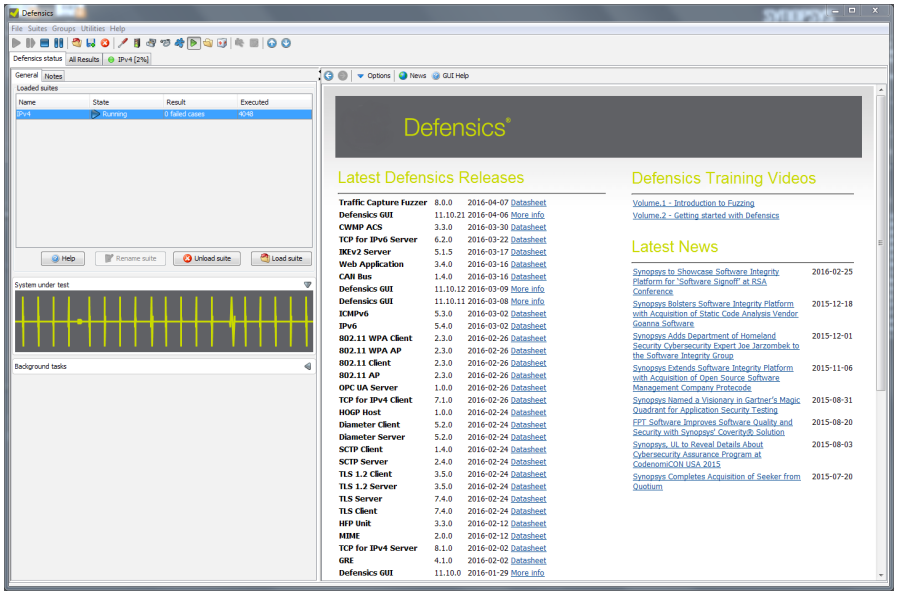
Defensics® is a powerful testing platform that enables developers and asset owners to proactively discover and remediate unknown vulnerabilities in software and devices.



Product Overview

Managing Unknown Vulnerabilities: An Infinite Space Problem

As technology continues to evolve and permeate the infrastructures that people and businesses rely on, mitigating unknown vulnerabilities in the software and devices that power our connected world is paramount.

The Attack Surface is Expanding: Every networked application and device represents an opportunity for attack. Today, there are nearly 13 billion connected devices, and by 2020 that number will rise to 25 billion.

The Stakes are Higher: Today, organizations depend on technology to process sensitive information and perform essential functions. Unknown vulnerabilities in business-critical software and devices pose a significant threat because they cannot be addressed by traditional forms of security such as firewalls, IDP/IPS, etc.

Power Lies in Prevention: The cost of addressing vulnerabilities increases exponentially as you move further down the development lifecycle and supply chain. Proactively discovering and remediating unknown vulnerabilities prevents attacks and reduces costs.

KEY FEATURES

- **Out-of-the-box functionality:** Pre-built test suites relieve the responsibility and burden of manual test creation and maintenance.
- **Ease of use:** Intuitive user interface makes advanced testing and remediation easy for anyone.
- **Clear paths to remediation:** Remediation packages provide detailed documentation and workflows, outlining clear paths to remediation for your development team or supplier.

Supported Protocols

(Not All Protocols Listed)

