Vulnerability Management Software Tools

1. Intruder

Function: IT teams can become more agile, secure, and proactive with the aid of Intruder. It offers significant advantages in proactive change detection, alerting users to newly discovered instances or hosts as well as potential security flaws.

Use Case: With a single platform that combines proactive threat response, automated vulnerability scanning, and continuous network monitoring, Intruder provides you with an accurate picture of your attack surface. It simplifies vulnerability management so you can concentrate on fixing what really matters.

Open Source/ Paid: Open Source

Pros	Cons
● Excellent choice for enterprises with complex networks and strict security needs ● Auto Scanning ● Alert Levels	● Reports could contain more detail

2. ESET Vulnerability & Patch Management

Function: It is integrated into the ESET PROTECT Platform, which offers you a single, unified solution for broader, enterprise-grade protection against ransomware and other malware types, as well as zero-day threat prevention across all endpoints, servers, and emails.

Use Case: Organizations that require their applications to be current but lack IT resources can benefit from an extra layer of security. It finds vulnerabilities, fixes them, or lessens the likelihood that they will be exploited by updating operating systems and applications on all endpoints.

Open Source/ Paid: Paid

Pros	Cons
● Automated Scanning ● Flexibility ● Orchestration	● Quite expensive ● Lower plans lack features, such as a firewall and password manager, that are included in other providers' basic plans ● No VPN functionality even on ESET's highest plan.

3. ManageEngine Vulnerability Manager Plus

Function: It combines all of the features of vulnerability management into a single package, handling security configurations of network endpoints, hardening internet-facing web servers, and vulnerability assessment and patching from a single, centralized console.

Use Case: It provides you with a vast array of pre-defined, informative reports that you can use to assess the security of your network, communicate risks, monitor developments, and brief executives on security requirements.

Open Source/ Paid: Paid

Pros	Cons
● Intuitive User Interface ● Easy to use with great feature set ● Good Customer Support	● Deploying security configurations can be risky and have adverse effects on the servers. ● Failed updates need to be manually downloaded from the internet. ● Confusion about needed patches,

	failures, and their fixes.

4. Qualys VMDR

Function: This cloud-based solution finds vulnerabilities in all networked assets, including workstations, servers, peripherals (like IP-based printers or fax machines), and network devices (like routers, switches, and firewalls).

Use Case: To scan and secure containerized apps and container orchestration platforms like Kubernetes, it offers container security solutions. It also offers FIM capabilities as well, allowing businesses to keep an eye on and identify unauthorized changes to important files and directories.

Open Source/ Paid: Open Source

Pros	Cons
● Contains tons of apps that extends its capabilities ● Reporting & dashboard are of highly professional quality ● Good GUI	● Limited scheduling tasks ● No offline deployment

5. Rapid7 InsightVM

Function: It provides you with the reporting, automation, and integrations you need to quickly and effectively identify, prioritize, and address those vulnerabilities. It does more than just show you what threats are in your IT environment.

Use Case: With InsightVM, you can see not just what vulnerabilities exist in your remote endpoints and on-premises IT environment, but also how much of a risk they pose to your business and which ones hackers are most likely to target.

Open Source/ Paid: Open Source

Pros	Cons
● Automatic scanning of devices ● Good Reporting ● Easy to manage	● Costing ● False positive findings

6. Tenable

Function: It is an exposure management tool that can be used by your company to effectively communicate cyber risk, focus efforts on preventing likely attacks, and obtain visibility across your modern attack surface in order to support peak business performance.

Use Case: For current web apps, its Web App Scanning offers thorough vulnerability scanning. By minimizing false positives and false negatives, its accurate vulnerability coverage helps security teams identify the real security risks in their web applications.

Open Source/ Paid: Open Source

Pros	Cons
● Provides quick reliable vulnerability testing ● Reports are in clean format ● It has variety in types of vulnerability scanning it does	● Difficult Asset Management ● Confusing User Interface ● Unorganized documentation

7. GFI Languard

Function: It gives you the ability to control and preserve endpoint security throughout your network. It gives you visibility into every component of your network, assists you in identifying any possible weak points, and lets you apply security fixes.

Use Case: It shows which USB devices are linked, what software they are running, whether any ports are open, hardware details, and more. All of the scanned machines

on your network will have comprehensive hardware configuration data identified by the GFI LanGuard network scanner.

Open Source/ Paid: Paid

Pros	Cons
● Excellent Automation and Monitoring Capabilities ● Good Vulnerability Scanning and Patch Management capabilities ● Flexibility in Organizing Computers and Setting Customized Schedules	● Limitation on number of ports and service dependencies ● Outdated interface lacking visual aspects ● Service requires frequent server restart

8. Arctic Wolf

Function: Installed on endpoints, this lightweight software allows you to respond to threats, scan endpoints for vulnerabilities and misconfigurations, and gather actionable intelligence from your IT environment.

Use Case: Its utilization of diverse detection techniques, such as machine learning, enables it to promptly identify questionable and non-standard behaviors in the gathered data set. It is able to provide a company with special, tailored protection based on customized detection rules.

Open Source/ Paid: Open Source

Pros	Cons
● Monitoring 365 logins ● Monitoring Windows processes ● Active Directory monitoring	● Some erroneous 365 alerts about failed logins ● Need an easier method to suppress alerts (outside of email) ● Too many places to look for info in console

9. TripWire

Function: Integrity Manager can be integrated with security configuration management (SCM), log management, and SIEM, among other security controls. Tripwire FIM includes additional components that allow for more intuitive tagging and management of the data from these controls, improving data protection over previous methods.

Use Case: Protecting vital infrastructure, Prevent unauthorized changes and vulnerabilities from occurring on servers, databases, and applications. Fulfilling the requirements for compliance: Obtain and uphold compliance with HIPAA, FISMA, SOX, PCI, and other laws.

Open Source/ Paid: Open Source

Pros	Cons
● It allows tracking development changes for engineer accountability. ● Allows to monitor changes/updates being done to systems ● Can be used to track user access and critical system changes.	● Reporting system not granular

10. Acunetix

Function: It makes it simple to manage the vulnerabilities found and enables you to secure your websites and web applications quickly and effectively. A standard web browser can be used to access Acunetix by multiple users in your organization through the Acunetix Online portal.

Use Case: It is an automated tool for web application security testing. It audits your web applications and looks for exploitable vulnerabilities such as cross-site scripting and SQL injection.

Open Source/ Paid: Paid

Pros	Cons
● Integration of tool with different IDE is great ● Easy to scan code and identify vulnerabilities ● Dashboard is easy to customize	● Configuration of DevSecOps can be improved for ease ● Dashboard can have API integration ● Broaden the scope of vulnerabilities