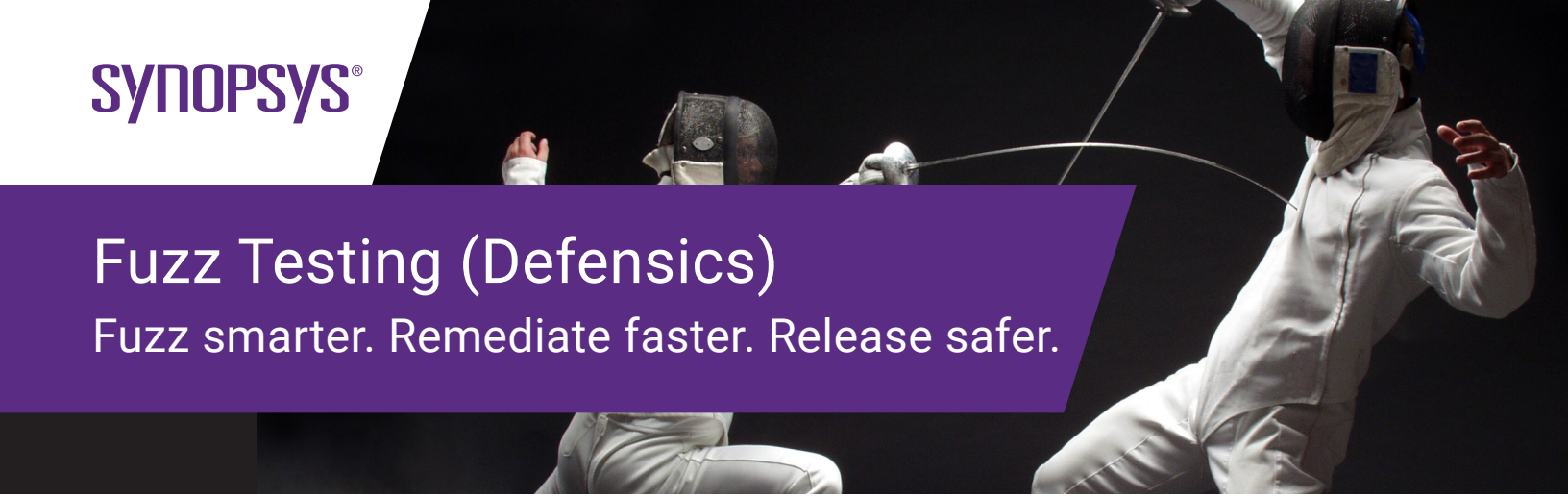
SYNOPSYS®



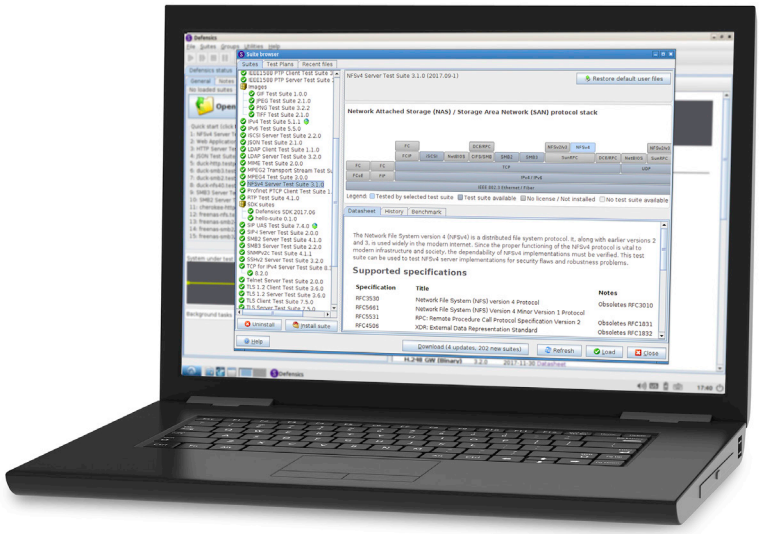
Fuzz Testing (Defensics)

Fuzz smarter. Remediate faster. Release safer.