(MEF-16)	H.248	NFS v4.0 / v4.1	SNMPv3
BACNET	H.264	NHRP	SOCKS
BFD	H.264 RTP	NTP	SSH1
BFD	H.323	OAM (802.3ah)	SSH2
BGP4+	HTTP	OCSP	STP
BICC/M3UA	IEC 60870-5-104	openFlow	STUN
Blueooth LE	IEC 61850/Goose/SV	OSPFv2	SunRPC
Bluetooth	IEC 61850/MMS	OSPFv3	SyncEthernet
CAN Bus	IEE1588 PTP	PBB-TE	Syslog
CFM	IKEv2	PBT (802.1ah)	Telnet
CIFS/SMB	IMAP4	PCP	TFTP
CIP	IPMI	PIM-SM/DM	TLS 1.2
CMP v2	IPSec	PMIPv6	TLS/SSL 1.0/1.1, SSL3
COAP	IPv4	POP3	Traffic Capture Fuzzer
CWMP (TR-69)	IPv6	PPPoE	Trill
DHCP/BootP	IS-IS	Profinet DCP (PLC)	TURN
DHCPv6	ISAKMP/IKEv1	Profinet PTCP (PLC)	Universal ASN.1 BER
Diameter	ISASecure Solution	RADIUS	Universal Fuzzer
DICOM	iSCSI	RIP	UPnP
DNP3	JSON format	RIPng	vCalendar format
DNS	Kerberos	RSVP	vCard format
DTLS	L2TPv2/v3	RTP/RTCP/SRTP	VRRP
DVMRPv1	LACP (802.3ad)	RTSP	WebApplication
DVMRPv3	LDAPv3	S1AP	WebSocket
E-LMI	LDP	SCEP	Wi-Fi AP
EAPoL/802.1x	LLDP (802.1AB)	SCTP	Wi-Fi AP WPA
ESTP	MAP	SIP	Wi-Fi Client
Ethernet	MIME	SIP-I	Wi-Fi Client WPA
FCoE + FIP	ModBus	SMBv2	WMV
FIX	MP4	SMBv3	WPA Enterprise
FTP	MPLS	SMPP SMS	X.509v3
GARP 802.1D	MQTT	SMS PDU/File	XML File
GRE	MSDP	SMS SMPP	XML SOAP
GTPv0	MSRP	SMTP	XMPP
GTPv1	NetBIOS	SNMP Trap	
GTPv2-control	NFS v2/v3	SNMPv2c	

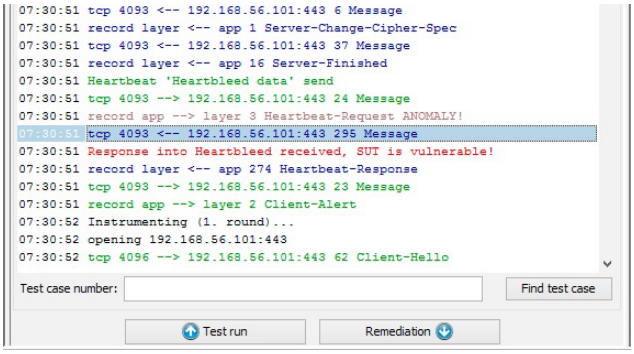
Key Features:

- Fully-automated testing platform with pre-built test suites relieve the responsibility and burden of manual test creation.
- Utilizes various techniques to generate effective test cases, including “template,” “generational,” and “evolutionary” test engines.
- Supports advanced techniques for detecting failures and anomalous behavior, including valid case or functional response, resource monitoring, dynamic binary analysis, and source code instrumentation.
- Advanced test suites available for 290+ network protocols, file formats, and other interfaces. Test suites are continuously added, improved, and supported by a dedicated team of test developers.
- Thorough documentation and reporting features allow Defensics to identify the root cause of critical failures in such a way that they are repeatable, easy to understand, and can be shared with the stakeholders involved in the remediation process.

Bringing the Unknown Into View

With security and transparency emerging as Board-level mandates, there is a renewed urgency to find the vulnerabilities that put business performance at risk. Defensics is a next-generation security-testing platform that enables developers and users of technology to rapidly, reliably, and efficiently find and correct dangerous errors and flaws. By proactively bringing the unknown into total view, Defensics sets the bar for superior vulnerability management.

The technology at the core of Defensics is fuzz testing. This is an automated methodology that tests for unknown vulnerabilities by systematically sending invalid or unexpected inputs to the system under test. Fuzz testing exposes software defects and vulnerabilities more effectively than any other solution in the market.



Defensics was used to identify the OpenSSL Heartbleed vulnerability in April 2014 (Google independently reported the vulnerability at the same time). A security researcher at Codenomicon (now Synopsys) had been running a routine test of the Defensics feature, SafeGuard, when he identified a flaw in OpenSSL. It had gone unidentified for over two years. Ultimately Heartbleed impacted over 500,000 websites.

