DATA SHEET

Keysight CyPerf

Distributed, Elastic Network Performance and Security Validation

Problem: Quantify Unknowns and Control the Chaos of Digital Transformation

Digital business transformation and edge computing are bringing major unknowns to the performance, scalability, and threat protection of network and security architectures. As an enterprise moving to more cost-effective and elastic off-premises networking and storage, you face new challenges—Are you delivering high-quality access to users, devices, and cloud services everywhere in your distributed, disaggregated networks? Is your cybersecurity infrastructure enough to limit exposure across your on- and off-prem networking? Are your security policies dynamically adjusting to your auto-scale events?

Your perimeter-less, elastic, dynamic network requires a new testing paradigm.

Solution: A Cloud-Native Test Solution that Replicates Distributed Networks in Action

Keysight CyPerf is the industry's first cloud-native software test solution that recreates every aspect of a realistic workload across a variety of physical and cloud environments to deliver unprecedented insights into end user experience, security posture, and performance bottlenecks of distributed, hybrid networks.

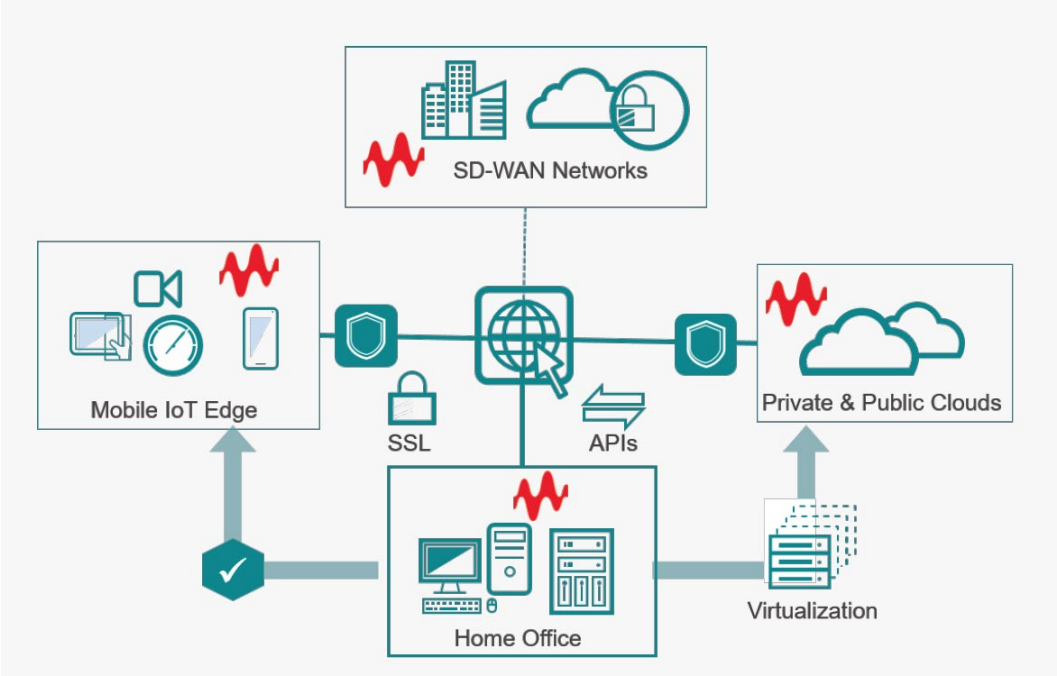
CyPerf employs lightweight agents deployed across a variety of heterogeneous environments to realistically modeling dynamic application traffic, user behavior, and threat vectors at scale. It validates hybrid networks, security devices, and services for more confident rollouts.

