Keysight CyPerf

Scalable Network Application and Security Testing for Distributed Cloud

Problem: Quantify Network Unknowns in Hybrid Distributed Environments

Digital business transformation and edge computing are bringing major unknowns to the performance, scalability, and threat protection of network and security architectures. As networks evolve to more cost-effective and elastic off-premises infrastructures, adopting new security frameworks like zero trust bring new challenges. Are you delivering high-quality access to users, devices, and cloud services everywhere in your distributed, disaggregated networks? Is your cybersecurity infrastructure secure enough to limit exposure across your on- and off-prem networking? Are your security policies dynamically adjusting to your auto-scale events? Are your zero trust policies reducing the attack surface without impacting performance?

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

Solution: An Instantly Scalable Test Solution to Replicate Distributed Cloud Networks in Action

The Keysight CyPerf is an instantly scalable cloud-native software test solution that recreates every aspect of a realistic workload across a variety of physical and cloud environments. It delivers unprecedented insights into end user experience, security posture, and performance bottlenecks of distributed, hybrid networks.

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

KEYSIGHT

Table of Contents

CyPerf Highlights

- Test the functionality and performance of zero trust network access policies with authenticated and unauthenticated application traffic and security attacks.
- Validate cloud, SASE, and SD-WAN migration in half the time with more fidelity by replicating distributed deployment environments with realistic workloads
- Prepare for the Post Quantum Cryptography (PCQ) transition by testing the functionality, performance and scale of network devices (e.g., NGFWs, MiTM/Decryption, ALB/ELB, SSL offload devices etc.) or end-to-end infrastructures with stateful TLS 1.3 PQC key agreement.
- Validate the performance, stability and security efficacy of AI runtime solutions (e.g., AI API Interceptor) or inline AI security gateways with realistic AI LLM legitimate and adversarial traffic.
- Benchmark the performance of AI inference deployments by generating high scale AI LLM prompt requests against a real inference server.
- Emulate thousands of SSL VPN tunnels to test the scale, performance, and robustness of VPN Gateways.
- Test the performance and functionality of smartNICs and DPUs by deploying virtualized/containerized test agents on the smartNIC host server as well as externally on COTS or the dedicated APS-ONE-100 hardware appliances.
- Validate the control plane performance and scalability of IPsec Gateways, as well as the application performance and security efficacy of IPsec VPN enabled network security solutions.
- 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 dynamic auto-scaling test agents.
- Access key performance indicators easily — application throughput, max concurrency (connections / users), application latency, Quality of Experience (QoE) metrics such as Mean Opinion Score (MOS) for media traffic, Transport Layer Security (TLS) performance, and threat detection efficacy.
- Measure and compare hybrid, multi-cloud, container infrastructures for your specific workloads and security controls.
- Accelerate your continuous integration / development (CI / CD) pipeline with the CyPerf REST APIs and Terraform orchestration.
- Leverage the hyperscale performance of the new APS-ONE-100 hardware appliance managed by the APS-M1010 controller. A single APS-ONE-100 delivers unmatched real-world TLS scalability of up to 6M concurrent connections, 165K TLS connections per second, and 185Gbps encrypted throughput. The ground-breaking scale of a 10-appliance system generates 60M TLS concurrent connections, 1.6M TLS connections per second and 1.85 Tbps encrypted TLS throughput.

CyPerf delivers new heights in realism by simultaneously generating legitimate application traffic and security attacks across a complex network of proxies, Software-Defined Wide Area Networking (SD-WAN), Secure Access Service Edge (SASE), SSL VPN tunnels, IPsec tunnels, Transport Layer Security (TLS) inspection, elastic load balancers, Web Applications Firewalls (WAF) and Zero Trust Network Access (ZTNA) environments. 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 accuracy than other solutions.

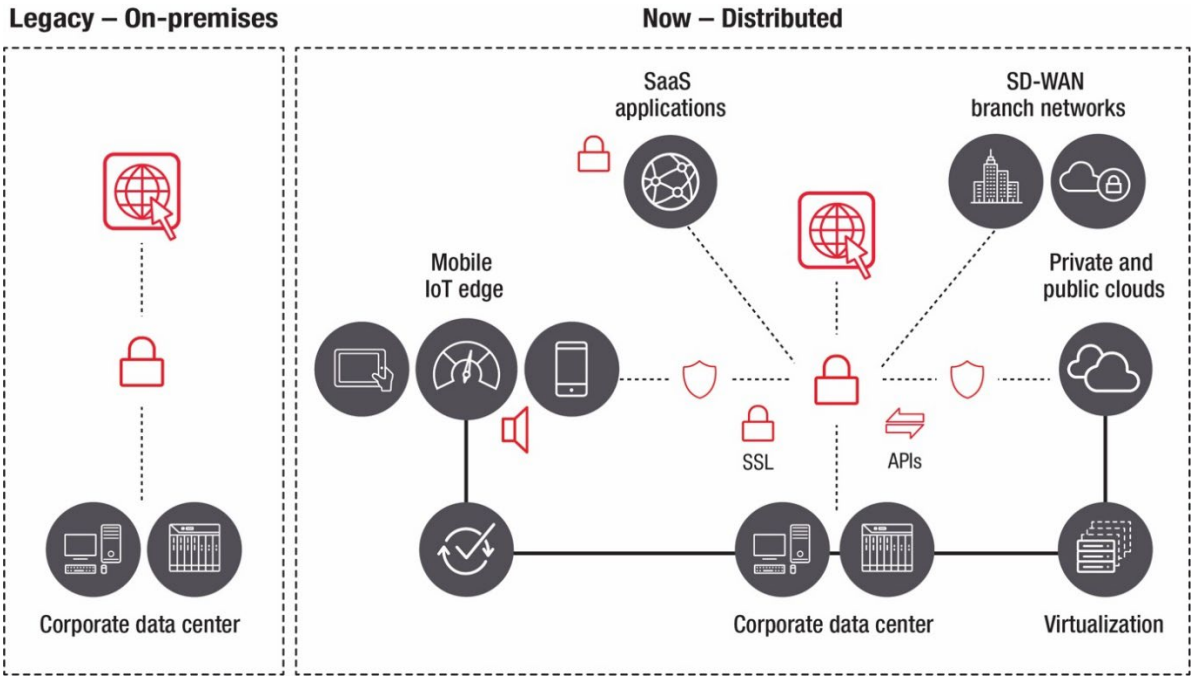

Figure 1. Evolution to a distributed topology with CyPerf agents installed across a heterogenous environment

