Brochure

# VIAVI
## TeraVM
Security Assertion Markup Language (SAML).
Performance validation at scale

TeraVM™ supports validation for single-sign on (SSO) applications using Security Assertion Markup Language (SAML), enabling users to measure the capacity of the Identify/Service Provider by emulating millions of unique Web Browser sessions. TeraVM's stateful per-flow architecture enables users of TeraVM to validate SAML performance with unique client credentials (including the use of digital certificates), with each and every emulated client having unique SAML assertions.

TeraVM supports validation of both SAML authentication flow options:

- IdP initiated (Authenticate with IdP and follow redirect to SP service)

- SP initiated (Attempt connection to SP, follow redirect to IdP, authenticate and return to SP)

### Validating SAML 2.0 authentication flows at scale

TeraVM is a stateful traffic emulator which enables users validate SAML SSO in a number of unique ways, this includes concurrent validation of both IdP and SP initiated authentication. TeraVM's per flow architecture further enhances the validation methodology by enabling unique SAML assertions per emulated client.
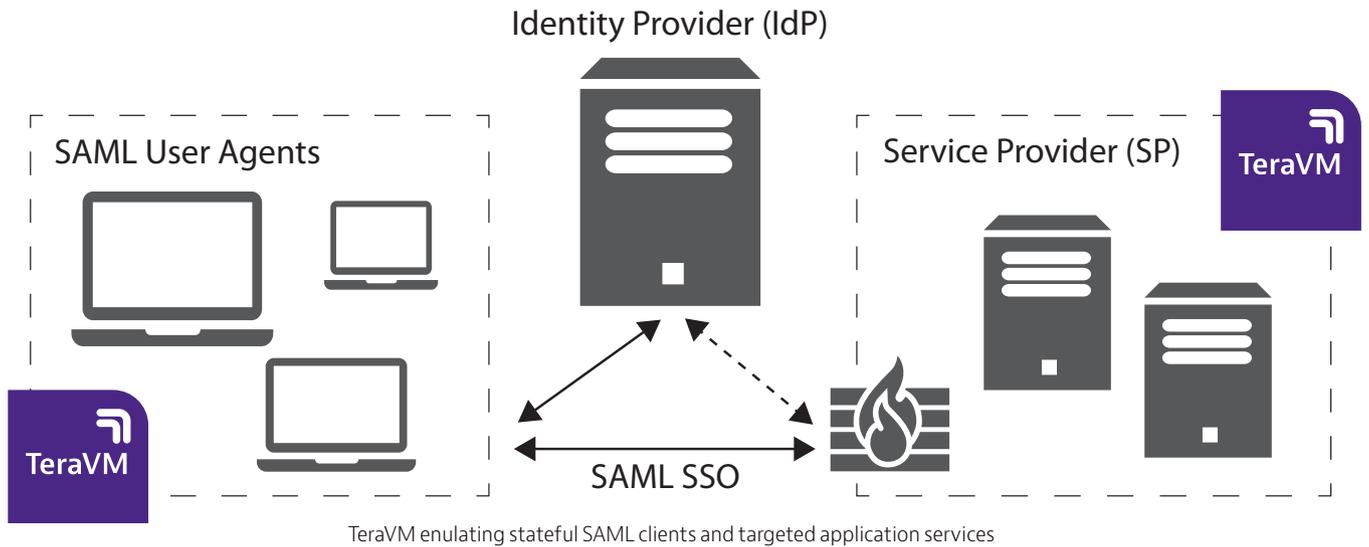
The flexible configuration options means users of TeraVM can assess the reliability of SAML with poorly configured assertions. Furthermore, the per-flow capability enables users to validate performance for more complex SAML scenarios such as realm discovery, using either unique user names, domain names, and/or url associations.

### Advantages

- Emulate millions of SAML sessions

- Unique credentials per client, supports the use of digital certificates

- Supports both IdP and SP authentication flow initiation

### Features

- Support of proprietary 3rd party authentication flows

- Cloud platform enabled, support for AWS, Azure, and OpenStack

- Out of millions of SAML sessions, easily pinpoint and isolate failed

- SAML sessions

Identity Provider (IdP)

SAML User Agents

Service Provider (SP)

TeraVM

TeraVM

SAML SSO

TeraVM enulating stateful SAML clients and targeted application services

## Introducing TeraVM

TeraVM is an application-emulation and security-performance solution, delivering comprehensive test coverage for application services, wired, and wireless networks.

