



**CODENOMICON**

**defensics™**

**DEFEND. THEN DEPLOY.**

---

PREEMPTIVE SECURITY AND ROBUSTNESS TESTING SOLUTIONS

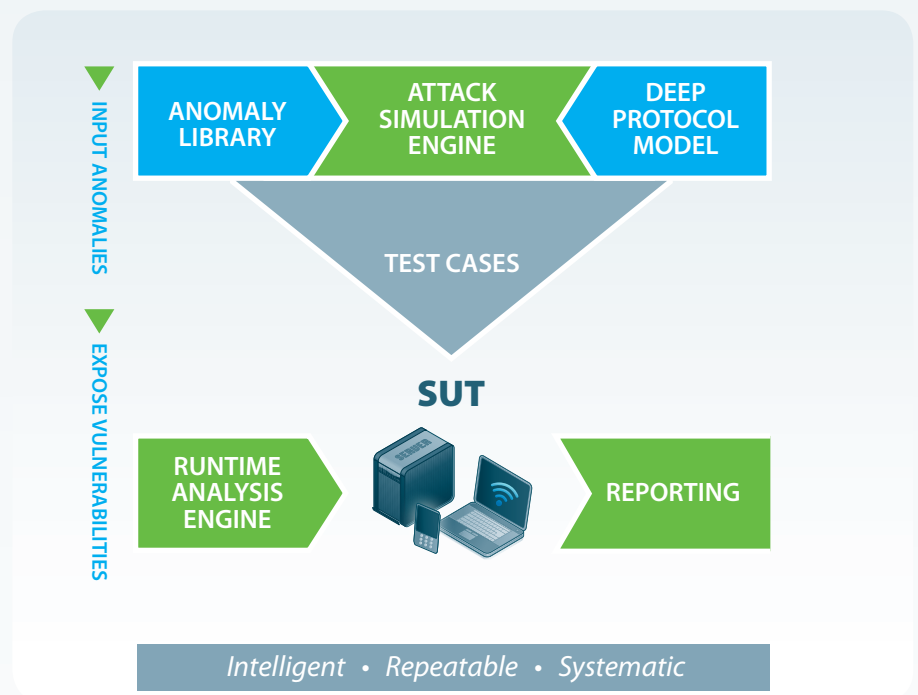
"It's what you don't know that makes you vulnerable."  
- David Chartier, CEO of Codenomicon Ltd

## The DEFENSICS™ Advantage

Codenomicon DEFENSICS™ testing solutions empower customers to mitigate known and unknown threats in products and services prior to release or deployment. Ensure the Secure Development Lifecycle (SDLC) of your system by building security into it and strengthen it, before exposures or outages occur and zero-day attacks strike.

The fundamental challenges in robustness testing are the infinite number of potential vulnerabilities and the difficulty of reaching the deeper protocol layers.

The DEFENSICS™ Attack Simulation Engine is the industry's first state-aware test case generator. It utilizes deep protocol models to intelligently target protocol areas most susceptible to vulnerabilities even in deeper protocol layers with high accuracy, while maintaining broad coverage through automatic test generation.



## FUZZING

### Fuzzing in a Nutshell

> **ROBUSTNESS TESTING:** Fuzzing is a form of robustness testing, which focuses on communication interfaces and the discovery of security related issues, such as overflows and boundary value conditions.

> **FEEDING INPUTS AND MONITORING OUTPUTS:** Robustness testing is a software testing technique, in which unexpected data is fed to the inputs of a system, and the behavior of the system is then monitored.

> **DISCOVERING PROTOCOL IMPLEMENTATION FLAWS:** If the system under test (SUT) fails, e.g., by crashing or by failing built in code assertions, then there is a bug in the software.

> **BLACK-BOX, GREY-BOX AND WHITE-BOX TESTING:** Fuzz tests can be conducted in a number of ways depending on the tester's needs and the amount of information available on the system being tested.

### Fuzzing Benefits

> **REPRESENTING REAL THREATS:** Fuzzing is essentially doing what the attackers do, but before them. Fuzz tests can also be used to simulate system aging or overload situations.

> **FINDING ZERO-DAY VULNERABILITIES:** The main strength of Fuzzing is its unparalleled ability to find unknown vulnerabilities. Fuzzing gives testers more time to create and implement patches.

> **HARDENING SYSTEMS BEFORE COMMERCIAL DEPLOYMENT:** The costs of bad Quality of Service (QoS) and downtime can be considerable to your company reputation and sales. Discover flaws and create patches for them proactively, before problems occur and flaws can be exploited.

> **BUILDING THE SECURITY INTO YOUR SYSTEM:** Fuzzing improves the quality of your code ensuring the security of your application. Most security systems merely add to the complexity of your system, making it more vulnerable.

How resilient is our service?  
Will the next attack take us down?

CHIEF SECURITY OFFICER  
CARRIER / OPERATOR

Does our application development process comply  
with risk management best practices?