Highlights

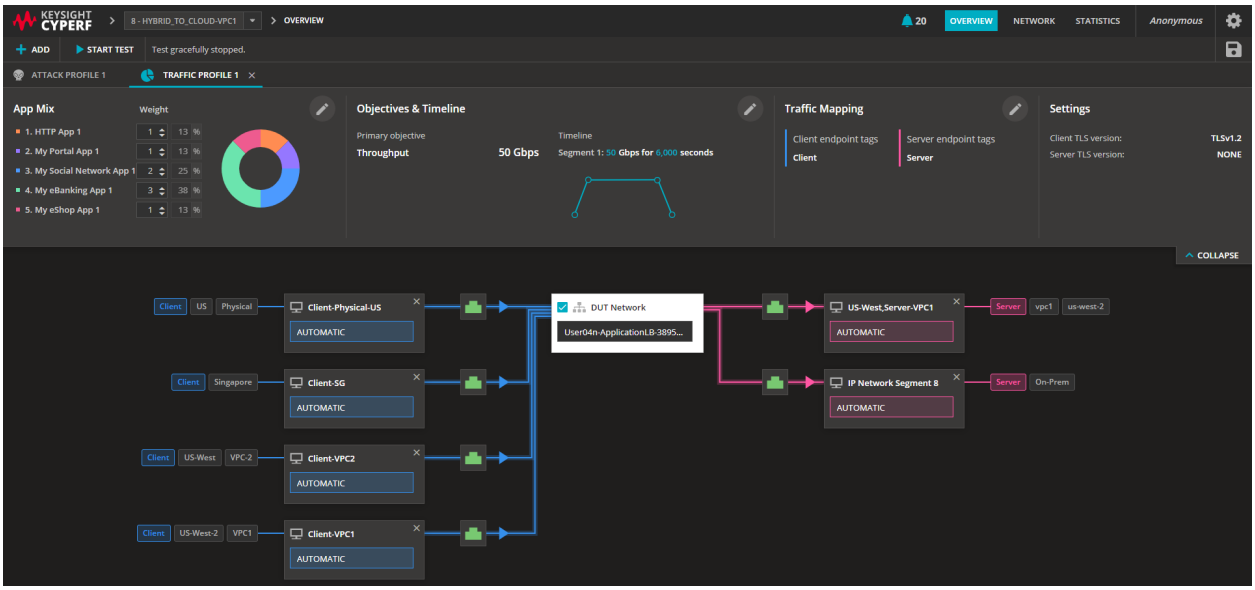
- Validate cloud and SD-WAN migration in half the time and with more fidelity by replicating distributed deployment environments with realistic workloads.
- Perform head-to-head comparisons to determine the most cost-effective cloud infrastructure and security controls.
- Validate elastic scalability of cloud infrastructures and security architectures with auto-scaling test agents.
- Easily access key performance indicators — application throughput, max concurrency (connections/user), application latency, Transport Layer Security (TLS) performance, and threat detection efficacy.
- Measure and compare hybrid and multi-cloud infrastructures for your specific workloads and security controls.
- Discover undisclosed infrastructure issues such as traffic shaping and throttling that are out of your control but impact your applications.
- Deploy a modern, cloud-native software solution on-premises or in the cloud to control and manage distributed agent-based validation.
- Accelerate your continuous integration / development (CI / CD) pipeline with a repeatable and automatable software solution.

KEYSIGHT TECHNOLOGIES

CyPerf delivers new heights in realism that comes from simultaneously generating both legitimate traffic mixes and malicious activities across a complex network of proxies, software-defined wide area networking (SD-WAN), VPN tunnels, Transport Layer Security (TLS) inspection, elastic load balancers, and web applications firewalls (WAF). Combined with the unique ability to interleave applications and attacks to model user behavior and security breaches, CyPerf enables a holistic approach in replicating distributed customer deployment environments faster and with more fidelity than other solutions.



Distributed topology with CyPerf agents installed.



CyPerf UI with an application and attack profile configured to validate distributed network security and performance.