TeraVM is offered as a virtualized solution enabling the flexibility to run anywhere - lab, datacenter, and the cloud, with consistent performance coverage, ensuring that highly optimized networks and services can be delivered with minimal risk.

### SAML emulation with the most realistic load scenarios

Using TeraVM SAML, users can emulate the most realistic load scenarios for performance validation of throughput, connections, and latency for single sign-on services. TeraVM supports 3rd party SAML flows which includes Citrix and F5.

TeraVM emulates stateful SAML request and responses used for validation of authentication flows originating at either the IdP or SP and/or the targeted application service. After successful authentication, TeraVM's per-flow architecture can be used to validate performance

of the targeted service and can be used to validate robustness of SAML by attempting to connect to additional application services, using the assigned SAML security tokens.

TeraVM can be deployed to cloud services such as Amazon Web Services (AWS), Azure, and/or OpenStack; allowing the user validate access privileges, performance of throughput, and latency of core IdP and SP services, alongside the targeted SP application service in the cloud.

## TeraVM SAML use cases

### Realm Discovery

Validate performance using unique client credentials (username) and/or url requests originating at the emulated client.

### SAML Assertions

Validate key SAML assertions such as lifetime of SAML tokens, validate new IdP profiles and/or malformed or with incomplete assertion values

| TeraVM Capability Overview | |
|---|---|
| **General** | Real-time isolation of problem flows |
| | Elastic test bed (up to 1Tbps) |
| **Network interface support** | Support for 1/10/40Gbps I/0 |
| | Mellanox ConnectX-4 support for 56/100Gbps |

## TeraVM Capability Overview

| | |
|---|---|
| **Data** | TCP / UDP, Teraflow, Ookla speed test |
| | HTTP (v1/2, incls. stateful response parser) |
| | SMTP / POP3 (incl. file attachments) |
| | FTP (Passive/Active), P2P applications, DNS |
| **Address assignment** | Configurable MAC |
| | DHCP, PPPoE (IPv4 & IPv6) |
| | Dual Stack (6RD, DS Lite) |
| **Ethernet switch** | VLAN tagging (up to 8 concurrent tags) |
| | ACL, 802.1p, DSCP |
| **Data center** | VxLAN, GRE, SR-IOV |
| **Replay** | Replay large PCAP files TCP, UDP and raw data playback |
| | Amplify and dynamically substitute data into PCAP files |
| **Video** | Multicast: IGMP v1/v2/v3 & MLD v1/v2 |
| | Automatic Multicast Tunneling (AMT) |
| | Video on Demand (VoD) |
| | Adaptive Bit Rate Video (HLS, HDS, MPEG-DASH, smooth) |
| | Video conferencing, Webex |
| **Secure access / VPN** | Clientless VPN (SSL/TLS/DTLS), IPSec (IKEv1/v2), generic remote access |
| | Cisco AnyConnect SSL VPN Client, Cisco AnyConnect IPsec VPN |
| | Cisco ScanSafe |
| | Juniper Pulse, Juniper Network Connect |
| | SAML (F5, Citrix SSO), Dell SSO |
| | 802.1x EAP-MD5 |
| **Securiy attack mitigation** | spam / viruses / DDoS |
| | Cybersecurity Database |
| **Voice** | VoIP: SIP & RTP (secure & unsecure), SMS |
| | Dual-hosted UACs, SIP Trunking |
| | Voice & video quality metric (MOS) |
| **LTE/4G** | EPC and RAN (Rel.8, 10, 11) |
| | VoLTE (secure/unsecure), ViLTE |
| | Wifi Offload (EoGRE) |
| **SLA** | TWAMP, PING |
| **Automation** | CLI, Perl, TCL, XML, Java API |
| | Python, Jython |
| | Qualisystems (CloudShell) |
| | OpenStack |

**viavisolutions.com/wirelessvalidation**