (VPN) tunnels, transport layer security (TLS) inspection devices, elastic load balancers, containerized devices, and web application firewalls. Combined with the unique ability to interleave applications and attacks, this setup enables a holistic approach to replicating distributed environments in half the time and with more accuracy than other solutions.

By creating a digital twin to realistically replicate users, applications, and threats, CyPerf validates complex distributed zero trust networks. This solution measures the impact on performance and quality of experience (QoE) in the lab and in live production networks.

One of the first steps is to validate the network in action — the testing is performed as close as possible to the production environment in a hybrid, distributed manner. As cloud infrastructures are ubiquitous, this type of testing is especially applicable to cloud-based networks and security solutions, as shown in Figure 1. However, the same concepts can apply to private cloud-based and distributed networks.

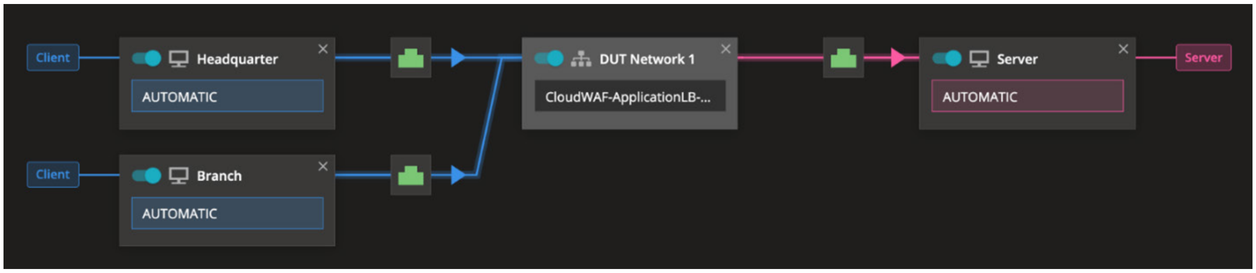

Figure 1. Example of CyPerf dashboard and distributed topology

A web-based graphical user interface (GUI) simplifies how you visualize and interact with various networked elements.

The graphical user interface (GUI) is critical to replicating your network in action as you measure and validate performance.

CyPerf is the first purpose-built test tool to validate and measure application performance and security efficacy of zero trust infrastructures for individual network components and across end-to-end architectures, as shown in Figure 2.

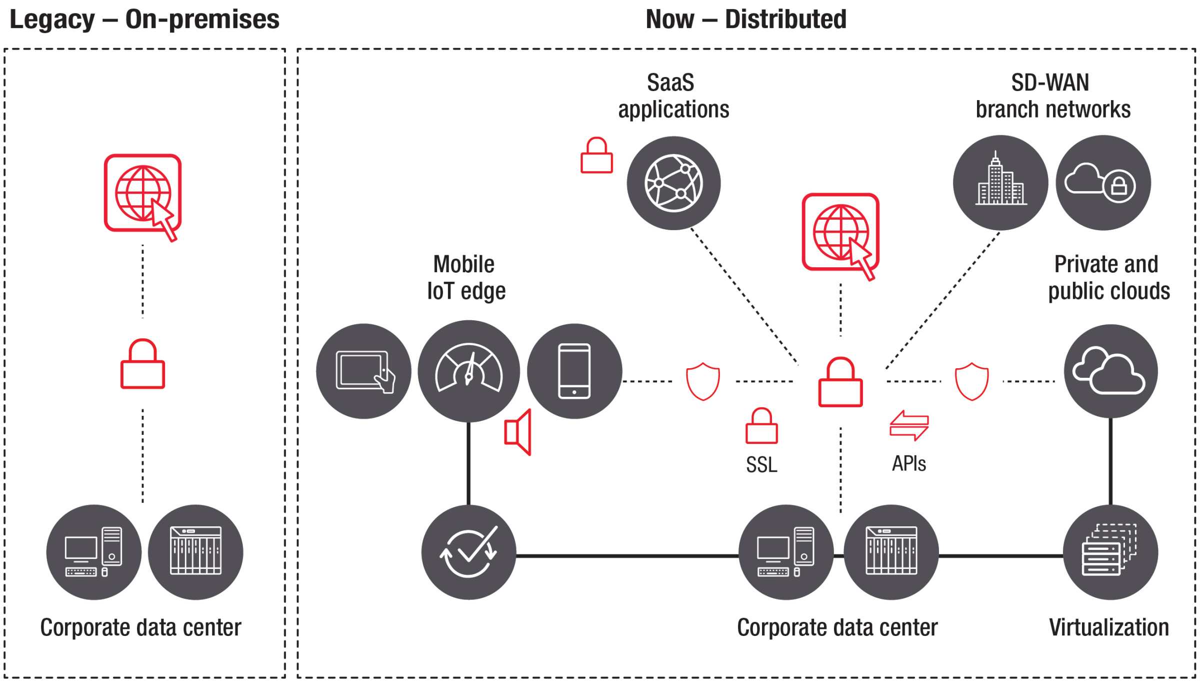

Figure 2. Deploy distributed CyPerf test agents into a variety of platforms and environments to validate application performance and the security efficacy of the underlying network infrastructure

