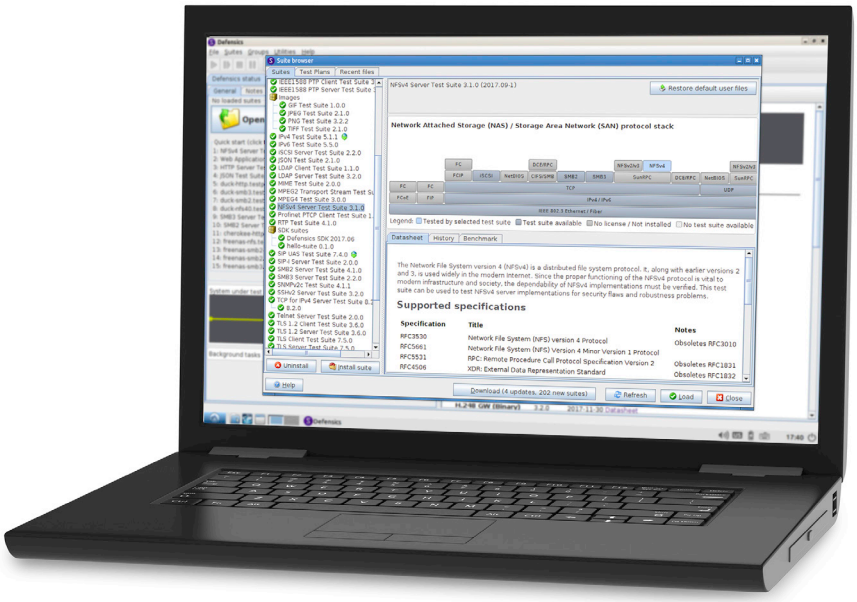
BLACKDUCK®

# Defensics
## Fuzz Testing

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

## Overview

Defensics® Fuzzing 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, Defensics allows organizations to ensure software security without compromising on product innovation, increasing time to market, or inflating operational costs.

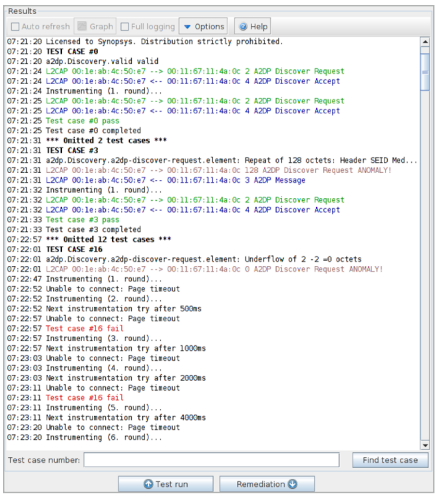



Defensics' logical user interface walks users through each step of the process, making advanced fuzz testing easy.

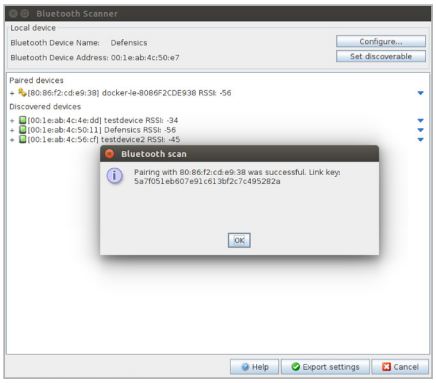
## Key features

### 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 you to reduce testing time without compromising cost or security.




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




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

## A comprehensive fuzzing solution

Our 300+ 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 Defensics' predefined scope.
- Need added extensibility? Use our template fuzzers. Universal Data Fuzzer is a file format template fuzzer, and SDK Express helps 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 and selected transport layers and comes equipped with instrumentations.
- Speed up testing with FuzzBox support. It's now easy to fuzz wireless LAN and IoT protocols, with test runs directly on custom hardware.
- Choose from five new vertical solution bundles: automotive, ICS, IoT, networking, and telecom. Vertical solution bundles include foundational protocols in addition to protocols relevant to that vertical market.

## Fits into most development life cycles

Defensics 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, Defensics 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 Defensics to share data for additional reporting and analysis, making Defensics 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 Defensics and the system under test (SUT) to help you identify the trigger and technical impact of each vulnerability.
- **Vulnerability mapping.** Defensics maps each vulnerability to industry standards such as CWE and injection type to enhance information discovery and expedite remediation.
- **Issue re-creation**. Defensics 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, Defensics 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

# **Defensics Fuzz Testing** | Test Suite Catalog

### Authentication, Authorization, and Accounting (AAA)
- Diameter Client/Server
- EAPOL Server
- LDAPv3 Client/Server
- RADIUS Client/Server
- TACACS+ Client/Server
- MACsec Server

### Application
- FIX
- gRPC
- JSON Format
- Web Application
- WebSocket Client/Server
- XML SOAP Client/Server
- XML File
- XMPP Server
- AMQP Server
- WAMP Server
- OWAMP Server
- TWAMP Server

### Automotive*
- CAN Bus
- CAN FD
- DoIP Server
- gPTP Server
- J1939
- SOME/IP
- SRP Server
- MMTP Server

### Core IP
- DHCP/BOOTP Client/Server
- DHCPv6 Client/Server
- DNS Client/Server
- FTP Client/Server
- HTTP Client/Server
- HTTP/2 Client/Server
- HTTP/3 Server
- ICAP Server
- IPv4 Package
  - ARP Client/Server
  - ICMP
  - IGMP
  - IPv4
  - TCP for IPv4 Client/Server
- IPv6 Package
  - ICMPv6
  - IPv6
  - TCP for IPv6 Client/Server
- SOCKS Client/Server
- Multicast DNS
- PPP over L2TP Client
- PPPoE