CHIEF INFORMATION OFFICER  
FINANCIAL SERVICES ENTERPRISE



"DEFENSICS™ solutions achieve remarkable efficiency in discovering both known and unknown bugs and they are valuable tools for companies seeking to harden their systems before deployment."

- Srihari Padmanabhan, Research Analyst, Test & Measurement, Frost & Sullivan

## Features and Benefits

- > BROADTEST TEST COVERAGE:**  
DEFENSICS™ provides off-the-shelf testing tools for over 200 protocols and file formats. It can be used to test digital media and wireless infrastructures and network protocols.
- > MILLIONS OF PREBUILT TEST CASES:**  
Built-in expertise and automated test case execution facilitate testing. No manual test case creation effort or testing experience is needed.
- > FAST TEST RUNS:**  
DEFENSICS™ utilizes intelligent model-based test cases. By targeting the test cases the amount of test cases needed is significantly reduced making the whole testing process quicker and more cost efficient.
- > EASY TO INTEGRATE:**  
As a software-only platform DEFENSICS™ can be easily integrated into your existing software development and testing processes. All the reporting and test case features can be processed with external editors and scripts.
- > PROACTIVE TESTING:**  
By integrating DEFENSICS™ into your software development process, you can discover flaws at the earliest possible moment. The earlier the bugs are discovered the cheaper and easier it is to fix them.
- > INTEGRATED ONLINE DOCUMENTATION:**  
Share online detailed test case material and results within your organization. The reports have direct links to test cases identifying specific problems making all identified flaws easily repeatable and traceable.
- > MULTIPLE USERS AND LOCATIONS:**  
All users can remotely access the same system and reproduce all identified flaws. It is no longer necessary to create identical test environments, because the same test runs can be executed by multiple users in multiple locations.
- > REGRESSION, COMPLIANCE AND AUDITING:**  
The off-the-shelf tools combined with powerful test reproduction, documentation and reporting tools make DEFENSICS™ the optimal solution for regression analysis, compliance testing and auditing.



How can we improve the efficiency of security and robustness testing within our organization?

GENERAL MANAGER  
NETWORK DEVICE DEVELOPER

Are flaws and patches impacting sales and damaging our brand?

DEVELOPMENT DIRECTOR  
CONSUMER DEVICE DEVELOPER

## CODENOMICON

### Expertise

Codenomicon Ltd. is recognized in the industry for its innovations in negative black-box testing and its unique targeted approach to fuzz testing networked and mobile applications. Its solutions are based on extensive research. Codenomicon is a spin-off of the widely acclaimed PROTOS project of the Oulu University Secure Programming Group (OUSPG).

### Innovation

First launched in 2001, the DEFENSICS™ testing platform continues to demonstrate a high degree of innovation by incorporating the latest research into its intelligent fuzzing techniques. While, traditional security testing has been overwhelmed by the fast adoption rate of new technologies, fuzzing has proven itself as an easily adaptable testing technique. Codenomicon fulfills the changing testing needs of its customers by providing not only state-of-the-art tools but also extensive customer support.

### Community

Codenomicon's main goal is to improve overall customer confidence in technology by helping companies and organizations to provide better products and services. Codenomicon is also actively engaged in the open source community and through its CROSS program and assists open source projects fix critical flaws in their code, also creating benefits for companies utilizing these projects in their products.

### Growth

In ten years, Codenomicon has grown from an university spin-off to an international company with over 200 customers including Alcatel-Lucent, AT&T, Cisco Systems, Nordea, Nortel, Microsoft and Nokia Siemens Networks. Headquartered in Oulu, Finland with offices in Helsinki, California and Hong Kong, the company markets its test solutions and services directly and through international partners. The company is privately held with investments from Verdane Capital and Prime Technology Ventures.

 [www.codenomicon.com](http://www.codenomicon.com)

## Test Suites

Core Internet	Net Management	Routing
IPv4 (TCP, UDP, IPv4, ICMP, IGMP, ARP), IPv6 (TCP, UDP, IPv6, ICMPv6), IPsec, DNS, DNS-SEC, NTP (Client, Server), DHCP/BOOTP Client, DHCP/BOOTP Server, HTTP Server, HTTP Client, FTP Server, DHCPv6 Client, DHCPv6 Server, MIPv6 (Client, Server)	HTTP Server, HTTP Client, TLS/SSL Server, TLS/SSL Client, Telnet Server, SSH1 Server, SSH2 Server, SNMPv1/v2 Server, SNMPv3 Server, TFTP Server, UPnP Server, Syslog, SNMP TRAP	IS-IS, DVMRP, GRE, OSPFv2, OSPFv3, PIM-SM/DM, RSVP, VRRP, BGP4, RIP, RIPng, MPLS/LDP, HSRP, NHRP