Key Features

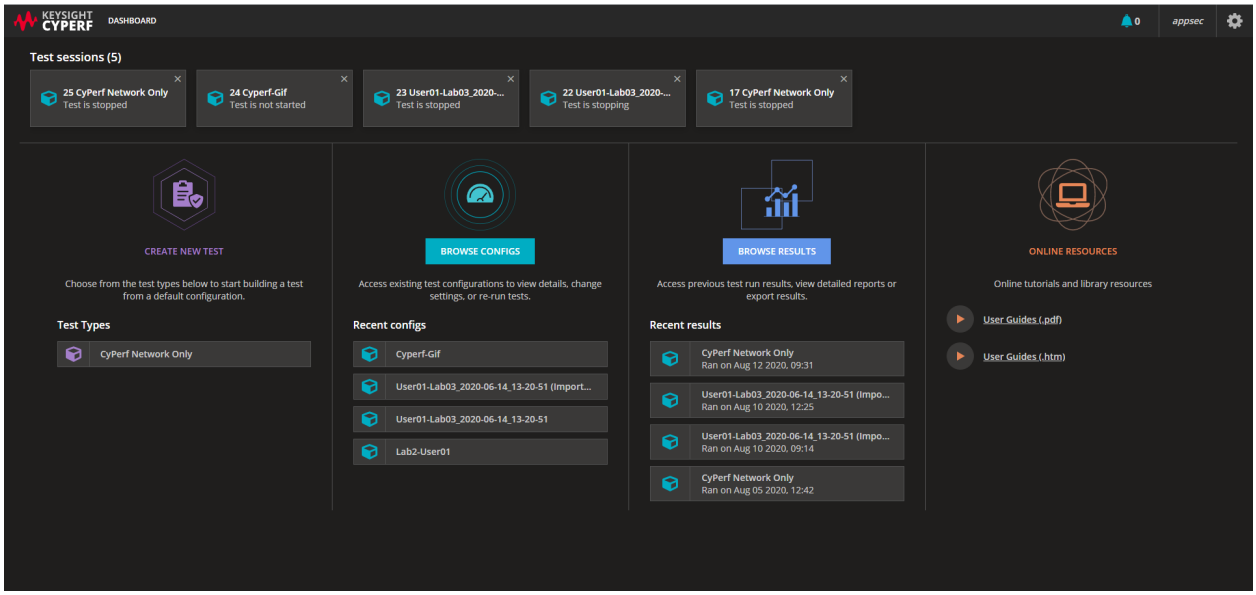
Traffic agents

- Light-weight software-based test agents are infrastructure agnostic, allowing operations on virtual machines, cloud instances, or off-the shelf servers — on-premises, and private and public clouds.
- Agents can be part of auto-scale groups, dynamically scaling up or down while the test runs to validate both the performance and security of such dynamic environments.
- With a proprietary goal-seeking algorithm, test agents achieve the highest possible performance to validate the performance limits of various compute environments.
- Intelligent network mapping features allows individual agent or groups of agents to include tagged application(s), allowing users to create complex topologies that can span dozens of agents with each carrying unique applications and attacks.
- Agents simulate both the clients and the servers to create the unique closed loop scenario where the underlying device / network performance or security can be tested without the added risk or cost of accidental exposure of attacks to actual endpoints or servers.
- Agents can query a host interface and leverage its capabilities to deliver superior TLS and application performance.
- Highly resilient test agents are designed to survive connection disruptions, crashes, or other events common in distributed and dynamic environments.

Dashboard showcasing multiple agents simulating geographically distributed clients and servers.

CyPerf Application

- CyPerf application is a completely cloud-native, microservices-based, elastically scalable application that can be deployed as a virtual machine or as cloud. It is developed-on top of a Kubernetes-based architecture, so it is scalable, resilient, and self-healing.
- It offers a modern, easy to use web-based user interface (UI) that is accessed through web browsers, making it flexible to configure and run tests from anywhere in the world.
- The session-aware UI supports multi-user authentication. Session support is tailor-made for teams to either individually or collaboratively manage sessions, upload configurations, run tests, monitor results or download reports.
- Developed ground up with a REST API approach that enables integration of CyPerf in all modern automation frameworks where users can configure tests, emulate applications and attack traffic, and gather results — all through REST API calls.