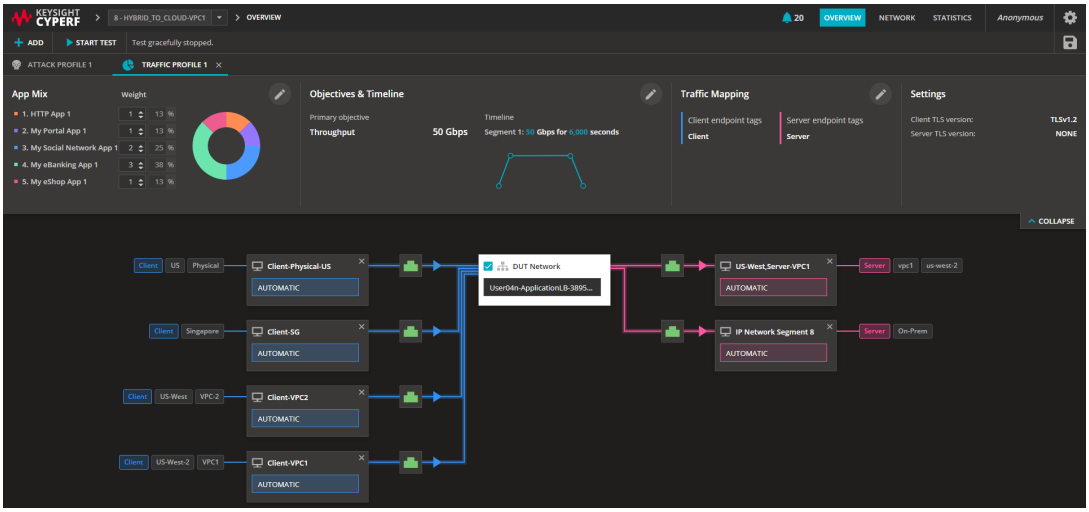

Figure 2. CyPerf UI configuration of an application and attack profile to validate distributed network security and performance

Key Features

Traffic Agents

- Deploy light-weight software-based test agents that are infrastructure agnostic, allowing operations on Virtual Machines (VM), containers, cloud instances, or off-the shelf servers on-premises, private, and public clouds.
- Scale agents in auto-scale groups up or down dynamically while the test is running to validate both the performance and security of such dynamic environments.
- Generate authenticated and unauthenticated application traffic and security attacks to validate zero trust network access authentication policies at scale.

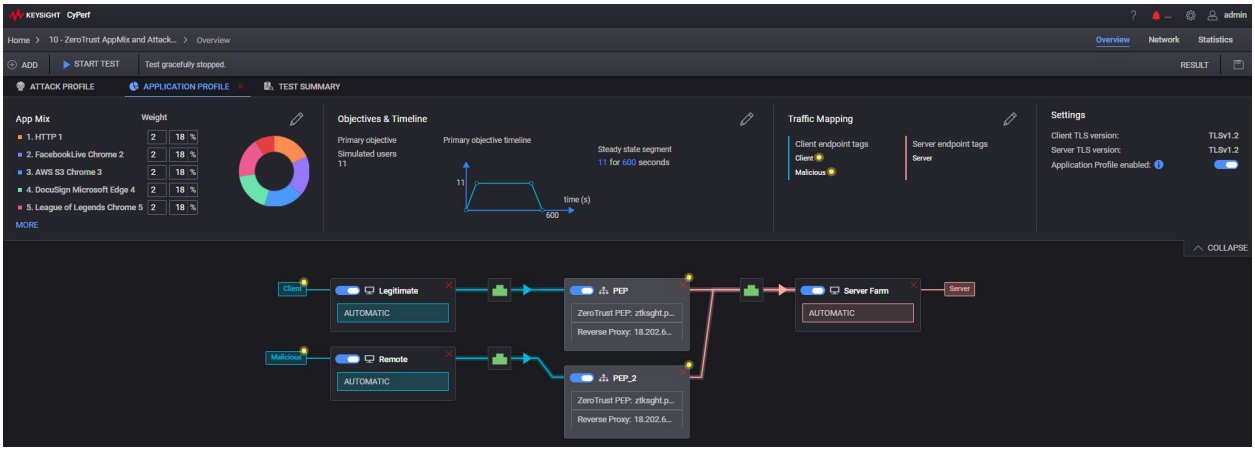

Figure 3. CyPerf UI configuration of a realistic application mix, security attacks and multiple user profiles to test Zero Trust Network Access policies

- Emulate thousands of SSL VPN tunnels and run applications and attack traffic through previously established VPN tunnels to test the scale, performance, and robustness of VPN Gateways.

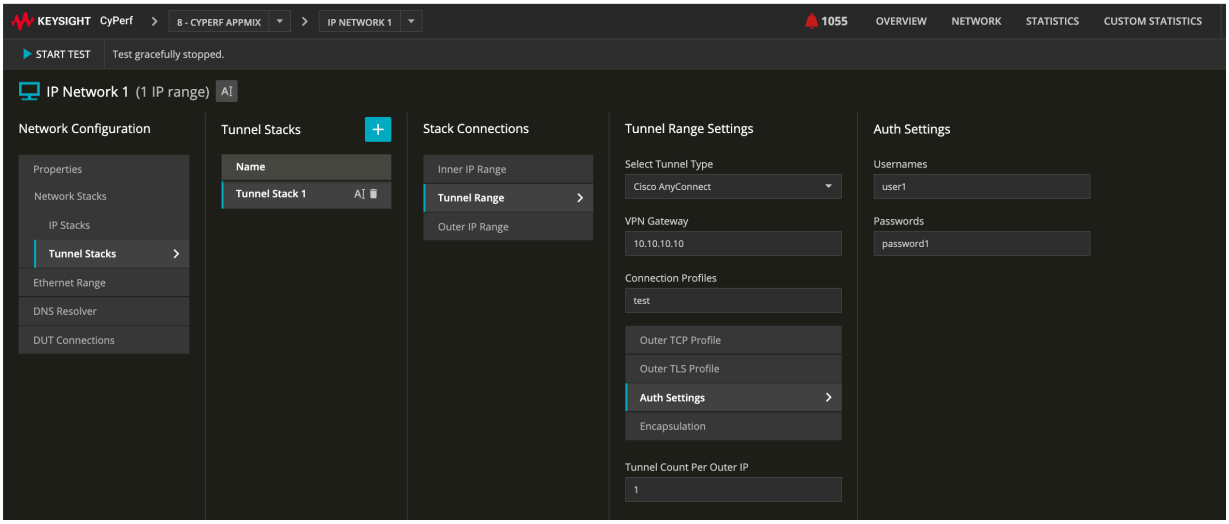

Figure 4. Built-in support for scalable SSL VPN testing

- Validate the control plane performance and scalability of various form factor IPsec Gateways, including VMs, public cloud instances or even containerized devices. Extend the control plane testing with application performance and security efficacy of IPsec VPN enabled network security solutions.

