

Full Feature List

	STANDARD	PREMIUM
ARCHITECTURE AND SCALE		
Unlimited Web Scanning	✓	✓
Multi-user		✓
User Roles and Privileges		✓
Multiple Scan Engines		✓
Number of Users	1	Unlimited
Max Number of Scan Engines	1	Unlimited
Delivery	Desktop Application	Hosted or On-premises
ACUNETIX VULNERABILITY ASSESSMENT ENGINE		
Scanning for 6500+ web application vulnerabilities	✓	✓
Scanning for 50,000+ 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 Online 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		✓
Role-Based Access Controls		✓
Trend Graphs		✓
WAF Virtual Patching**		✓
Issue Tracker Integration (Jira, Azure DevOps, GitHub)		✓
Jenkins Plug-in Integration		✓
Integration APIs		✓

Information in this document was correct at the time of preparation - March 2020. E & OE

* 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