What to Look for in a Vulnerability Mangement Solution

FORTRA

User-friendly Interface

Automated and On-Demand Scanning

Accuracy and Asset Correlation

Historical Data

Data Management

API

User-friendly Interface

- A prebuilt, intuitive interface is essential.
- Many tools can find vulnerabilities, but not all are user-friendly.
- A good interface enables repeatable, consistent scans.
- Easy-to-use tools save time, especially with IT staff shortages and turnover.
- Complicated tools can risk network damage in inexperienced hands.

Historical Data

A strong VM system provides more than current network status—it includes historical data.

- Many tools lack this, but it's crucial for tracking vulnerability impact, duration, and fix attempts.
- Helps assess broader business impact on customers, vendors, or third parties.
- Useful for uncovering assets potentially masked by malware.

Automated and On-Demand Scanning

Scanning is essential to any VM tool. Key points:

- Run scans at least monthly or after system changes.
- Systems change constantly; new vulnerabilities appear daily.
- Daily checks are time-consuming but can be automated with the right tool. Automation is useful, especially if it assigns remediation tickets to IT staff.
- On-demand scans are valuable for validating fixes, tracking KPIs, and monitoring vulnerability timelines.
- Combining automation with on-demand scanning offers control and responsiveness.

Data Management

After scans reveal vulnerabilities, top VM systems offer strong data management tools.

- Customize reports and access actionable insights anytime.
- Query scanned assets, track unscanned devices, and monitor fix attempts.
- Tag and label devices and reports for easy sorting and searching.
- Avoid manual data compilation—get the info you need quickly and efficiently.

Accuracy and Asset Correlation

Scan results must be accurate and actionable.

- Enterprise VM tools reduce false positives to save time.
- Built-in tech tracks devices across scans, even with changing IPs.
- Asset data correlation ensures consistent device identification.
- Prevents missed fixes or unnecessary remediation.
- Offers flexible matching, sorting, and manual overrides for unique needs.

API

- Systems that are available via API are even more beneficial, integrating into the broader security ecosystem.
- VM data can help enrich SIEM, SOAR, NAC and more.
- Integration with ticketing would allow a manager to apply a filter to return vulnerabilities that meet certain criteria and auto assign a certain tech to fix them then follow-up with automated validation activities.

FORTRA

www.fortra.com