Find the Right Balance Between User Experience and Security

The more features and functionality you enable or add to any security architecture, the more stringent the overall security becomes. But this can also incur a cost in terms of performance, which eventually impacts user experience. Dynamic environments with workloads that scale up and down with demand present new challenges in configuring and managing security infrastructure and policies with existing hardware and software.

With the right test solution, you can find the right balance of user experience and cybersecurity.

CyPerf benefits include:

High realism: Emulates real user and application behavior, customizable application mixes, and authentic attacks to replicate a real-world environment.

Native authentication: Supports authentication and authorization with the ability to send application and security traffic over authenticated sessions at a large scale.

High scalability: Supports tens of millions of concurrent users and millions of connections per second that elastically scale up and down, enabling both resiliency and chaos testing.

Containerized agents: Deploys lightweight agents as containerized pods to support a range of on-premises or managed Kubernetes deployments. Easily deploy traffic agents as virtual machines (VMs) or public cloud instances such as Amazon web services (AWS), Google cloud platform (GCP), and Azure.

Lab and live network testing: Creates a digital twin of users, applications, and threats. CyPerf supports performance and security testing in both pre-deployment lab settings and in live production networks. As parameters change or you add applications and tools, CyPerf test agents can test and validate the impact on QoE without impacting the live network.

Auto-scaling: Delivers elastically scaling traffic agents that you can easily set up and tear down dynamically during a test to validate auto-scale policies. This capability enables you to fine-tune the balance between user experience and security.

Resilient: Scales automatically and is easily portable. CyPerf is a subscription-based software solution that includes a user-friendly cloud-native GUI management dashboard that provides real time visibility.

Software test agents are the right choice for validating highly distributed networks since they can check and bring back data without impacting live network traffic. This process enables you to easily track what's happening at any given time.

Troubleshoot Hybrid Cloud Migration

CyPerf's lightweight, software agent-based architecture makes it easy to deploy and operate in lab networks, sandbox environments, and live production hybrid networks. It enables a proactive, continuous data-driven approach to validate and analyze user experience, performance, and security changes compared with previously established baselines. By distributing software traffic agents across all key network segments, you can gain immediate insights across the entire network infrastructure — reducing the time to identify network faults or baseline deviations. As a result, you will improve uptime and assure ongoing user quality of experience (QoE), performance, and security. Even in public clouds, where the underlying infrastructure is not under your control, you can uncover undisclosed infrastructure limits that impact your application performance.

Rely on Proven Application Threat Intelligence

With the application and threat landscape continuously changing, it's time to rely on Keysight, the industry leader in network applications and security testing. CyPerf is powered by the Keysight Application and Threat (ATI) subscription service — ensuring continuous up-to-the minute threat intelligence. Updates of realistic application scenarios, pre-canned traffic mixes, and a relevant library of threat vectors are updated regularly. Using advanced surveillance techniques and methodologies, our dedicated team of application and security researchers identify, capture, and provide ongoing updates to your ATI.

Keysight's ATI service won the 2020 Cybersecurity Excellence Award in the threat detection, intelligence, and response category. The Cybersecurity Excellence Awards is an annual competition honoring individuals and companies that demonstrate excellence, innovation, and leadership in information security.

CyPerf is a revolutionary solution for network testing that accelerates application delivery in today's modern networks. CyPerf effortlessly validates performance, security effectiveness, and user experience to deliver real actionable insights.

With CyPerf, NEMs can deliver the appropriate network technologies by relying on a test solution that enables them to prove and measure how their products and services perform at scale in complex distributed zero trust environments. Now enterprises and service providers also have a data-driven approach to help them choose the NEMs and other vendors that best fit their needs. Having a solution that provides continuous validation of change management will also help them to ‘right-size’ their ongoing investments.

To learn more about CyPerf or to take a free test drive, visit www.keysight.com/us/en/products/network-test/cloud-test/cyperf.

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