How to Choose the

BEST VULNERABILITY SCANNER

Not all vulnerability scanners are created equal. Here are some tips to help you select the right vulnerability scan tool for your organization.

ROUND 1

UNDERSTAND YOUR PCI DSS VULNERABILITY SCANNING REQUIREMENTS

- 11.2.1 Perform quarterly internal vulnerability scans
- 11.2.2 Perform quarterly external vulnerability scans via an ASV (Approved Scanning Vendor)
- 11.2.3 Rescan as needed, after any significant change.

SCAN TYPES

INTERNAL VULNERABILITY SCAN:
Scans other hosts on the same network to identify internal vulnerabilities.

EXTERNAL VULNERABILITY SCAN:
Works from a location external to your IPs and identifies known weaknesses.

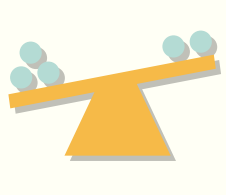
ROUND 2

ASK QUESTIONS WHEN SELECTING A SCANNER

UPDATES:
Is the scanner updated daily, weekly, monthly, or annually?

PLUGINS:
Does the internal scanner use correctly updated plug-ins?

FALSE POSITIVES:
Is the scanner bogged down with thousands of false positives?

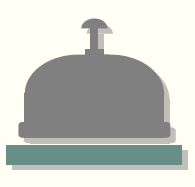


QUANTITY:
How many vulnerabilities does the scan search for? (Over 50,000 is recommended)

REPORTING:
Do reports give clear, concise, and thorough recommendations to fix the problems?

SIZE:
Will scanners overload and crash vulnerable servers?

CONFIDENCE:
Do you trust the organization performing your scans? (If hackers can access scan results, they know your weaknesses.)



ASSISTANCE:
How much technician help will you receive to fix vulnerabilities? Does it cost extra?

TRIAL:
Can you test out the scanner before purchase?

ROUND 3

MEET UNIQUE COMPANY NEEDS

Find a system that has the ability to adjust with changing company goals, works well with IT staff, and finds both new and old vulnerabilities.

securityMETRICS®