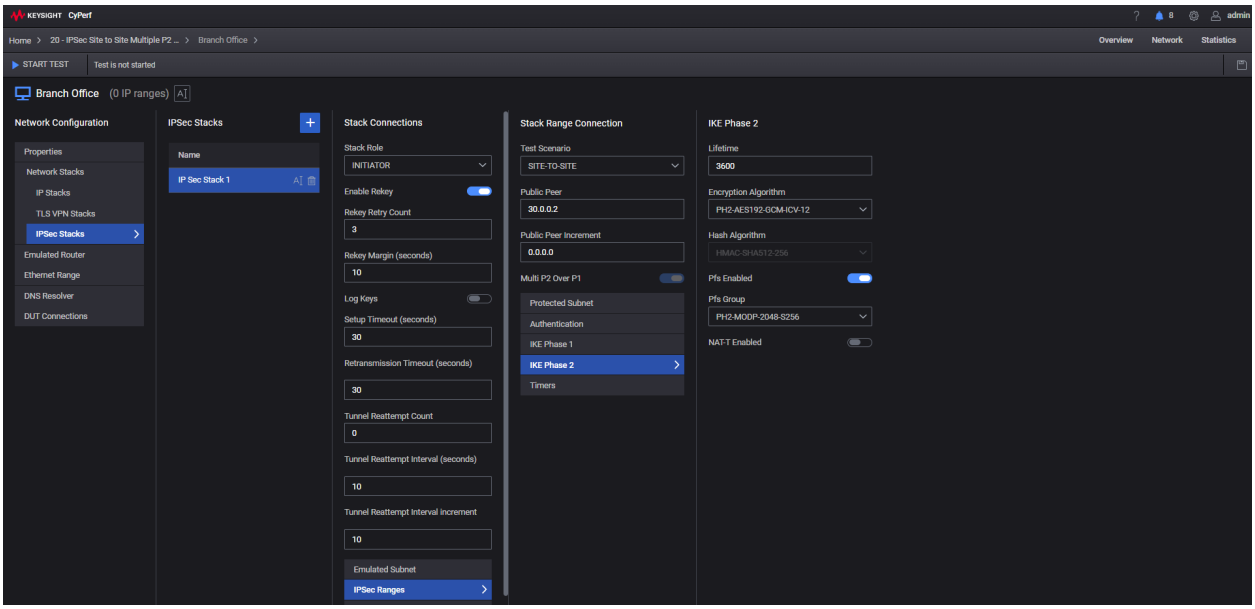

Figure 5. Emulate stateful IPsec VPN tunnels and realistic application mixes and security attacks on top

- Run applications and attack traffic through all major proxy modes: reverse proxy, transparent, and forward proxy (including tunnel mode).

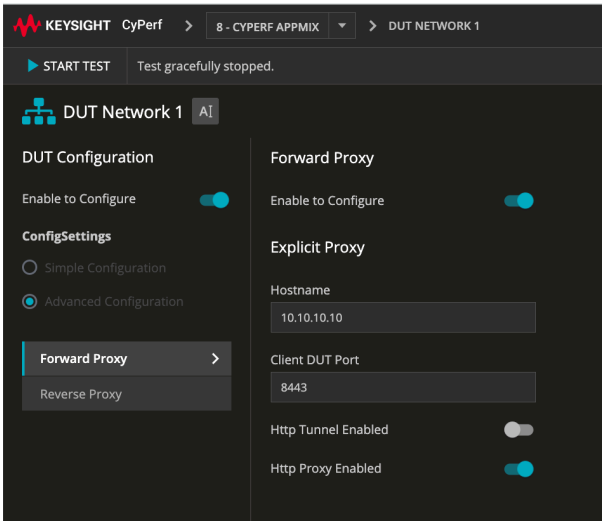

Figure 6. CyPerf has native support for all major proxy modes for both applications and attack traffic

- Granular network mapping features allow individual agent or groups of agents to include tagged application(s), allowing users to create complex topologies that can span dozens of agents, each carrying unique applications and attacks.
- Achieve the highest possible performance with minimal user intervention to validate performance limits of various devices and infrastructures using a proprietary goal-seeking test agent algorithm.
- CyPerf traffic agents can scale up to millions of concurrent connections and millions of connections per second (depending on the underlying hardware resources).

- Agents simulate clients and servers to create a unique closed loop scenario where the underlying device / network performance or security is tested without the added risk or cost of accidental exposure of attacks to actual endpoints or servers.
- Highly resilient test agents can survive connection disruptions, crashes, or other events common in distributed and dynamic environments.

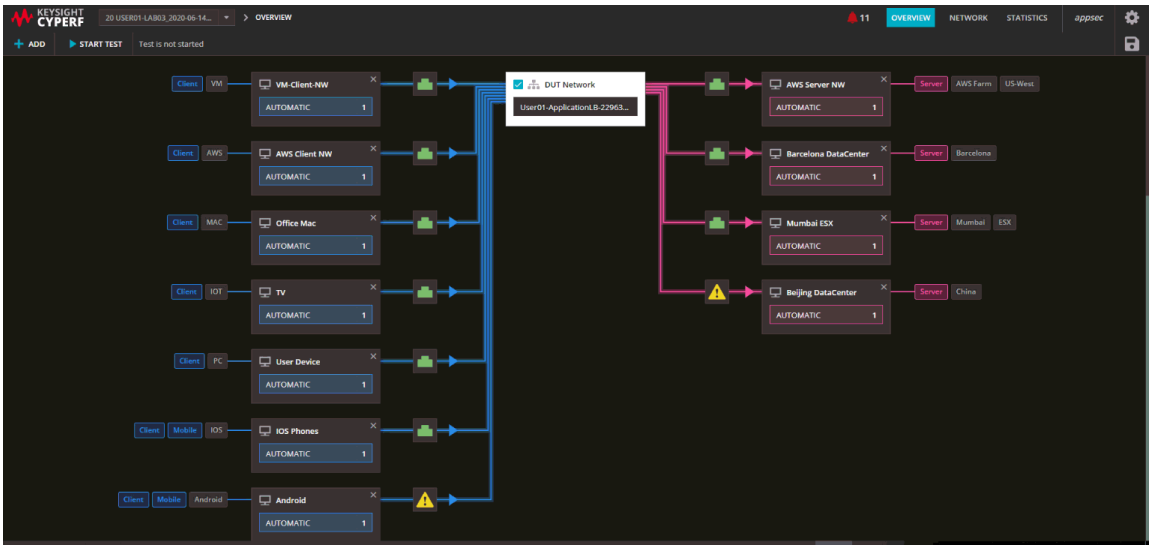

Figure 7. Dashboard showcasing multiple agents simulating geographically distributed clients and servers

CyPerf Controller

- CyPerf controller is a completely cloud-native, microservices-based, elastically scalable application deployed as a virtual machine (on-prem or in public clouds). Developed on top of a Kubernetes-based architecture, it leverages attributes that make it scalable, resilient, and self-healing.
- A modern, easy to use web-based User Interface (UI) allows access through web browsers, making it flexible to configure and run tests without introducing the frictions of a thick dedicated application.
- Session-aware UI supports multi-user authentication. Session support is tailor-made for teams to manage sessions individually or collaboratively, upload configurations, run tests, monitor results, or download reports.
- Developed from the ground up with a REST API approach enables integration of CyPerf in modern automation frameworks where users can configure tests, emulate applications, and attack traffic, and gather results — all through REST API calls.