Remote Access	VPN	VoIP/IMS
EAPOL Server, PPPoE, Diameter Server, Diameter Client, LDAPv3 Server, TACACS+ Server, TACACS+ NAS, RADIUS (Server, Client), Kerberos Server	IPSec, SSH1 Server, SSH2 Server, TLS/SSL Server, TLS/SSL Client, ISAKMP/IKEv1 (Client, Server), IKEv2, OCSP (Client, Server), L2TPv2, L2TPv3, x.509	SCTP, H.248, H.323, RTSP (Client,Server), TLS/SSL Server, TLS/SSL Client, SIP UAS, SIP UAC, SigComp, RTP/RTCP/SRTP, MGCP, UPnP Server, SMPP, x.509, BICC, STUN, TURN, Diameter

3G / 4G-LTE	Digital Media	Email
SCTP, GRE, IPsec, Diameter (Server, Client), LDAP Server, TLS /SSL (Server, Client), SIP UAS, SIP UAC, GTPv0, GTPv1, GTPv2, RADIUS (Server, Client), PMIP	AIFF, AU, AMR, IMY, MP3, VOC, WAV, BMP, GIF, JPEG, MBM, PCX, PNG, PIX, PNM, RAS, TIFF, WBMP, XBM, XPM, WMF, AVI, Quicktime, MPG1, MPG2, MPEG4, ZIP, CAB, JAR, LHA, GZIP, vCalendar, VCard	POP3 Client, POP3 Server, IMAP4 Client, IMAP4 Server, SMTP Client, SMTP Server, MIME

File Systems/Storage	WLAN	Link Management
CIFS/SMB Server, iSCSI Server, SunRPC Server, NFS Server, SMBv2, FCoE, FIP, PFC	802.11 Server, 802.11 Client, WPA Server, WPA Client	LACP, STP, MSTP, RSTP, ESTP

Bluetooth	IPTV	PDA/ Smartphone
L2CAP, SDP, RFCOMM, OBEX, OPP, FTP, IrMC Sync, BIP, BPP, BNEP, HFP, HSP, DUN, PBAP, FAX, AVRCP, A2DP, HCRP, HID, SAP, HFP Client, HSP Client, BPP, MDP/HDP, 2.1 compliant	MPEG4, MPEG2, IPsec, TLS/SSL, RTP/RTCP, RTSP, HTTP, FTP, TFTP, IPv4, PIM-SM/DM, RSVP, IGMP, CWMP(TR-69), MPEG2-TS, SIP-UAS, SIP-UAC	IPv4, DHCP/BOOTP, HTTP, TLS/SSL, UPnP, SIP, Audio, Images, Video, Bluetooth, 802.11

Industrial Automation	Archives	Metro Ethernet
(SCADA/DCS) Modbus, IPv4 (TCP, UDP, IPv4, ICMP, IGMP, ARP)	GAB, GZIP, JAR, LHA, ZIP	BFD, CFM, E-LMI, Ethernet, GARP, LLDP, OAM, PBT/PBB-TE, STP/RSTP/MSTP/ESTP, PTP, SyncEthernet

General Fuzzers	Finance
XML (File, SOAP), Traffic Capture Fuzzer, Universal Fuzzer	FIX

## Protocols Supported

802.11	IPsec	RSTP
ARP	IPv4	RSVP
BGP4	IPv6	RTCP
BFD	IS-IS	RTP
BICC	ISAKMP/IKE	RTSP
BOOTP	iSCSI	SCTP
BT	Kerberos	SigComp
CFM	L2TPv2	SIP
CIFS/SMB	L2TPv3	SIP TT
CWMP (TR-69)	LACP	SMBv2
DHCP	LDAPv3	SMPP
DHCPv6	LLDP	SMTP
Diameter	LPD	SNMP TRAP
DNS	MGCP	SNMPv1
DNS-SEC	MIPv6	SNMPv2c
DVMRP	MIME	SNMPv3
E-LMI	Modbus	SRTP
EAP	MPEG2-TS	SSH1
ESTP	MPLS/LDP	SSH2
Ethernet	MSTP	STP
Finger	NFS	STUN
GARP	NetBIOS	SunRPC
FCoE	NHRP	SyncEthernet
FIP	NTP	Syslog
FIX	OAM	TACACS+
FTP	OCSP	TCP
GRE	OSPFv2	Telnet
GTPv0	OSPFv3	TFTP
GTPv1	PBT/PBB-TE	TLS/SSL
GTPv2	PFC	TURN
H.248	PIM-DM/SM	UDP
H.323	PMIP	UPnP
HSRP	POP3	VLACP
HTTP	PPPoE	WPA1 WPA2
ICMP	PTP	VRRP
ICMPv6	RADIUS	X.509
IGMP	RIP	XML
IKEv2	RIPng	
IMAP4	Rlogin	

## Technical Requirements

### Supported Operating Systems

Windows 7, Windows XP SP3 and Linux CentOS

### Minimum System Requirements

1 GHz processor, 1 GB of free disk space, 1024x768 graphics resolution, 1 GB of RAM, CD-ROM or DVD drive, Network card (NIC)

### Oracle Java™ 2 Runtime Environment

Standard Edition 6 (1.6) 32-bit

USB port required for Bluetooth and WLAN tools