Improve software robustness, ensure systems interoperability, and identify vulnerabilities, whether you're procuring software for business operations or building it.

Product overview

Synopsys Fuzz Testing (Defensics) is a comprehensive, powerful, and automated black box solution that enables organizations to effectively and efficiently discover and remediate security weaknesses in software. By taking a systematic and intelligent approach to negative testing, Synopsys Fuzz Testing allows organizations to ensure software security without compromising on product innovation, increasing time to market, or inflating operational costs.

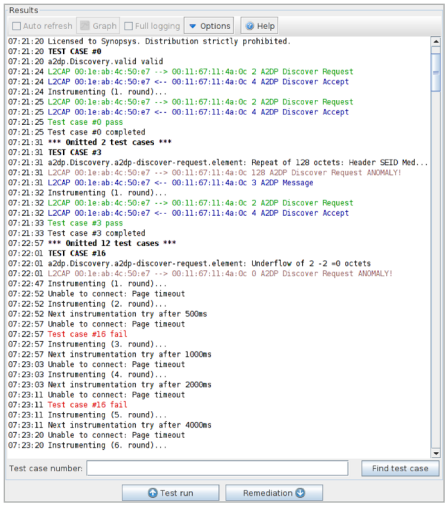


Synopsys Fuzz Testing's logical user interface walks users through each step of the process, making advanced fuzz testing easy.

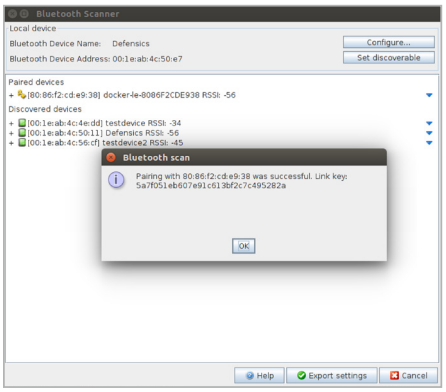
Key features

Intelligent fuzzing engine

The Defensics engine is programmed with knowledge on input type, whether it's an interface, protocol, or file format. Because the engine has a deep understanding of the rules that govern communication within the input type, it can deliver targeted test cases that exploit that input type's inherent security weaknesses. This intelligent and systematic approach to fuzz testing allows Synopsys to reduce testing time without compromising cost or security.



Synopsys Fuzz Testing reports contain message sequence logs to help users identify the root cause of an anomalous reaction.



Synopsys Fuzz Testing offers automated capabilities throughout the testing process, such as Defensics Device Explorer, to relieve users of the burden of manual configuration.

See the full list of unknown vulnerabilities Synopsys Fuzz Testing has discovered.

A comprehensive fuzzing solution

Our 250+ prebuilt, generational test suites ensure quick time to fuzz and relieve you of the burden of creating manual tests. We continuously update our test suites for new input types, specifications, and RFCs.

- Customize any of our test suites by fine-tuning the message sequence. The data sequence editor allows you to cover corner cases not within Synopsys Fuzz Testing's predefined scope.
- Need added extensibility? Use our template fuzzers. Universal Data Fuzzer (a file format template fuzzer) and Traffic Capture Fuzzer (a protocol template fuzzer) generate test cases by reverse engineering sample files you provide.
- Have proprietary or custom input types? Write your own test suites with Defensics SDK, which supports Java, Python, and selected transport layers and comes equipped with instrumentations.

Fits into most development life cycles

Synopsys Fuzz Testing contains workflows that enable it to fit almost any environment from a technological and process standpoint. Whether you employ a traditional SDL or a CI development life cycle, Synopsys brings fuzz testing into development early, allowing you to catch and remediate vulnerabilities more cost-effectively. Got an unconventional development life cycle? Our experienced Professional Services team can help you identify fuzz testing checkpoints, define fuzz testing metrics, and establish a fuzz testing maturity program.

It's not just about fitting into the development process; it's also about working with surrounding technologies. API and data export capabilities allow Synopsys Fuzz Testing to share data for additional reporting and analysis, making Synopsys Fuzz Testing a true plug-and-play fuzzer.