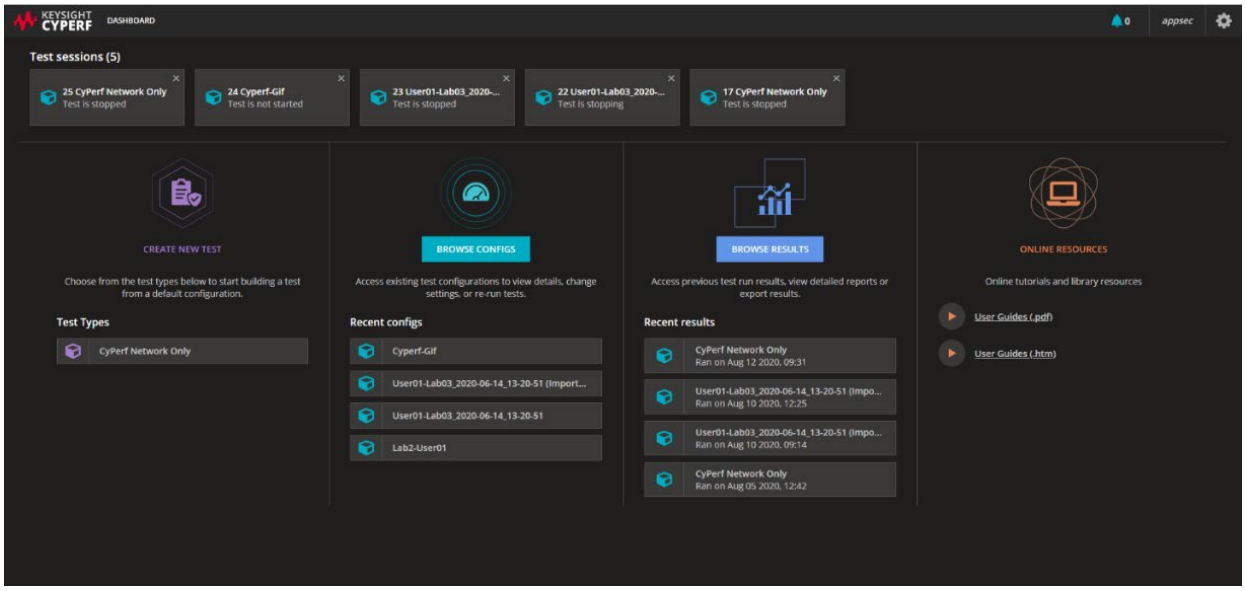

Figure 8. CyPerf UI dashboard with ability to access sessions, browse configurations, results, and create new tests

CyPerf Hardware Platforms

The Keysight APS-100/400GE family next-generation application and security test platform, consisting of the APS-M1010 controller and APSONE-100 appliance, recreates hyperscale environments in a modular, grow-as-you-need approach. With CyPerf, the APS-ONE-100 appliance is used in a stack mode and controlled by the APS-M1010 controller, which supports up to ten appliances in a single system. Leveraging the unmatched power of APS-ONE-100 compute nodes and the unparalleled CyPerf capabilities, users can address high-performance test scenarios within the most challenging deployment requirements. Complex test topologies can be achieved combining APS-ONE-100 compute nodes with virtual test agents building test environments for smarNICs / DPUS or geographically distributed topologies for testing SD-WAN / SASE or even cloud interconnects.

CyPerf Application and Attack Simulation

CyPerf is built on 20+ years of leadership in network security testing to reveal your security exposure across public, private, and hybrid networks. The research of our Application and Threat Intelligence (ATI) team ensures regular updates that provide access to the latest application and threats simulations.

- Comprehensive, continuously expanding library of applications with the ability to emulate:
  - Common enterprise applications, including complete Office 365 suite (for example, Outlook, OneDrive, Excel), Yammer, Google suite (for example, Drive, Sheets, Slides), Jira, Salesforce, AWS, DocuSign, Dropbox, Verse, ChatGPT, Open AI API, and Gemini AI API.
  - Datacenter: SMTP, DNS, FTP MongoDB, ADP, MSSQL, PostgreSQL, SMBv2, NFS, CIFS, UDP
  - IoT: MQTT, Modbus, S7comm, Profinet, CAPWAP, DNP3, IEC104, BACnet-IP.
  - Social Media: ChatGPT, Instagram, Shopify, Facebook, Reddit, Skype, Tubi, YYLive, Hulu
  - Gaming/Entertainment: League of Legends, Dreambox, NetEase Music, Airbnb, Baidu
- Realistic media emulation (that is, MS Teams, Zoom, Whatsapp, VoIP) with voice and video support, including quality of experience metrics such as Mean Opinion Score (MOS)
- High-scale, customizable AI LLM prompt requests emulation (client-only) to validate and benchmark real AI inference deployments providing inference native statistics (e.g,, token rates, time-to-first-token, time-to-last-token)
- Realistic AI LLM legitimate and attack traffic generation to test individual network solutions or end-to-end AI inference infrastructures (frontend networks, AI security gateways, AI API Interceptors, smartNICs)
- Think/idle actions mimic user inactivity periods (interleaved with regular application actions)
- Parameterize application actions to emulate real-world users and applications that align with your production environment
- Highly realistic attacks can be interleaved with application actions, allowing replication of complex malicious activities, customization of attacks, and executing advanced use cases where a certain pre-condition (like authentication) is necessary before executing the attacks
- Web applications emulating common web interaction types accurately represent the wide variety of internet traffic

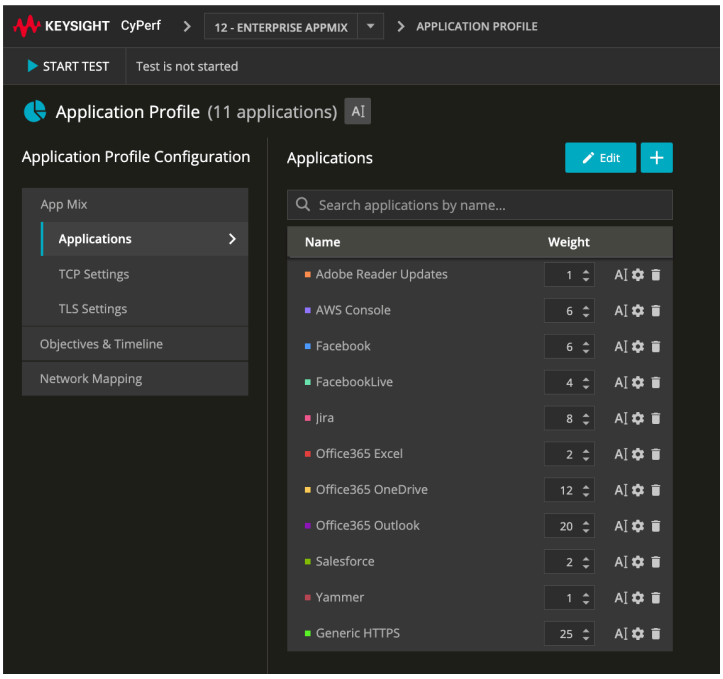

Figure 9. CyPerf supports a variety of applications to realistically represent internet traffic

- AppReplay functionality enables users to create custom applications from imported capture (pcap) files and regenerate them either standalone or within a mix of applications. Such pcap-generated custom applications can be run with configurable TCP or UDP parameters including an optional stateful TLS layer.
- AppReplay also features native HTTP transport capabilities enabling advanced test scenarios for HTTP-based pcap replay with additional customization through various fields parametrization (for example, URLs, headers, body). HTTPS encrypted packet captures can now be imported and decrypted (using the corresponding SSL keys) for creating custom apps using the real payload.
- Application variants support different browsers, including Chrome, Firefox, Safari, Edge, Internet Explorer, Opera, Android, and server technologies such as Apache, IIS, and Nginx.
- Customizable UDP Streams generates high performance UDP traffic flows for testing iMIX scenarios, background UDP traffic with realistic application mixes and raw forwarding performance using standard UDP packet sizes.

