TeraVM Portable Security

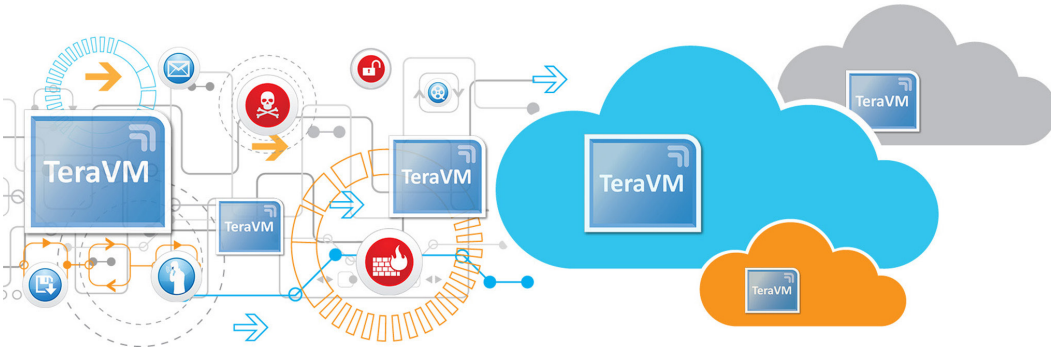
Virtualized Application and Security Testing

The most important thing we build is trust

Benefits

- Ensure the accuracy and validity of network device evaluations and security testing
- Continuous security intelligence with real-world applications and relevant threats
- Comprehensive library of 11,000+ CVE validated threat signatures, with frequent updates
- Realize savings from the only elastic test bed without compromising security
- Maximize security by sharing virtual test assets to run anywhere, anytime

Security threats constantly evolve with new vulnerabilities discovered weekly. Attackers continue to develop new methods and attacks to find undiscovered holes in the most advanced network defenses. Application performance testing and security validation must reflect the latest and most relevant security threats to ensure network security devices will perform and protect the network infrastructure from the most advanced and malicious attacks. TeraVM provides scalable real-world application and threat emulation which leverages veritable internet threats from popular Common Vulnerability and Exposures (CVE) repositories. Frequent updates available ensure users assess their security posture in the landscape of ongoing changes for applications, attacks and standards to stay protected.



Security Hardening

By emulating the latest security threat and exploit profiles, users of TeraVM can assess security vulnerabilities in a safe and contained manner. TeraVM enables users to quickly pinpoint where the weaknesses are in their security counter measures ensuring the appliance or application is patched for any vulnerability.

Actionable Insight

TeraVM provides a suite of applications and security threats through a comprehensive cyber security threat database. Together they provide unique, actionable insight into threat activity, its relevance, and how to achieve a desired balance between security cost and business risk.

Performance under Duress

Determine with precision the effectiveness of security counter measures against scaled and targeted attacks. Assess what the impact is on network operations. Using TeraVM, emulate distributed denial of service attacks with known exploits.

Portability

TeraVM's application emulation and cybersecurity solution is deployed on any industry standard hardware with any major hypervisor (e.g. VMware ESXI, Hyper-V, and KVM). With TeraVM you are no longer locked in to proprietary hardware that seems to be obsolete almost the minute you receive it.

Mobility

TeraVM cybersecurity solution is packaged as a virtual appliance on standard hardware and only requires a software license to operate. For geographically dispersed testing and security validation moving a test bed across the world is as simple as checking out a license from a centrally deployed license server.

Cybersecurity Database

TeraVM Cybersecurity Database provides a comprehensive resource and service for proactively protecting and hardening the most advance networks. The TeraVM Cybersecurity Database is frequently updated as new threats are discovered and validated.

TeraVM Cybersecurity Database

See below example of recent threat updates. For a complete list of all threats, contact us.

Vulnerability	Description
Out-of bounds Vulnerability	A successful remote denial of service attack against Google Chrome before 47.0.2526.73.
Microsoft Windows Library Loading Vulnerability	A successful remote code execution attack against Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1.
Microsoft Windows Remote Code Execution Vulnerability	A successful remote code execution attack against Windows Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8, and Windows 8.1.
HTTP WordPress Plugin Vulnerability	WordPress Plugin WP Easy Poll 1.1.3 is vulnerable to a CSRF attack.
HTTP Alcatel Lucent Home Device Manager Vulnerability	Alcatel-Lucent Home Device Manager is prone to multiple cross-site scripting vulnerabilities.
HTTP D-Link DIR-645 Buffer Overflow Vulnerability	D-Link DGL5500 is vulnerable to a buffer overflow, caused by improper bounds checking by UPNP.
HTTP AlegroCart 1.2.8 SQL Injection Vulnerability	Alegrocart is vulnerable to multiple SQL injection. A remote attacker could view, add, modify or delete information in the back-end database.

About 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. www.cobhamwireless.com

TERAVM FEATURES AND FUNCTIONALITY

GENERAL
Real-time isolation of problem flows
Elastic Test Bed (up to 11Tbps)

NETWORK INTERFACE SUPPORT
Support for 1/10/40Gbps I/0
Mellanox Connect X-4 support for 56/100Bbps

DATA
TCP / UDP, Teraflow, Ookla speed test
HTTP (headers, substitution, attachments)
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 and Double VLAN Tagging (Q-Q)
ACL, 802.1p, DSCP

DATA CENTER
VxLAN, 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 Tunelling (AMT)
Video on Demand (VoD)
Adaptive Bit Rate Video (HLS, HDS, Smooth)
Video conferencing

SECURE 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
Dell SSO, Fortinet Fortigate and F5
802.1x EAP-MD5

SECURITY ATTACK MITIGATION
Spam / Viruses / DDoS
Cybersecurity threat library

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

SLA
TWAMP, PING

AUTOMATION
CLI, Perl, TCL, XML, Java API
Python, Jython
Qualisystems (CloudShell)
OpenStack

Connected – Seamless – Wireless