Test Suite Reference Bundles

Core Internet: IPv4 (TCP, UDP, IPv4, ICMP, IGMP, ARP), IPv6 (TCP, UDP, IPv6, ICMPv6), DNS, DNSSEC, NTP Client, NTP Server, DHCP/ BOOTP Client, DHCP/ BOOTP Server, HTTP Server, HTTP Client, FTP Server, DHCPv6 Client, DHCPv6 Server, FTP Client, NetBIOS, PMIPv6 Client, PMIPv6 Server

Net Management: HTTP Server, HTTP Client, TLS/SSL, TLS 1.2, Telnet Server, SSH1 Server, SSH2 Server, SNMPv1/v2 Server, SNMPv3 Server, TFTP Server, UPnP Server, Syslog, SNMP Trap

Routing: IS-IS, DVMRP, GRE, OSPFv2, OSPFv3, PIM-SM/DM, RSVP, VRRP, BGP4, RIP, RIPng, MPLS/LDP, HSRP, NHRP, CDP, OpenFlow

Remote Access: EAPOL Server, PPPoE, Diameter Server, Diameter Client, LDAPv3 Server, TACACS+ Server, TACACS+ NAS, RADIUS (Server, Client), Kerberos Server

VPN: IPsec, SSH1 Server, SSH2 Server, TLS/SSL, TLS 1.2, ISAKMP/ IKEv1 (Client, Server), IKEv2, OCSP (Client, Server), L2TPv2, X.509

VoIP/IMS: SCTP, H.248, H.323, RTSP (Client, Server), TLS/SSL, TLS 1.2, SIP UAS, SIP UAC, SigComp, RTP/RTCP/SRTP, MGCP, UPnP Server, X.509, BICC, SIP TT

3G/4G LTE: SCTP, GRE, IPsec, Diameter Server, Diameter Client, LDAP Server, TLS/SSL, TLS 1.2, SIP UAS, SIP UAC, GTPv1, GTPv0, RADIUS (Server, Client), GTPv2, SMPP, SMS/SMPP, SMS/PDU, PMIPv6

Digital Media: Audio (AIFF, AU, AMR, IMY, MP3, VOC, WAV), Images (BMP, GIF, JPEG, MBM, PCX, PNG, PIX, PNM, RAS, TIFF, WBMP, XBM, XPM, WMF), Video (AVI, QuickTime, MPEG1, MPEG2, MPEG4, MOV), Archives (ZIP, CAB, JAR, LHA, GZIP), vCalendar, vCard, MPEG2-TS, NFS Media, UPnP

Email: POP3, IMAP4, SMTP, MIME

File Systems / Storage: CIFS/SMB Server, iSCSI Server, SunRPC Server, SMBv2, NFSv2, NFSv3, NFSv4

WiFi: AP Test Suite, AP WPA Test Suite, Client Test Suite, Client WPA Test Suite

Link Management: LACP, STP, MSTP, RSTP, ESTP

Bluetooth: L2CAP, SDP, RFCOMM, OBEX, OPP, FTP, IrMC Synch, BIP, BPP, BNEP, HFP, HSP, DUN, PBAP, FAX, AVRCP, A2DP, HCRP, HID, SAP, MDP

IPTV: MPEG4, MPEG2, IPsec, TLS/SSL, TLS 1.2, RTP/RTCP, RTSP, HTTP, FTP, TFTP, IPv4, IPv6, PIM-SM/DM, RSVP, IGMP, CWMP(TR-69) ACS, CWMP(TR-69) CPE

PDA/Smartphone: IPv4, IPv6, DHCP/BOOTP, HTTP, TLS/SSL, TLS 1.2, UPnP, SIP, Audio, Images, Video, Bluetooth, 802.11, SMS/PDU, SMS/SMPP

Industrial Automation: (SCADA/DCS) Modbus, IPv4 (TCP, UDP, IPv4, ICMP, IGMP, ARP), IPv6 (TCP, UDP, IPv6, ICMPv6), Profinet, DNP3, IEC-61850/MMS, GOOSE-SV, IEC-104, TCF, OPC UA, CoAP, BACnet, CIP/EtherNet/IP

Metro Ethernet: BFD, CFM, E-LMI, Ethernet, GARP, LLDP, OAM, PBT/PBB-TE, L2TP

General Purpose: XML SOAP, Traffic Capture Fuzzer, Universal Fuzzer

Finance: FIX

Web Applications: FIX, JSON, OAuth, SOCKS Client, SOCKS Server, Traffic Capture Fuzzer, Universal Fuzzer, Web Applications Fuzzer, Web Sockets, XML file format, XML SOAP Server, XML SOAP Client

Web: HTTP, XML, Web Applications, Digital Media, Universal Fuzzer

Automotive: Bluetooth, WiFi, Digital Media, SMS, General purpose fuzzers

SYNOPSYS®

www.synopsys.com/software

Synopsys Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: sales@coverity.com