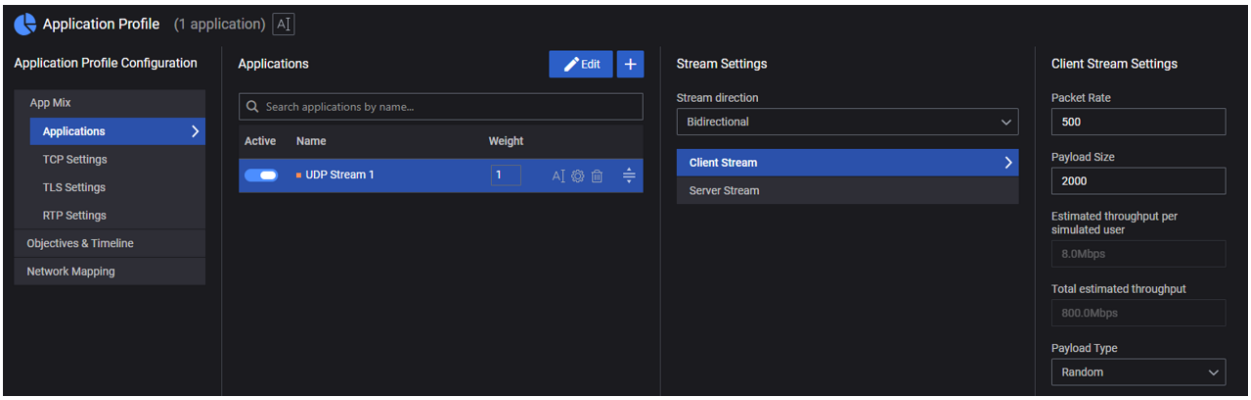

Figure 10. UDP Stream allows customization of various custom UDP flows

- Exploits and malware cover a wide array of attack strategies and injection types like XSS, and other OWASP and non-OWASP exploits and families of well-known malware.
- Extend configuration flexibility with playlists (for selected attacks and application fields) and macros (for HTTP headers and payload), allowing users to create unique application and attack variations.

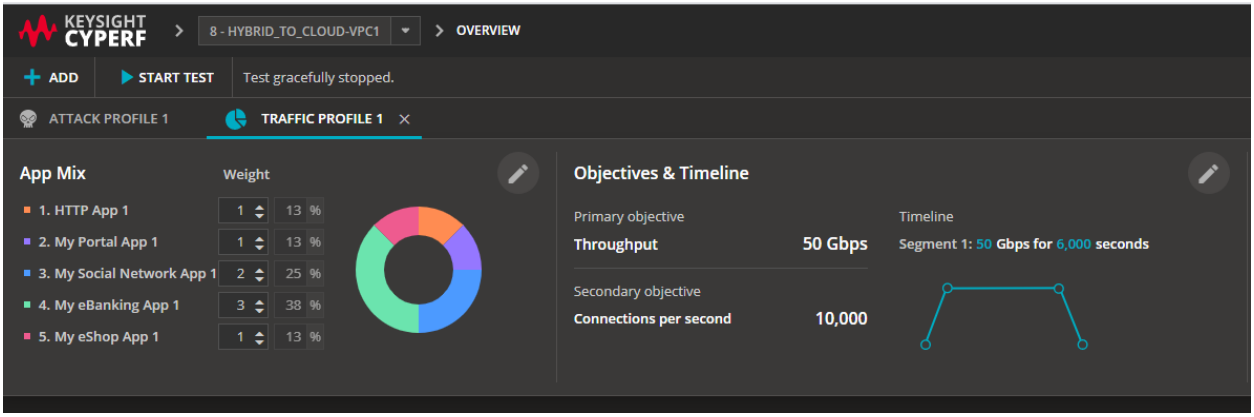

Figure 11. Application Mix configurations allow replication of various custom profiles

CyPerf Objectives

Keysight's proprietary goal seeking algorithm allows CyPerf test agents to converge towards stable and consistent Key Performance Indicators (KPIs) like bandwidth and connections per second, which represents the real performance of the network infrastructure or device being tested with minimal user intervention. The Keysight CyPerf dual-objective support allows you to set multiple test objectives to determine if the underlying network infrastructure can achieve a specified throughput while maintaining a set number of simulated users. CyPerf can also gradually ramp up the traffic load up to the required target in configurable increments for rate-based objectives (throughput and connections per second).

Because of the CyPerf ability to set attack rate as an objective, for the first time, users can now send exploits, malware, or other attack types at a predictable, predetermined rate.