Detailed, data-rich reports for efficient remediation

- Contextualized logs. Remediation logs detail the protocol path and message sequences between Synopsys Fuzz Testing and the system under test (SUT) to help you identify the trigger and technical impact of each vulnerability.
- Vulnerability mapping. Synopsys Fuzz Testing maps each vulnerability to industry standards such as CWE and injection type to enhance information discovery and expedite remediation.
- Issue re-creation. Synopsys Fuzz Testing narrows the vulnerability trigger to a single test case so you can re-create the issue and verify the fix.
- Remediation packages. Generate encrypted remediation packages for your software suppliers to facilitate secure, collaborative remediation across the supply chain.

Scale fuzz testing with automation

From scanning for the test target to determining the number of layers to connect to, Synopsys Fuzz Testing offers a rich set of APIs for flexible, scalable automation to meet all your needs:

- Test single devices
- Set up repeatable automation to ensure test plans are followed every time
- Reduce testing times with the latest in scalable virtualization

SYNOPSYS®

Fuzz Testing (Defensics)
Test Suite Catalog

Authentication, Authorization, and Accounting (AAA)

- Diameter Client
- Diameter Server
- EAPOL Server
- Kerberos Server
- LDAPv3 Client
- LDAPv3 Server
- RADIUS Client
- RADIUS Server
- TACACS+ Client
- TACACS+ Server

Application

- FIX
- JSON Format
- Web Application
- WebSocket Client
- WebSocket Server
- XML SOAP Server
- XML SOAP Client
- XML File
- XMPP Server

Bus Technologies

- CAN Bus
- CAN FD

Cellular Core

- BICC / M3UA
- GRE
- GTP Prime
- GTPv0
- GTPv1 Client
- GTPv1 Server
- GTPv2-C Client
- GTPv2-C Server
- PMIPv6 Client
- PMIPv6 Server
- S1AP
- SCTP Client
- SCTP Server
- SMPP
- SMS (SMPP injection)
- SMS (file injection)
- X2-AP

Core IP

- DHCP / BOOTP Client
- DHCP / BOOTP Server
- DHCPv6 Client
- DHCPv6 Server
- DNS Client
- DNS Server
- FTP Client
- FTP Server
- HTTP Client
- HTTP Server
- HTTP/2 Server
- ICAP Server
- IPv4 Package
  - ARP Client
  - ARP Server
  - ICMP
  - IGMP
  - IPv4
  - TCP Client for IPv4
  - TCP Server for IPv4
- IPv6 Package
  - ICMPv6
  - IPv6
  - TCP Client for IPv6
  - TCP Server for IPv6
- SOCKS Client
- SOCKS Server

Email

- IMAP4 Server
- MIME
- POP3 Server
- SMTP Client
- SMTP Server

General Purpose

- Traffic Capture Fuzzer
- Universal ASN.1 BER Server
- Universal Fuzzer

ICS

- 60870-5-104 (iec104) Client
- 60870-5-104 (iec104) Server
- 61850 / Goose / SV
- 61850 / MMS Client
- 61850 / MMS Server
- BACNET
- CIP Server
- COAP
- DNP3 Client
- DNP3 Server
- MQTT Client
- MQTT Server
- Modbus Master
- Modbus PLC
- OPC UAC
- Profinet DCP
- Profinet PTCP Client
- Profinet PTCP Server

Link Management

- LACP (802.3ad)
- STP / RSTP / MSTP / ESTP

Media

- Archives Package
  - GZIP
  - JAR
  - ZIP
- Audio Package
  - MP3
  - MPEG4 (M4A / MP4)
  - OGG
  - WAV
  - Windows Media (WMA / WMV)
- Images Package
  - GIF
  - JPEG
  - PNG
  - TIFF
- Video Package
  - H.264 File Suite
  - H.264 RTP Format
  - MPEG2-TS
  - MPEG4 (M4A / MP4)
  - OGG
  - Windows Media (WMA / WMV)
- vCalendar
  - vCard

Medical

- DICOM Server
- HL7v2 Server

Metro Ethernet

- BFD
- CFM (802.1ag, Y.1731)
- E-LMI (MEF-16)
- Ethernet (802.3, 802.1Q)
- GARP (802.1D)
- LLDP (802.1AB)
- OAM (802.3ah)
- PBB-TE Server
- Synchronous Ethernet (ESMC)