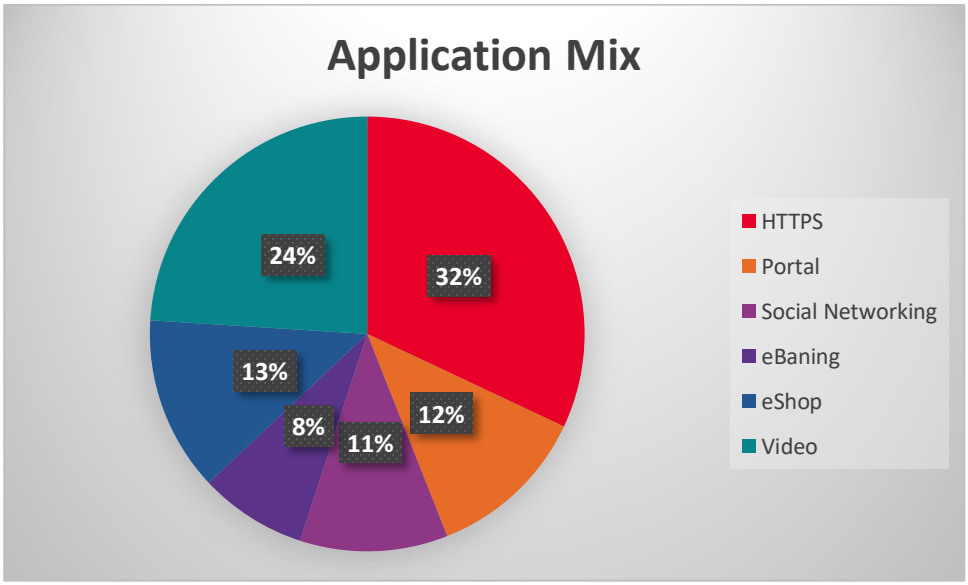
CyPerf UI dashboard with ability to access sessions, browse configurations and results, create test, etc.

CyPerf Application and Attack Simulation

CyPerf builds on 20+ years of leadership in network security testing to reveal your security exposure across public, private, and hybrid networks. The ongoing research of our Application and Threat Intelligence (ATI) team ensures regular updates so you have access to the latest application and threat simulations.

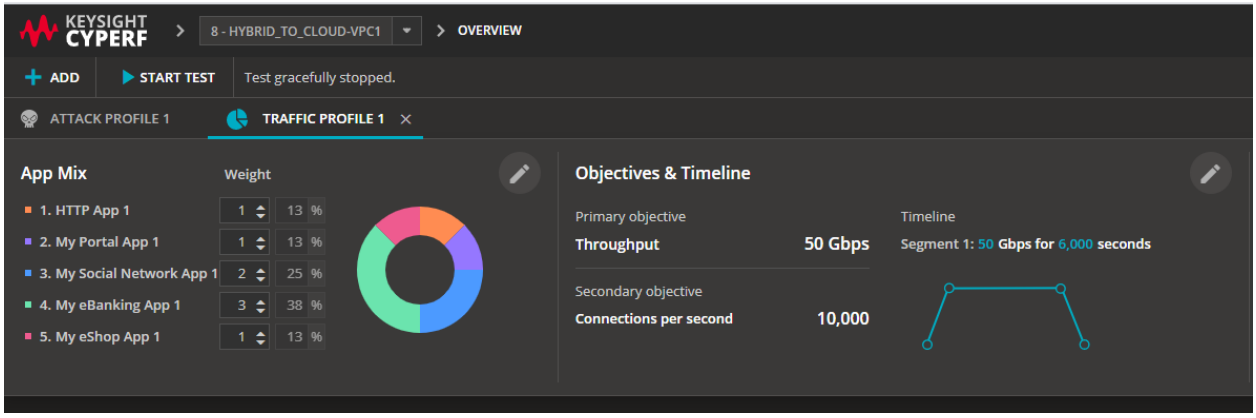
- Comprehensive application and attack support with the ability to emulate applications and attacks interleaved together.
- Application actions can be fully parameterized to emulate real-world users and applications aligned with your test environment.

- Highly realistic attacks that can be interleaved with application actions, allowing replication of kill chains, customization of attacks, and executing advanced use cases where a certain pre-condition (like authentications) are needed before the execution of the attacks.
- Web applications emulating common website types to accurately represent the wide variety of traffic seen in the internet.



CyPerf supports a variety of applications to represent internet traffic

- Various application variants covering different browser and server technologies like Chrome, Firefox, Opera, Safari, Android, Apache, IIS, and Nginx.
- Exploits and malware that cover a wide array of attack strategies and types like injections, XSS, and other OWASP and non-OWASP exploits and families of well-known malware.