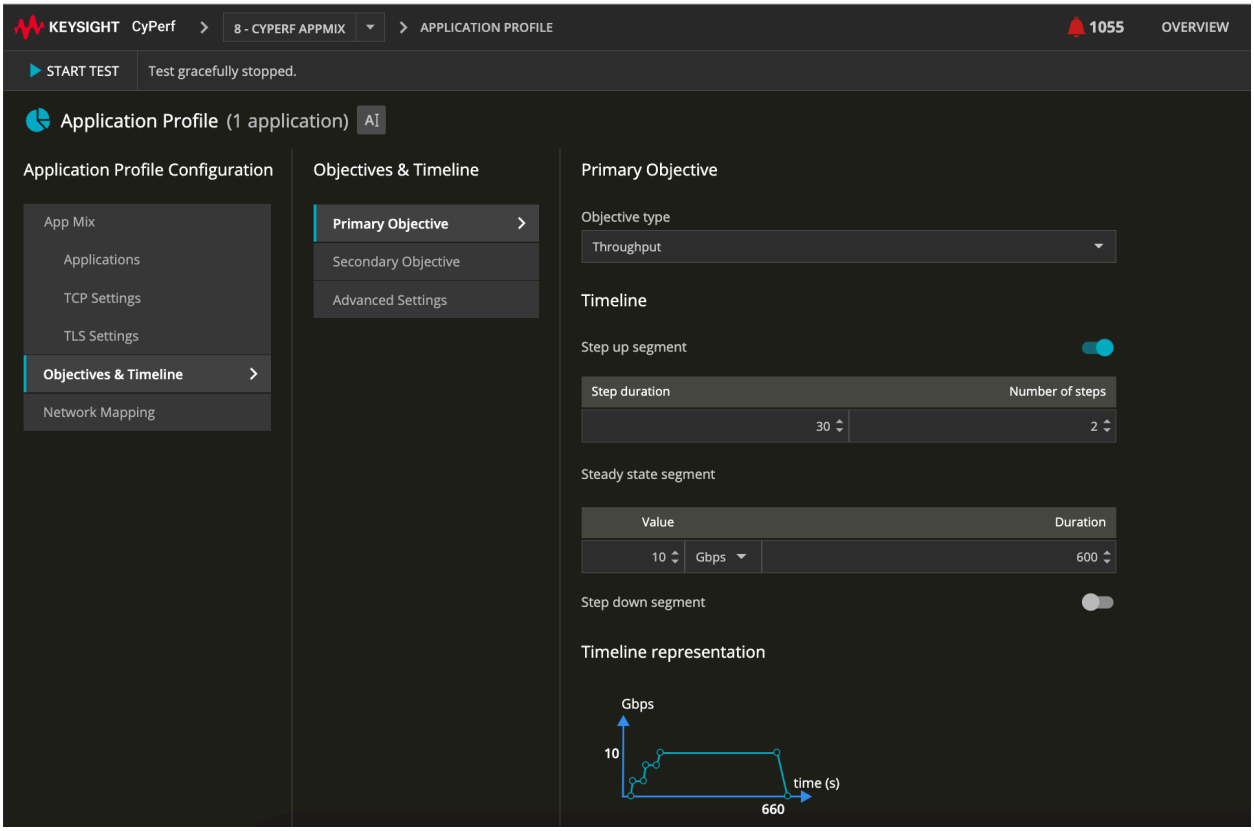

Figure 12. Objective and timeline functions enable users to control application or attack objectives

Statistics and Reporting

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

Figure 13. CyPerf's visually rich statistics and reporting delivers comprehensive performance metrics

CyPerf provides access to an extremely granular set of statistics allowing users to inspect detailed statistics on a **per-playlist entry** basis and acquire needed insights, through customizable dashboards when iterating through a long list of entries for fields such as user credentials, URL paths or various attacks variants.

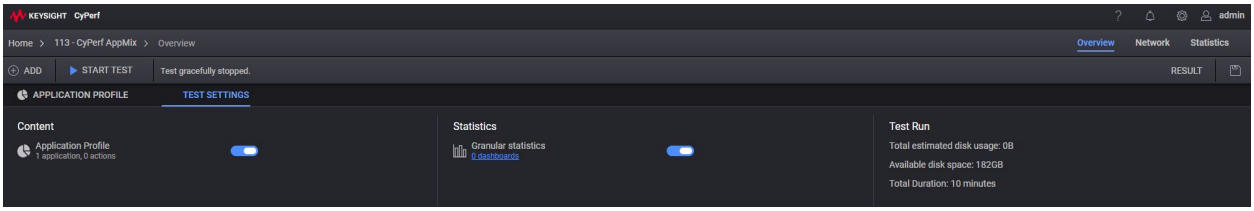

Figure 14. Granular statistics provides users with in-depth access to per-playlist entry statistics

CyPerf Performance on APS-ONE-100

Metric	1 x APS-ONE-100 Managed with APS-M1010 Controller
HTTP Bidirectional Throughput (L23)	**190 Gbps**
HTTP Unidirectional Throughput (L23)	**190 Gbps**
HTTP Connections per Second	**4.8 M**
HTTP Concurrent Connections	**45 M**
AI LLM Prompts per Second	**10 K**
TLS Throughput (TLS 1.2, ECDHE ECDSA, 256 P, 1MB page)*	**185 Gbps**
TLS Handshakes per Second (TLS 1.2, ECDHE ECDSA, 256 P 1B page)*	**165 K**
TLS Concurrent Connections (TLS 1.2, ECDHE ECDSA, 256 P)*	**6 M**
TLS Throughput (TLS 1.2, ECDHE RSA 2k key, 256 P 44 KB page)* (L23)	**150 Gbps**
TLS Handshakes per Second (TLS 1.2, ECDHE RSA 2k key, 256 P 44KB page)*	**110 K**

CyPerf Specifications

Key Specifications	Options
Deployment options for agents	• Public Clouds: ◦ Amazon Web Services (AWS) - Marketplace ◦ Microsoft Azure - Marketplace ◦ Google Cloud Platform (GCP) • Private Clouds: ◦ VMware ESXi 8.0, 7.0 and ESXi 6.5 ◦ KVM over Ubuntu 20.04 • Containers: ◦ Kubernetes (on-prem) with Flannel and Calico ◦ Amazon Web Services (AWS) – EKS ◦ Microsoft Azure - AKS • Supported architectures: ◦ x86 and ARM • Bare metal via Debian installer packages over stock Ubuntu 24.04/22.04
Deployment options for controller	• Public Clouds: ◦ Amazon Web Services (AWS) - Marketplace ◦ Microsoft Azure - Marketplace ◦ Google Cloud Platform (GCP)

Key Specifications	Options
	• VMware ESXi 8,0. 7.0 and ESXi 6.5 • KVM over Ubuntu 20.04 • IPv4 or IPv6 management
Secure Remote Access client emulation (ZTNA, SSL VPN)	• Zero Trust Network Access PEPs (Policy Enforcement Points): ◦ Palo Alto, Global Protect Clientless (GP) / Explicit Proxy (EP) ◦ F5 BIG-IP (Identity Aware Proxy) ◦ Cisco Umbrella / Firepower • Zero Trust Network Access IdP (Identity Providers): ◦ Okta (SAML) ◦ Internal Simulated IdP (SAML) • Client VPN emulation: ◦ Cisco AnyConnect SSL VPN ◦ Palo Alto GlobalProtect, Prisma Access Agent (PAA) ◦ F5 BigIP SSL VPN ◦ Fortinet SSL VPN
IPsec support	• IKEv2 • Site-to-Site and Remote Access • Pre-shared key authentication • Initiator mode (both Client and Server side) • Tunnel mode with ESP • NAT-Traversal • Multiple Phase2 over Phase1 • Dynamic tunnel creation and tear down • Initial contact payload • Rekey support and Dead Peer Detection • Perfect Forward Secrecy (PFS) • Lifetime negotiation and re-keying • NSA Suite B Cryptography
AI API Intercept (Runtime Security)	• Legitimate and adversarial LLM traffic support to test AI runtime security solutions • 1-arm emulation for testing AI API Intercept solutions: ◦ Palo Alto Prisma AIRS ◦ Google Model Armor
Test topologies support	• Geographically distributed location – Send application and security traffic between test agents deployed in multiple physical locations • Hybrid – Send application and security traffic between test agents distributed across on-prem locations and public cloud • Multiple cloud – Send application and security traffic between test agents deployed in different public clouds • Deploy agents in dynamically scaling auto-scale groups
Objective types support	• Throughput • Connections per second • Prompts per second • Simulated users

