VULNERA

DATA SHEET

Vulnerability Scanners vs. VULNERA Solution

What are Vulnerability Scanners?

All IT assets, including desktops, laptops, mobile devices, on-prem and cloud servers, network appliances, FAX machines and printers, cloud apps, and IoT and wireless devices can be identified and inventoried using vulnerability scanners, through an automated process. For each asset, it attempts to identify operational details such as its operating system and the software installed on it. It might also reveal additional characteristics, such as open ports and software running with known vulnerabilities.

Security teams use vulnerability scanners to identify security vulnerabilities, including:

- Weaknesses in the environment
- Insight into degrees of risk from each vulnerability
- Recommendations on how to mitigate the vulnerability

It's crucial to comprehend precisely how vulnerability scanning will fit into a larger vulnerability management and security posture before investing in a tool.

Beyond Scanning

The networks and devices used by a business change frequently, which increases the possibility of threats developing. Therefore, ongoing scanning is required to stay ahead of these risks.

If vulnerability scans are performed frequently, traditional vulnerability scanning technologies can be quite helpful in identifying common CVEs. However, to classify these vulnerabilities according to their level of exploitability and prioritize remediation efforts, a comprehensive vulnerability management program is also necessary. Additionally, it is crucial to confirm that security controls have been successful in reducing risk once they have been implemented.

Security teams can find, categorize, and fix security vulnerabilities thanks to VULNERA, an all-in-one solution. The hassles of purchasing, constructing, and administering security tools and employees are removed by this fully-managed solution.

	VULNERA	Vulnerability Scanners
Management	Fully managed. Client supplies the targets, and VULNERA supplies the sensors for internal, external, and cloud environments. The dashboard displays results, and regular meetings are used to assess the data and progress.	100% DIY. Internal resources are used for configuration, management, upkeep, reporting, analysis, and context.
Time to Value	Results will be accessible within 24 hours of sensor deployment and connectivity validation.	Even with SaaS solutions, procurement and deployment take time and expertise. Scans must be configured, executed, and reviewed to prioritize issues and eliminate false positives.

	VULNERA	Vulnerability Scanners
Coverage	Uses a variety of livehost enumeration and service identification techniques, building on manual testing methodology. All TCP ports 0-65535 and top UDP ports are included by default.	Primitive enumeration methods and a severe lack of port coverage. Can be configured, but this can lead to scans that take a long time or fail.
Validation	Client is notified when issues are new, remediated or reopened as well as when hosts or services are online/offline.	Enterprise edition required or not available. Additional tooling may be required.
Remediation Tracking	Identifies why an issue was remediated and documents the reason.	Enterprise edition required or not available. Additional tooling may be required.
Audit-Readiness	Industry-standard deliverables and a letter of attestation is provided. As a third-party firm, deliverables have been scrutinized by auditors and governing bodies for years.	Vulnerability scanner results do not apply to third-party security assessments because the organization runs them. Auditor objectivity requires a third-party assessment.
Continuous Coverage	Assessments are conducted at least once per day, upward of once every hour or continuously.	Scanners must be scheduled. Due to generic profiles, they are frequently slow and, unless specifically customized, lack thorough coverage.
Vulnerability Management KPIs	Available out of the box. ROI is clearly demonstrated by tracking remediation and validation efforts.	Enterprise edition required or not available. Additional tooling may be required.
Risk Context & Prioritization	To give a consolidated and prioritized perspective of risk, vulnerability data is enhanced with information from public feeds, third party repositories, and vendor advisories.	Provides severity ratings and CVSS scores with no additional risk context. It's possible to incorporate more enterprise tooling and threat intelligence options to add context.

+1 626.515.5523
www.vulnera.com | info@vulnera.com

VULNERA