

Acunetx Websites Vulnerability Features List

Features	Standard	Premium
ARCHITECTURE AND SCALE		
Unlimited Web Scanning	✓	✓
Number of Users	1	Unlimited
User Roles and Privileges	--	✓
Max Number of Scan Engines	1	Unlimited
ACUNETIX VULNERABILITY ASSESSMENT ENGINE		
Scanning for 4500+ Web Application Vulnerabilities	✓	✓
Scanning for Network Vulnerabilities	--	✓
Acunetix DeepScan Crawler	✓	✓
Acunetix AcuSensor (IAST Vulnerability Testing)	✓	✓
Acunetix AcuMonitor (Out-of-band Vulnerability Testing)	✓	✓
Acunetix Login Sequence Recorder	✓	✓
Manual Intervention during Scan	✓	✓
Malware URL Detection	✓	✓
Scanning of External Web Application Assets	✓	✓
Scanning of Internal Web Application Assets	✓	✓
KEY REPORTS AND VULNERABILITY SEVERITY CLASSIFICATION		
Key Reports (Affected Items, Quick, Developer, Executive)	✓	✓
OWASP TOP 10 Report	✓	✓
CVSS (Common Vulnerability Scoring System) for Severity	✓	✓
Remediation Advice	✓	✓
Compliance Reports*	--	✓
CENTRALIZED MANAGEMENT AND EXTENSIBILITY		
Dashboard	✓	✓
Scheduled Scanning	✓	✓
Notifications	✓	✓
Continuous Scanning	--	✓
Target Groups	--	✓
Assign Target Business Criticality	--	✓
Prioritize by Business Criticality	--	✓
Assign Target Management to Users	--	✓
Trend Graphs	--	✓
WAF Virtual Patching**	--	✓
Issue Tracking System Integration (Jira, Microsoft TFS, GitHub)	--	✓

Jenkins Plug-in Integration	--	✓
Integration APIs	--	✓

** PCI DSS, ISO/IEC 27001; The Health Insurance Portability and Accountability Act (HIPAA); WASC Threat Classification; Sarbanes-Oxley; NIST*

Special Publication 800-53 (for FISMA); DISA-STIG Application Security; 2011 CWE/SANS Top 25 Most Dangerous Software Errors.

*** Imperva SecureSphere, F5 BIG-IP Application Security Manager, and Fortinet FortiWeb WAF*