8 Vulnerability Management Tools to Consider in 2023

In this handbook:

8 Vulnerability Management Tools to Consider in 2023

KAREN SCARFONE, PRINCIPAL CONSULTANT

Vulnerability management programs continue to expand beyond patch management and discovering insecure configurations. Vulnerability management now tackles security weaknesses and vulnerabilities within system and software designs -- with the right tools for the job.

Once an organization implements a vulnerability management program, the next step is providing the program's team with powerful vulnerability management tools to automate as many tasks as possible.

Evaluate these eight open source and vendor-supported vulnerability management tools. Organizations should expect to deploy multiple tools in a mature vulnerability management program. No single tool can do everything an organization needs for vulnerability management.

The following vulnerability management tools were selected because they continue to see development and maintenance, are a mixture of emerging and established, and cover a variety of vulnerability management approaches. The list is in alphabetical order.

1. Aqua Security Trivy

Trivy is an open source vulnerability scanner for cloud-native environments, acquired by Aqua Security in 2019. It scans OSes, container images and code repositories to identify software with missing patches, known CVEs and infrastructure-as-code configuration issues. Trivy checks numerous programming languages and detects missing patches in those languages and in application dependencies. It offers some basic capabilities to identify configuration issues in popular container-related tools.

Trivy is free to use. Aqua Security offers additional paid vulnerability scanning and management capabilities through Aqua Wave and Aqua Enterprise. Organizations can request a trial or demo of these tools.

For more information, visit Aqua Security's Trivy page.

2. CrowdStrike Falcon Complete XDR

CrowdStrike offers several products and services through its Falcon brand. Falcon Complete XDR is a managed extended detection and response (MXDR) service for endpoints and cloud instances. Many MXDR platforms, including Falcon Complete, offer vulnerability management capabilities as part of a wider range of endpoint protection services.

CrowdStrike provides bundled enterprise pricing for its various products, including Falcon Spotlight, which handles vulnerability management, upon request.

For more information, visit Crowdsrike's Falcon Complete XDR page.

3. Greenbone OpenVAS

OpenVAS is an open source vulnerability scanner with a frequently updated feed of vulnerability tests for detecting OS and application vulnerabilities. It scans for missing patches and configuration errors and can handle unauthenticated and authenticated scans. For deeper vulnerability management and scanning, Greenbone offers the open source Greenbone Community Edition, which includes a security assistant and a vulnerability manager daemon.

OpenVAS is free to use, while Greenbone provides a larger set of vulnerability tests as part of its commercial vulnerability service. Greenbone offers a free trial for its paid vulnerability management tool.

For more information, visit Greenbone's OpenVAS page.

4. Microsoft Defender Vulnerability Management

Microsoft Defender Vulnerability Management's tools for vulnerability scanning and assessment complement Microsoft Defender for Endpoint and the Microsoft 365 E5 productivity suite. Defender Vulnerability Management identifies and prioritizes missing patches and configuration errors on endpoints. Defender Vulnerability Management also checks browser extensions, looks for expiring digital certificates and finds other security issues. It scans managed and unmanaged endpoints, even when not connected to the corporate network, through agentless scanners and built-in modules.

For Microsoft Defender for Endpoint Plan 2 and Microsoft 365 E5 customers, Defender Vulnerability Management comes as an add-on feature for $2 per user, per month -- up to five devices each. Non-Microsoft customers can try Defender Vulnerability Management standalone for free.

For more information, visit Microsoft Defender's Vulnerability Management page.

5. Qualys VMDR 2.0

Qualys Vulnerability Management, Detection and Response (VMDR) 2.0 is a risk-based vulnerability management platform. The VMDR tool detects missing patches, configuration errors and expiring digital certificates. It can prioritize and implement remediation of each problem, and it integrates with various ticketing systems and patch and configuration management products. Qualys VMDR 2.0 is cloud-based and deploys a lightweight agent to each endpoint it monitors and protects.

Organizations interested in Qualys VMDR 2.0 can try a 30-day free trial and request a quote from the vendor for pricing.

For more information, visit Qualys' VMDR 2.0 page.

6. Rapid7 InsightVM

Rapid7 InsightVM is an agent-based vulnerability management product. It identifies a variety of vulnerabilities in endpoints and provides the capability to remediate them and provide tracking capabilities into existing ticketing systems. InsightVM can scan endpoints to determine if they comply with various cybersecurity standards. It integrates with more than 40 tools used in IT environments, including Splunk, AWS and ServiceNow.

Rapid7 offers a free trial for InsightVM. Organizations can request a per-asset quote.

For more information, visit Rapid7's InsightVM page.

7. Tenable Nessus

Tenable Nessus supports diverse platforms, including IoT devices running on Raspberry Pi. Nessus discovers vulnerable software versions, security misconfigurations and default passwords. It features a plugin library with more than 190,000 plugins and more than a hundred released weekly.

Tenable offers Professional and Expert licenses starting at $3,590 and $5,290, respectively. The vendor also offers the free, but limited, Nessus Essentials.

For more information, visit Tenable's Nessus page.

8. Trellix ePolicy Orchestrator

Trellix ePolicy Orchestrator is a SaaS-based cybersecurity management platform for endpoints. It provides a single interface to automate and monitor cybersecurity management tasks, such as identifying missing patches, misconfigurations and other endpoint issues. It automatically remediates and removes any discovered vulnerabilities. It includes APIs that integrate with more than 150 third-party tools.

Organizations can contact Trellix for a demo and quote.

For more information, visit Trellix's ePolicy Orchestrator page.