WS32C64G

Dynamic Web Application Security Testing Tool

The **The Omni WS32C64G** is designed specifically for applications, and as such it's important to look beyond traditional vulnerability scanners when it comes to identifying gaps in an organization's application security. To really understand your risks, learn more about some types of web application and cybersecurity attacks, and how web scanners can help increase the safety of your applications.

Web application vulnerabilities involve a system flaw or weakness in a web-based application. They have been around for years, largely due to not validating or sanitizing form inputs, misconfigured web servers, and application design flaws, and they can be exploited to compromise the application's security.

Application Security

Web applications power many mission-critical business processes today, from public-facing e-commerce stores to internal financial systems. While these web applications can enable dynamic business growth, they also often harbor potential weaknesses that, if left unidentified and unremediated, could quickly lead to a damaging and costly data breach.

To address this growing threat, businesses are increasingly deploying **The Omni WS32C64G** dynamic application security testing (DAST) tools as part of a more security-forward approach to web application development. **The Omni WS32C64G** tools provide insight into how your web applications behave while they are in production, enabling your business to address potential vulnerabilities before a hacker uses them to stage an attack. As your web applications evolve, **The Omni WS32C64G** solutions continue to scan them so that your business can promptly identify and remediate emerging issues before they develop into serious risks

High Performance Computing WS32C64G

Dynamic Application Security Testing which famous with Web Application Vulnerability Scanners are automated tools that scan web applications, normally from the outside (black-box), to look for security vulnerabilities such as Cross-site scripting, SQL Injection, Command Injection, Path Traversal, and insecure server configuration.

WS32C64G

Service Features and Benefits

Technical Description

Version	14
Vulnerability Assessment Engine	Scanning for 7,000+ web application vulnerabilities
	Scanning for 50,000+ network vulnerabilities
	DeepScan Crawler
	AcuSensor (IAST Vulnerability Testing)
	AcuMonitor (Out-of-band Vulnerability Testing)
	Login Sequence Recorder
	Business Logic 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 (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)
Centralized Management and Extensibility	Dashboard
	Assign Target Business Critically
	Prioritize by Business Critically
	Role-Based Access Controls
	Trend Graphs
	Issue Tracker Integration (Jira, Azure DevOps, GitHub, Gitlab, Bugzilla, Mantis)
	Jenkins Plug-in Integration
	Integration APIs
Product Support	SLA-based commercial remote and onsite support for 5 Years
Rack Unit	2 RU
Ports	6 Ports 10GbE SFP+
Processor	Dual, Intel® Xeon® Silver 4314 2.4G, 16C/32T, 10.4GT/s, 24M Cache, Turbo, HT (135W) DDR4-2666
Memory	64 GB
Hard Drives	Dual, 480GB SSD SATA Mix Use 6Gbps 512 2.5in Hot-plug AG Drive, 3 DWPD
Power Supply	Dual, Hot-Plug, Fully Redundant Power Supply

Resolve vulnerabilities faster than you can say “remediation”

- **Eliminate false positives.** Save yourself from hours of manually confirming which vulnerabilities are real.
- **Pinpoint vulnerability locations.** See the exact lines of code that need to be fixed so you don’t have to search for them.
- **Get remediation guidance.** Give developers all the information they need to resolve security flaws on their own.

One Source Distribution Pte Ltd
12 New Industrial Road #07-03
Singapore 536202
sales@onesource.com.sg