Key Specifications	Options
	• Concurrent Connections • Multiple objective support - Ability to set dual objectives (i.e., throughput and simulated user set at the same time) • Attacks per second • Max Concurrent attacks
Network	• Emulated Router support • IPv4 and IPv6 support • VLAN support • Configurable MAC addresses • Static ARP
Application type support	• Web-based enterprise apps including Office365 (Outlook, OneDrive, Excel), AWS S3, Google Drive, and many others • Datacenter: SMTP, DNS, FTP MongoDB, ADP, MSSQL, PostgreSQL, SMBv2, NFS, UDP • AI LLM traffic: OpenAI API, ChatGPT, Grok, Gemini, Anthropic Claude, Github Copilot, MCP and many others • IoT: MQTT, Modbus, S7comm, Profinet • Social Media: Facebook, Reddit, Google Hangouts, Skype, Tubi, YYLive, Hulu • Gaming/Entertainment: League of Legends, Dreambox, NetEase Music, Airbnb, Baidu • Realistic media emulation (i.e., MS Teams, Zoom, Whatsapp VoIP) with voice and video support, including quality of experience metrics such as Mean Opinion Score (MOS)
Encryption support	**TLS 1.3 with major ciphers and key sizes supported:** • AES128-GCM-SHA256 • AES256-GCM-SHA384 • CHACHA20-POLY1305-SHA256 **TLS 1.3 key agreement groups:** • Standard key agreement groups: P-256, P-384, P-521 • Pure PQC algorithms: ML-KEM • Hybrid PQC algorithms: x25519_MLKEM768, P384_MLKEM1024, etc **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

Key Specifications	Options
Attack type support	Over 10000 unique attacks and thousands of attack variants for SQLi, XSS and Brute force. Attack's coverage includes the following: • Generic Injection attacks • AI LLM prompt 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 performance indicators	• Total number of active client and server agents in a test • Throughput • Connection per second • Simulated users • Total count of attacks allowed / blocked • Total application iterations success / failed • Average latencies: connect time, time to first byte (TTFB), time to last byte (TTLB)
Statistics	• Zero Trust statistics • Attacks sent / allowed / blocked • Per network segment applications / attacks metrics • Average Packet Size • TCP level statistics • TLS handshake / throughput • Per application action statistics • Per playlist-entry statistics • Per agent traffic statistics • Per agent CPU and Memory utilization
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 — Software Only

Part Number	Description
938-1040	CyPerf Bundle with 1 license x 10 Gbps and 10 Agents (1-year subscription, floating worldwide). TAA Compliant (938-1040). 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 deployable on the customer's environment • Single performance unit count of up to 10 Gbps of throughput performance, 100K connections per second, 1M concurrent connections, 500 prompts per second, 1M simulated users, 14M attack frames/sec, and 1K concurrent attacks • Access to ATI, software updates, and customer support for the purchased term of the subscription REQUIRES: License term to be specified (MUST be purchased in multiples of years). List price is per unit, per year. TAA Compliant.
938-1050	CyPerf Bundle with 1 license x 100 Gbps and 10 Agents (1-year subscription, floating worldwide). TAA Compliant (938-1050). 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 deployable on the customer's environment • Single performance unit count of up to 100 Gbps of throughput performance, 1M connections per second, 10M concurrent connections, 5K prompts per second 10M simulated users, 140M attack frames/sec, and 10K concurrent attacks • Access to ATI, software updates, and customer support for the purchased term of the subscription REQUIRES: License term to be specified (MUST be purchased in multiples of years). List price is per unit, per year. TAA Compliant.
938-1060	CyPerf Bundle with 1 license x 400 Gbps and 40 Agents (1-year subscription, floating worldwide). TAA Compliant (938-1060). All-inclusive Distributed Application Performance and Security Testing Bundle. The bundle includes: • Access to the CyPerf cloud-native software application • Up to 40 CyPerf test agents deployable on the customer's environment • Single performance unit count of up to 400 Gbps of throughput performance, 4M connections per second, 40M concurrent connections, 20K prompts per second 40M simulated users, 560M attack frames/sec, and 40K concurrent attacks • Access to ATI, software updates, and customer support for the purchased term of the subscription REQUIRES: License term to be specified (MUST be purchased in multiples of years). List price is per unit, per year. TAA Compliant.
938-1010	CyPerf Bundle with 10 licenses x 1 Gbps and 10 Agents (1-year subscription, floating worldwide). TAA Compliant (938-1010). 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 deployable on the customer's environment • 10 x performance license units, each unit includes up to 1 Gbps of throughput performance, 10K connections per second, 100K concurrent connections, 50 prompts per second, 100K simulated users, 1.4M attack frames/sec, and 100 concurrent attacks • Access to ATI, software updates, and customer support for the purchased term of the subscription REQUIRES: License term to be specified (MUST be purchased in multiples of years). List price is per unit, per year. TAA Compliant.
938-1011	CyPerf Bundle with 2 licenses x 1 Gbps and 4 Agents (1-year subscription, floating worldwide). TAA Compliant (938-1011). All-inclusive Distributed Application Performance and Security Testing Bundle. The bundle includes:

Part Number	Description
	• Access to the CyPerf cloud-native software application • Up to 4 CyPerf test agents deployable on the customer's environment • 2 x performance license units, each unit includes up to 1 Gbps of throughput performance, 10K connections per second, 100K concurrent connections, 50 prompts per second, 100K simulated users, 1.4M attack frames/sec, and 100 concurrent attacks • Access to ATI, software updates, and customer support for the purchased term of the subscription REQUIRES: License term to be specified (MUST be purchased in multiples of years). List price is per unit, per year. TAA Compliant.
938-1001	CyPerf Add-on with single agent license (1-year subscription, floating worldwide). TAA Compliant (938-1001). Requires a previous purchase of any CyPerf Bundle license. This add-on includes 1 x CyPerf test agent deployable on the customer's environment. REQUIRES: License term to be specified (MUST be purchased in multiples of years). List price is per unit, per year. TAA Compliant.
938-1002	CyPerf Add-on with 10 licenses x 1 Gbps (1-year subscription, floating worldwide). TAA Compliant (938-1002). Requires a previous purchase of any CyPerf Bundle license. This add-on includes 10 x performance license units, each unit includes up to 1 Gbps of throughput performance, 10K connections per second, 100K concurrent connections, 50 prompts per second, 100K simulated users, 1.4M attack frames/sec, and 100 concurrent attacks. REQUIRES: License term to be specified (MUST be purchased in multiples of years). List price is per unit, per year. TAA Compliant.
938-1030	CyPerf Bundle with 10 licenses x 1 Gbps and 10 Agents (30-day subscription, floating worldwide). TAA Compliant (938-1030). 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 deployable on the customer's environment • 10 x performance license units, each unit includes up to 1 Gbps of throughput performance, 10K connections per second, 100K concurrent connections, 50 prompts per second, 100K simulated users, 1.4M attack frames/sec, and 100 concurrent attacks • Access to ATI, software updates, and customer support for the purchased term of the subscription.
938-1101	CyPerf Bundle with 2 licenses x 1 Gbps and 4 Agents (30-day subscription, floating worldwide). TAA Compliant (938-1101). All-inclusive Distributed Application Performance and Security Testing Bundle. The bundle includes: • Access to the CyPerf cloud-native software application • Up to 4 CyPerf test agents deployable on the customer's environment • 2 x performance license units, each unit includes up to 1 Gbps of throughput performance, 10K connections per second, 100K concurrent connections, 50 prompts per second, 100K simulated users, 1.4M attack frames/sec, and 100 concurrent attacks Access to ATI, software updates, and customer support for the purchased term of the subscription.
938-1003	CyPerf Add-on with single agent license (30-day subscription, floating worldwide). TAA Compliant (938-1003). Requires a previous purchase of any CyPerf Bundle license. This add-on includes 1 x CyPerf test agent deployable on the customer's environment. TAA Compliant.
938-1004	CyPerf Add-on with 10 licenses x 1 Gbps (30-day subscription, floating worldwide). TAA Compliant (938-1004). Requires a previous purchase of any CyPerf Bundle license. This add-on includes 10 x performance license units, each unit includes up to 1 Gbps of throughput performance, 10K connections per second, 100K concurrent connections, 50 prompts per second, 100K simulated users, 1.4M attack frames/sec, and 100 concurrent attacks. TAA Compliant.

