

# APPLICATION SECURITY PRODUCTS

Enterprises have an increasingly wide range of tools available for protecting Web applications, detecting vulnerabilities and facilitating secure development. Here's a sampling of such offerings:

## WEB APP SCANNERS, FIREWALLS AND PEN-TESTING PRODUCTS

Company	Product	Description
Application Security www.appsecinc.com	AppDetective	Detects database applications, scans for known vulnerabilities, executes pen tests and delivers audit reports.
Breach Security www.breach.com	BreachGate WebDefend	Appliance builds behavior-based profile of each Web application, passively decrypts SSL.
Cenzic www.cenzic.com	Hailstorm	Pen-testing and vulnerability assessment tool to integrate security into QA and development process.
eEye Digital Security www.eeye.com	SecureIIS	ISAPI filter uses a variety of detection methods to detect and block attacks against IIS servers.
F5 www.f5.com	TrafficShield	Web application firewall available as dedicated appliance or as module on BIG-IP application switches.
Fortify Software www.fortifysoftware.com	Fortify Source Code Analysis Suite	Utilizes a mock compiler that's executed at compile-time to look for insecure coding patterns.
Imperva www.imperva.com	SecureSphere Web Application Firewall	Uses "Dynamic Profiling" to build a baseline of normal behavior and detects and blocks dangerous behavior on a high-performance appliance.
Kavado* www.kavado.com	InterDo, ScanDo	InterDo software re-based Web application firewall can be deployed on Web server or inline on dedicated box; ScanDo discovers vulnerabilities and recommends fixes.
LogicLibrary www.logiclibrary.com	BugScan	Binary code scanning integrated into LogIDex software development asset tool; also available as stand-alone appliance.
NetContinuum www.netcontinuum.com	NC series	Web app firewall and application security gateway appliances detect Web attacks based on session states, such as forms and cookie-tampering, rather than signatures.
Ounce Labs www.ouncelabs.com	Praxis	Source code scanner identifies potentially dangerous functions. Can deliver an overall risk score.
Secure Software www.securesw.com	CodeAssure WorkBench, CodeAssure Integrator	WorkBench discovers vulnerabilities and policy violations in source code; Integrator incorporates vulnerability assessment into existing QA/developer processes.
Sentryware www.sentryware.com	HIVE	Inline appliance uses unique application-layer token technology to proxy Web transactions and validate requests.
SPI Dynamics www.spidynamics.com	WebInspect	Web app/Web services vulnerability assessment scanner.
Teros** www.teros.com	Teros	Series of Web application firewall appliances models correct application behavior and detects attacks without signatures.
Watchfire www.watchfire.com	AppScan	Suite of three application security assessment tools: AppScan DE, for developers; AppScan QA for QA personnel; and AppScan Audit for auditors and compliance officers.

## FREWARE

Tool	Description
Bugscam www.sourceforge.net/projects/bugscam	Works with commercial debugger IDA Pro to scan binaries for problematic use of certain library functions.
FlawFinder www.dwheeler.com	Documents and traverses C and C++ code trees looking for myriad potential vulnerabilities.
RATS www.securesw.com	Scans for risky functions in multiple languages to include C, C++, Perl, Python and PHP.
SPIKE www.immunitysec.com	Large strings, typical attack patterns or randomized payloads can be sent to a target host to attempt to elicit atypical responses.
Splint www.splint.org	Complements RATS by adding quality-assurance components such as memory leaks and strong bounds checking capability.

\*Kavado was acquired by Protegrity in August. \*\*Teros was recently acquired by Citrix Systems.