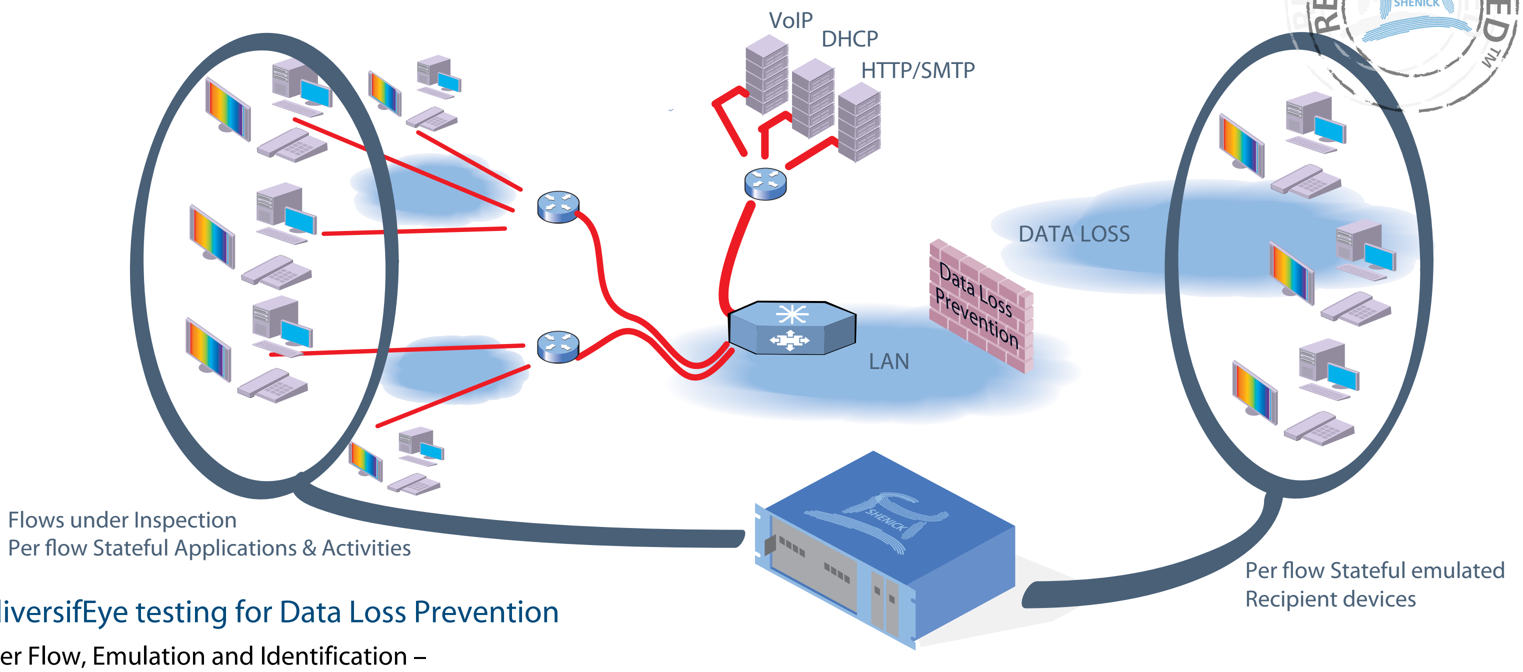
SHENICK

Test Data Loss Prevention systems with diversifEye™

Data Loss is an every day threat within all organizations. The leaking of confidential data ultimately results in a loss of revenue. A quarter of all Data Loss is widely attributed to the use of applications such as Voice, Email, Instant Messaging, Social Networks, Blogs, P2P and Videos.

A common approach adopted to preventing Data Loss is to use sophisticated data detection algorithms and the deployment of systems to control applications attempting to access the outside world.Data Loss is an every day threat within all organizations. The leaking of confidential data ultimately results in a loss of revenue. A quarter of all Data Loss is widely attributed to the use of applications such as Voice, Email, Instant Messaging, Social Networks, Blogs, P2P and Videos.

REALITY CHECKED™ SHENICK



diversifEye testing for Data Loss Prevention

Per Flow, Emulation and Identification –
Emulate thousands of real users running multiple applications. Within the vast array of users and applications, configure a single user to send out 'confidential' information periodically.