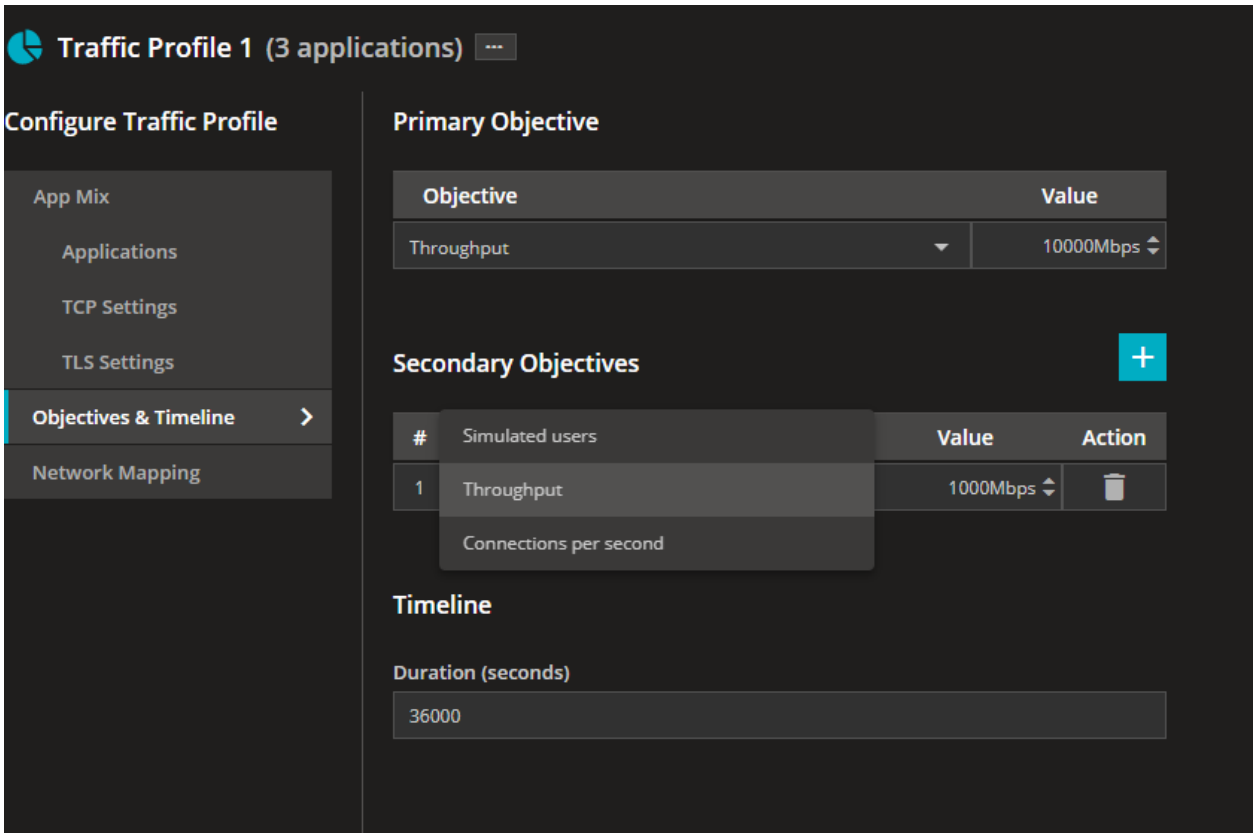


Application Mix configurations allow replication of various custom profiles

CyPerf Objectives

CyPerf is armed with Keysight's proprietary goal seeking algorithm that allows the test agents to achieve stable and consistent key performance indicators (KPIs) like bandwidth and connections per second, which truly represents the real performance of that network infrastructure or WAN link. CyPerf's dual-objective support helps customer set multiple test objectives to check if the underlying network infrastructure can achieve a certain throughput while maintaining a certain number of active flows per seconds or simulated users.

CyPerf's ability to set attack rate as an objective allows users for the first time to send exploits, malware, or other attack types at a pre-determined rate.



Objective and timeline functions enable users to control application or attack objectives

Statistics and Reporting

CyPerf delivers a comprehensive statistics and reporting framework that is visually rich and contains concise performance metrics at test, application, attacks, and agent levels. It covers the key performance and security indicators of the entire test so users also have the flexibility to drill-down into traffic profile statistics or attack profile statistics where they can explore application performance or attacks per network segment/agent. More application-specific statistics are available for the next level of debugging for each individual application-action or attack.

CyPerf's visually rich statistics and reporting delivers comprehensive performance metrics.