Product Ordering Information — Hardware

Part Number	Description
941-0110	**APS-ONE-100 Fusion Compute Node with 4x100GE**. Compatible for use in stand-alone mode (BreakingPoint only), with APS-M1010 Management Controller (941-0113), or with APS-M8400, 8-port 400GE QSFP-DD appliance (941-0111). If running in stand-alone mode or with APS-M1010 Management Controller, requires at least 2 x QSFP28 transceivers/cable assemblies to be ordered separately using QSFP28-SR4-XCVR (QSFP28 100GBASE-SR4 100GE pluggable optical transceiver, MMF (multimode), 850 nm, 100 m reach) or 2 x QSFP28 direct attach cable to be ordered separately using 942-0088 (QSFP28 passive, copper, Direct Attach Cable). Note: each APS-ONE-100 Fusion Compute Node supports fan-out from 2 x 100GE to 8 x 25GE or 8 x 10GE using 2 x MT-to-4x10GE LC fan-out, MMF, 3-meter cable for 10GE and 25GE fan-out to be ordered separately (942-0067). Requires ONE of the following options (sold separately at the time of purchase): (1) BreakingPoint Application & Threat Intelligence (ATI) (909-0856); (2) CyPerf perpetual software license for a single APS-ONE-100 appliance, floating license (per controller) TAA Compliant (938-2001); (3) CyPerf and BreakingPoint software license bundle for a single APS-ONE-100 appliance. TAA Compliant (938-2003)
941-0116	**APS-M1010 Management Controller. Supports BreakingPoint, CyPerf and IxLoad applications. This management controller can manage up to 10 x APS-ONE-100 Compute Nodes (941-0110 or 941-0114). Note: APS-ONE-100 compute nodes are purchased separately.**
938-2001	**CyPerf perpetual software license for a single APS-ONE-100 appliance, floating license (per controller).** TAA Compliant. (938-2001) The license enables all-inclusive CyPerf functionality on a single APS-ONE-100 appliance (compute node), at 18% of purchase price of hardware. It can be used with any single appliance managed by a management controller (APS-M1010). Access to ATI, CyPerf software updates, and customer support after the purchased term can be renewed using (909-6001) part. TAA compliance is determined by the hardware on which the license is enabled.
938-2003	**CyPerf and BreakingPoint software license bundle**. TAA Compliant. (938-2003) The license enables: - CyPerf, all-inclusive license for a single APS-ONE-100 appliance and, - BreakingPoint Application & Threat Intelligence all-inclusive license for a single APS-ONE-100 appliance Bundle price calculated as 24% of purchase price of hardware. Must renew both BreakingPoint and CyPerf together at 24% of purchase price of hardware, otherwise each component (CyPerf or BreakingPoint) can be separately renewed at 18% of purchase price of hardware. TAA compliance is determined by the hardware on which the license is enabled
938-2002	**CyPerf perpetual software license add-on for a single APS-ONE-100 appliance with an active BreakingPoint - Application & Threat Intelligence subscription (floating license per controller).** TAA Compliant. (938-2002). The license enables all-inclusive CyPerf functionality on a single APS-ONE-100 appliance (compute node), at 9% of purchase price of hardware. It must be used only on an APS-ONE-100 appliance with an active BreakingPoint - Application & Threat Intelligence subscription. Must renew both BreakingPoint and CyPerf together at 24% of purchase price of hardware, otherwise each component (CyPerf or BreakingPoint) can be separately renewed at 18% of purchase price of hardware. TAA compliance is determined by the hardware on which the license is enabled.
983-2402	**Field HW Upgrade for APS-ONE-100 (941-0114) to add CyPerf Software Perpetual License**, TAA Compliant (983-2402). Enables fusion mode to support IxLoad and CyPerf software on any APS-ONE-100 non-fusion appliance. The upgrade option increases the hardware value of the original base hardware. -- Requires CyPerf software license for a single APS-ONE-100 appliance (938-2001), sold separately, at time of purchase, calculated as 18% of the end-user price of the upgraded system (base system + upgrade option). -- The upgrade option is covered by the hardware warranty of the original base hardware until the original contract lapses. -- Renewal of warranty and CyPerf software license to be calculated based on end-user price of the upgraded system (base system + upgrade option).

Part Number	Description
983-2403	**Field HW Upgrade Bundle for APS-ONE-100 (941-0114) to add BreakingPoint and CyPerf Perpetual Software Licenses**, TAA Compliant (983-2403). Enables fusion mode to support IxLoad, BreakingPoint and CyPerf software on any APS-ONE-100 non-fusion appliance. The upgrade option increases the hardware value of the original base hardware. Bundle requires: -- BreakingPoint Perpetual Software License for APS-ONE-100 Appliance, TAA Compliant (983-2404). Enables BreakingPoint functionality on any APS-ONE-100 non-fusion appliance (compute node) at 12% of the end-user price of the upgraded system (base system + upgrade option). NOTE: 983-2404 is a component of bundle 983-2403 and is NOT quotable individually. -- CyPerf Perpetual Software License for APS-ONE-100 Appliance, TAA Compliant (938-2401). Enables all-inclusive CyPerf functionality on a single APS-ONE-100 appliance (compute node) at 12% of the end-user price of the upgraded system (base system + upgrade option). NOTE: 938-2401 is a component of bundle 983-2403 and is NOT quotable individually. -- NOTE: Combined BreakingPoint ATI and CyPerf price is calculated as 24% of the end-user price of the upgraded system: (base system + upgrade option). Must renew both BreakingPoint ATI and CyPerf together at 24% of the end-user price of the upgraded system, otherwise each individual component (BreakingPoint or CyPerf) can be renewed separately at 18% of the end-user price of the upgraded system: -- NOTE: The upgrade option is covered by the hardware warranty of the original base hardware until the original contract lapses. -- NOTE: Renewal of warranty, ATI, and CyPerf software license to be calculated based on end-user price of the upgraded system (base system + upgrade option).

To explore CyPerf or to take a free test drive, visit:

www.keysight.com/us/en/products/network-test/cloud-test/cyperf.html