Public Key Infrastructure (PKI)

- CMPv2 Client
- CMPv2 Server
- CSR

Remote Management

- CWMP (TR-69) ACS
- CWMP (TR-69) CPE
- IPMI Server
- Netconf test suite
- PCP Server
- SNMP trap
- SNMPv2c Server
- SNMPv3 Server
- SSHv1 Server
- SSHv2 Server
- Syslog
- TFTP Server
- Telnet Server

Routing

- BGP4+ Client
- BGP4+ Server
- DVMRP Package
  - DVMRPv1
  - DVMRPv3
- IS-IS
- LDP
- MPLS Server
- MSDP
- NHRP
- OSPFv2
- OSPFv3
- Openflow controller
- Openflow switch
- PIM-SM/DM
- RIP
- RIPng
- RSVP
- TRILL Server
- VRRP

Storage

- CIFS / SMB Server
- DCE / RPC Server
- FCOE + FIP Client
- FCOE + FIP Server
- NFSv3 Server
- NFSv4.0/4.1 Server
- Netbios Server
- SMBv2 Client

SYNOPSYS®

Fuzz Testing (Defensics)
Test Suite Catalog (cont.)

- SMBv2 Server
- SMBv3 Client
- SMBv3 Server
- SunRPC Server
- iSCSI Client
- iSCSI Server

Time Synchronization

- IEEE1588 PTP Client
- IEEE1588 PTP Server
- NTP Client
- NTP Server

VoIP

- H.323 Client
- H.323 Server
- MGCP Server
- MSRP Server
- RTP / RTCP / SRTP
- RTSP Client
- RTSP Server
- SIP UAC
- SIP UAS (+TT)
- SIP-I Server
- STUN Client
- STUN Server
- TURN Client
- TURN Server

VPN

- DTLS Client
- DTLS Server
- IKEv2 Server
- IKEv2 Client
- IPSec
- ISAKMP / IKEv1 Client
- ISAKMP / IKEv1 Server
- L2TPv2/v3 Server
- L2TPv2/v3 Client
- OCSP Client
- OCSP Server
- SCEP
- SSTP
- TLS / SSL Client 1.1
- TLS / SSL Client 1.2
- TLS / SSL Server 1.1
- TLS / SSL Server 1.2
- X.509v3 Certificates

Wireless

- Bluetooth LE Package
  - ATT Client
  - ATT Server
  - Advertisement
  - HOGP Host
  - Health
  - Profiles
  - SMP Client
  - SMP Server
- Bluetooth Package
  - A2DP
  - AVRCP
  - BNEP
  - HDP
  - HFP-AG
  - HFP-Unit
  - HSP-AG
  - HSP-Unit
  - L2CAP
  - OBEX-Server
  - RFCOMM
  - SDP
- Wi-Fi AP Package
  - 802.11 WLAN AP
  - 802.11 WPA AP
  - WPA Enterprise
- Wi-Fi Client Package
  - 802.11 WLAN Client
  - 802.11 WPA Client

Monitoring and engine capabilities

Instrumentation

- Valid case
- Syslog
- Agent
- SNMP
- Custom scripting at each testing execution

SafeGuard checkers

- Amplification
- Authentication bypass
- Blind LDAP injection
- Blind SQL injection
- Certificate validation
- Compressed signer's name in RRSIG record
- Cross-site request forgery
- Cross-site scripting
- Extra cookie compared to valid case
- Heartbleed
- Information leakage
- Insufficient randomness
- LDAP injection in response
- Malformed HTTP
- Remote execution
- SQL injection in response
- Unexpected data
- Unprotected credentials
- Weak cryptography

Anomaly categories

- ASN.1 / BER anomalies
- Credential anomalies
- Deep packet inspection
- EICAR antivirus test file
- GTUBE (generic test for unsolicited bulk email)
- Control plane injection anomalies
- Integer anomalies
- Network address anomalies
- Overflow anomalies
- Underflow anomalies

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity.

For more information go to 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: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™

03/21/18.DS_FuzzTesting_032118.