### Email
- IMAP4 Client/Server
- MIME
- POP3 Server
- SMTP Client/Server

### General Purpose
- SDK Express
- Universal ASN.1 BER
- Universal Fuzzer

### ICS
- 60870-5-104 (iec104) Client/Server
- 61850/Goose/SV
- 61850/MMS Client/Server
- BACNET
- CIP Server
- COAP Server
- DNP3 Client/Server
- MQTT Client/Server
- Modbus Master
- Modbus PLC
- OPC UA Server
- Profinet DCP
- Profinet PTCP Client/Server
- DLMS/COSEM Client/Server
- ISASecure Testing Solution

### 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)

### Medical
- DICOM Server
- HL7v2 Server
- FHIR Client/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)
- /IPv6

### Public Key Infrastructure (PKI)
- CMPv2 Client/Server
- CSR

### Remote Management
- CWMP (TR-69) ACS
- CWMP (TR-69) CPE
- IPMI Server
- NETCONF
- PCP Server
- SNMP trap
- SNMPv2c Server
- SNMPv3 Server
- SSHv1 Server
- SSHv2 Server
- Syslog
- TFTP Server
- Telnet Server

### Routing
- BGP4+ Client/Server
- IS-IS
- LDP
- MPLS Server
- MSDP
- OSPFv2
- OSPFv3

- Openflow controller
- Openflow switch
- PIM-SM/DM
- RIP
- RIPng
- RSVP
- TRILL Server
- VRRP
- COPS Client/Server

### Storage
- CIFS/SMB Server
- DCE/RPC Server
- NFSv3 Server
- NFSv4.0 / 4.1 Server
- Netbios Server
- DNNG
- SMBv2 Client/ServerMP
- SMBv3 Client/Server
- SunRPC Server
- iSCSI Client/Server

### Telecom - Cellular Core
- BICC/M3UA
- GRE
- GTP Prime
- GTPv1 Client/Server
- GTPv2-C Client/Server
- PMIPv6 Client/Server
- SCTP Client/Server
- SMPP
- SMS
- MAP
- BSSAP
- BSSAP+
- CAP
- INAP
- ISUP
- MTP3 / M2UA|M2PA
- TCAP / SCCP / M3UA

### Telecom - 5G Technology
- E1AP Client/Server
- F1AP Client/Server
- PFCP Client/Server
- NGAP/NAS Client/Server
- SBI
- X2AP Client/Server
- XnAP Client/Server
- S1AP/NAS Client/Server
- eCPRI Client/Server

### Telecom – O-RAN
- O-RAN O2 Producer/Consumer
- O-RAN A1-P Producer/Consumer
- O-RAN A1-EI Producer/Consumer
- E2AP E2 Node
- E2AP Near-RT RIC

### Time Synchronization
- IEEE1588 PTP Client/Server
- NTP Client/Server

### Universal Plug and Play
- UPnP Package
  - UPnP Multicast Eventing
  - UPnP SOAP
  - UPnP SSDP Control Point
  - UPnP SSDP Device

### VoIP
- H.323 Client/Server
- H.248 GW Binary/Text
- H.248 MGC Binary/Text
- MGCP Server
- MSRP Server
- RTP/RTCP/SRTP
- RTSP Client/Server
- SIP UAC
- SIP UAS (+TT)
- SIP-I Server
- STUN Client/Server
- TURN Client/Server
- SigComp Server

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

### Wireless
- Zigbee Package
  - FuzzBox Zigbee APS
  - FuzzBox Zigbee MAC
  - FuzzBox Zigbee NWK
- Thread package
  - FuzzBox Thread 6LoWPAN
  - FuzzBox Thread MAC
- Bluetooth LE Package
  - ATT Client/Server
  - Advertisement
  - HOGP Host
  - Health
  - L2CAP Server
  - LL Peripheral
  - Profiles
  - SMP Client/Server
- Bluetooth Package
  - A2DP
  - AVRCP
  - BNEP
  - HFP AG/Unit
  - HSP AG/Unit
  - L2CAP
  - MAP Client
  - OBEX-Server
  - PBAP Client
  - RFCOMM
  - SDP
- Wi-Fi AP Package
  - 802.11 WLAN AP
  - 802.11 WPA AP
  - 802.11 WPA3 AP
- Wi-Fi Client Package
  - 802.11 WLAN Client
  - 802.11 WPA Client
  - 802.11 WPA3 Client

For full list of test suites, please see https://www.blackduck.com/fuzztesting/defensics.html

## 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
- ECDH Public Key validation
- Extra cookie compared to valid case
- Heartbleed
- Information leakage
- Insufficient randomness
- LDAP injection in response
- Malformed HTTP
- Remote execution
- SQL injection in response
- SMP insecure pairing parameters
- 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

**Note:** We add test suites frequently. Please contact us for the latest list.


phase pacific
A subsidiary of CoverTel Telecommunications Group

***Need Local Support?***

***Contact: Frank Cappellari***
***Email: frank.cappellari@phasepacific.com***
***Mobile: +61 449 205 670***
***Office: +61 (03) 9381 7818***


## About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.


©2025 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. March 2025