Real World Traffic Flows –
More than just traffic simulation or packet stuffing, emulate large volumes of real or stateful traffic flows, such as POP/SMTP, HTTP, VoIP, Telepresence, VoD, P2P, IM, etc.

Configurable Unique Properties –
Configure individual MAC address, IP address, VLAN Tags, ToS/DiffServ right through to Port assignments. Utilize a mix of IPv4, IPv6 and Dual-Stack Lite sessions concurrently.

Fully Customizable Content –
Customize content for Email, HTTP and FTP. Send customizable emails with content attachments such as docs, pdf, zip files, etc. Generate email with confidential information such as social security numbers.

diversifEye is utilized to test and verify Data Loss Prevention (DLP) systems and algorithms through emulating thousands of "good" users with real or stateful TCP and UDP based applications and a small number of "bad" users. diversifEye's Per Flow metrics can rapidly determine if the "bad" users activities are properly identified and blocked.

diversifEye™

diversifEye™ is the only integrated network, application and security attack emulation and performance analysis IP test system providing granularity on a per flow basis.

diversifEye's per flow architecture provides unrivaled control on a per flow basis. diversifEye's control extends through to traffic profiling through a mix of randomness and dynamic capabilities to add or remove individual flows during live tests.

The Shenick diversifEye platform & GUI supports per flow test and measurement of :

Analysis Software Overview

- DHCP v4 & DHCP v6
- PPPoE
- VLAN & Double Tagging (Q-in-Q) with priority
- Concurrent IPv4, IPv6 and Dual-Stack Lite flows
- IGMP v1, v2, v3 - MLD v1, v2
- Voice and Video Quality Metrics
- Telepresence
- RTSP (Video on Demand)
- SSL
- VoIP (SIP & RTP)
- HTTP
- FTP
- SMTP
- POP3
- P2P
- TWAMP
- Attack Traffic - Spam / Viruses / DDOS
- PCAP file replay (>1Gb)

Data Loss Prevention testing Efficacy vs Effectiveness

Efficacy

- Data Loss

  Per-flow granularity is key when trying to capture outbound traffic. Therefore the more diverse the flows and applications the more difficult it is for a DLP system to respond.

- Multiple Protocol Flows

  Emulate multiple IP flows for unique users and applications, determine if "bad" user flows and signatures are identified and blocked correctly.

Effectiveness

- Quality of Experience

  Ensure in real-time, on a per flow basis that DLP system has no impact on revenue generating or delay sensitive applications, especially under varying algorithm settings.

- Security Attack Mitigation

  It is equally important to measure performance under extreme conditions. The DLP must identify and block unwanted traffic such as spam or even ddos attacks, while maintaining operation. Emulate a mix of legal and illegal traffic flows on both sides of the device.

Key Features and Benefits

- Network QoS and per flow QoE granularity for individual emulated client users across multiple devices and application traffic flow types.
- Latest protocols supported from Data Applications (HTTP, FTP, POP/SMTP, P2P), IPTV (IGMP/MLD), VoD (RTSP), VoIP (SIP/RTP), Telepresence all in a single test package.
- TCP Replay Substitution, automatically varies payloads so no two PCAP sessions are the same.
- Support for SSL, TWAMP, IPv4, IPv6 and Dual-Stack Lite.
- DHCP emulation, PPPoE and IPoE Service Interoperability Scenarios. Emulate per device MAC and IP address assignments.
- Security Attack Mitigation support for DDoS style attacks SYN/RST/UDP/ARP floods, reflective DDoS attacks, Ping of death, etc.
- Large memory space (>1Gb) for PCAP replay for Instant Messaging or Web Mail.
- Client and server support on a single blade within one chassis with complete flexibility on port allocation. Full support for multiple daisy chained chassis all controlled from a single GUI.
- Low cost of ownership and ease of use by avoiding multiple test systems and non integrated software applications.

North America | 533 Airport Boulevard, Burlingame, CA 94010, USA Tel: +1-650-288 0511 Fax: +1-650-745 2641
Europe | Brook House, Corrig Avenue, Dun Laoghaire, Dublin, Ireland Tel: +353-1-236 7002 Fax: +353-1-236 7020

web: www.shenick.com email: info@shenick.com