CyPerf Specifications

Key specifications	Options
Deployment Options for Agents	• AWS-AMI or via CFT • VM-OVA • Bare metal via Debian installer over stock Ubuntu 18.04
Deployment options for Application & UI	• Bare metal • AWS-AMI or via CFT • VM-OVA
DUT Configurations Supported	• Reverse / transparent proxy • Application load balancer / elastic load balancer • NGFW / IPS / web application firewall • VPN tunnels • Others (The client and server test agents are completely detangled allowing them to traverse any kind of DUT configurations as long as there is IP communication between them)
Test Topologies Support	• Geographically distributed location – Application and security traffic sent between test agents deployed in multiple physical locations • Hybrid - Application and security traffic sent between test agents distributed between physical locations and cloud

Key specifications	Options
	• Multiple cloud - Application and security traffic sent between test agents deployed in different cloud locations • Agents deployed in dynamically scaling auto-scale groups
Objective Types Support	• Throughput • Connections per second • Simulated users • Objective with constraints • Attacks per second • Concurrent attacks • Multiple objective support - Ability to set dual objectives like throughput and simulated user be set at the same time
Application Type Support	• Web-based apps including social media, portal, e-commerce, financial, video, etc.
Encryption Support	TLS 1.2 with major ciphers and key sizes supported: • AES128-GCM-SHA256 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA- AES128-GCM-SHA256 • ECDHE-RSA- AES256-GCM-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA384
Attack Type Support	• Injection • XML external entities (XXE) • Cross site scripting (XSS) • Insecure deserialization • Directory traversal • File inclusion (both LFI & RFI) • Information disclosure • Cross site request forgery • Authentication bypass • A small set of server-to-client attacks • Client to server malware • Webshell attack lifecycle

Key specifications	Options
Key Performance Indicators	• Total number of client and server agents in a test • Throughput • Connection per second • Simulated users • Total count of attacks allowed / blocked • Total applications success / failed • Average latencies: connect time, time to first byte (TTFB), time to last byte (TTLB)
Statistics	• KPI statistics • Attacks sent – Allowed / blocked • Per network segment application / attacks • TCP • TLS handshake / throughput • Per application actions • Per agent KPI statistics
Reporting	• PDF • CSV
Max IP Addresses per Agent	10,000
Automation	• Complete coverage of all actions through REST API • REST API documentation

Product Ordering Information

Part Number	Description
938-1010	**IXIA, CyPerf 10 Agents and 10Gbps of Performance Bundle (1-year subscription)**. All-inclusive Distributed Application Performance and Security Testing Bundle. The bundle includes: • Access to the CyPerf Cloud-native software application • Up to 10 CyPerf test agents that can be deployed on customer's environment • Up to 10 Gbps of throughput performance • Access to ATI, software updates and customer support for the purchased term of the subscription License term needs to be specified (must be purchased in multiples of years, up to 5-years maximum, the list price is per unit per year).

Part Number	Description
938-1001	**IXIA, CyPerf Single Agent Floating License (1-year subscription).** Requires previous purchase of 938-1010 CyPerf Bundle. License term needs to be specified (must be purchased in multiples of years, up to 5-years maximum, the list price is per unit per year).
938-1002	**IXIA, CyPerf 10G Performance Floating License (1-year subscription).** Requires a previous purchase of 938-1010 CyPerf Bundle. License term needs to be specified (must be purchased in multiples of years, up to 5-years maximum, the list price is per unit per year).
938-1030	**IXIA, CyPerf 10 Agents and 10Gbps of Performance Bundle (30-day subscription).** All-inclusive Distributed Application Performance and Security Testing Bundle. The bundle includes: • Access to the CyPerf Cloud-native software application • Up to 10 CyPerf test agents that can be deployed on customer's environment • Up to 10 Gbps of throughput performance • Access to ATI, software updates and customer support for the purchased term of the subscription
938-1003	**IXIA, CyPerf Single Agent Floating License (30-day subscription).** Requires a previous purchase of 938-1030 CyPerf Bundle.
938-1004	**IXIA, CyPerf 10G Performance Floating License (30-day subscription).** Requires previous purchase of 938-1030 CyPerf Bundle.

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

This information is subject to change without notice. © Keysight Technologies, 2020, Published in USA, September 4, 2020, 3120-1464.EN