VMDR with TruRisk™

Essential Guide to Vulnerability Management: A Risk-Based Approach

With attackers using increasingly sophisticated methods to break into systems, manual methods of locating and inspecting assets on your network, clouds and endpoints are no longer enough. The right Vulnerability Management (VM) solution can monitor your environment, enabling you to: discover devices running in your network, detect vulnerabilities with libraries of signatures, determine which vulnerabilities have been weaponized for attack, correlate them with exploit intelligence, provide fixes for them, and protect your enterprise during the remediation process. One must-have capability is to accurately prioritize vulnerabilities based on their true risk to your unique business and IT environment.

This checklist of best practices will save you time and help you understand what to look for when selecting a VM solution, whether you have a handful of systems or millions.

Modern VM solutions should be assessed according to 5 key functions and capabilities:

1 Risk-Based Vulnerability Assessment

Managing cyber risk has become a major business issue. Organizations lost more than $49.2M due to ransomware attacks in 2021, according to the **FBI ICR 2021 report**. Furthermore, cybersecurity resources are often limited and unable to scale with the growing volume of vulnerabilities, which has doubled from 2016 to 2021. The good news is that modern VM solutions have grown more capable of detecting vulnerabilities and identifying threats. However, more alerts do not equate to more security. Cybersecurity solutions in general, and Vulnerability Management specifically, need to do more to accurately detect and prioritize vulnerabilities based on cyber risk. Enterprises should demand automated and risk-based alert prioritization that allows security practitioners to focus on the vulnerabilities most critical to their specific and unique business environment.

2 Vulnerability Detection

Vulnerability management solutions are only as robust as the data they can obtain and leverage for vulnerability identification and intelligent management. Regretfully, not all VM solutions are equal in their detection ability. Security practitioners should look for VM solutions that continuously monitor your perimeter, cloud, and internal systems and can identify rogue or unknown devices in your network. Be sure to test any VM solution's ability to prioritize vulnerabilities based on threat intelligence feeds and business-critical assets to make sure that scan results you receive is beneficial for informed and efficient response.

3 VM Beyond Detection

Traditional VM products merely scan your networks and report on the data they discover. This conventional scanner-based approach typically runs vulnerability scans once every few days, resulting in outdated information and elevated risk exposure. Comprehensive VM solutions track the state of your systems to provide an ongoing, always up to date view of your security posture. Integration and orchestration with endpoint security offerings such as EDR (Endpoint Detection and Response) and XDR (eXtended Detection and Response) should also be considered, as VM solutions are inevitably deployed alongside endpoint security solutions. When building your VM strategy, make sure your solution leverages a robust agent-based approach and works well with your current or planned EDR or XDR solutions, assuring that you can leverage VM for the detection, identification, prioritization, and response to vulnerabilities in under 2-seconds, wherever they are.

4 Deployment and Perimeter Coverage

Traditional VM solutions installed within your networks require users to acquire, configure, and manage vulnerability management servers, perform backups on them, and handle patch updates on a continuous basis. In contrast, a more comprehensive vulnerability management solution should not require ongoing updates or database backups. Your VM solution should be able to automatically cover your evolving network perimeter, diverse endpoints, and the adoption of cloud services to cover multiple site locations. When assessing your vulnerability management strategy, make sure the solutions you rely on provide your organization with the scalability required to handle new devices, users, and locations to anticipate the inevitable changes that will happen to your network perimeter over time.

5 CapEx and Hidden Costs

Some VM software solutions lock you in with up-front investments in equipment and require ongoing updates, database backups, etc. This can couple high upfront capital expenditures (CapEx) with potential hidden costs along the way. When selecting a vulnerability management solution, be sure to evaluate the solution's capabilities against its cost of implementation and cost of ongoing management to accurately assess the TCO over time. Modern risk-based vulnerability management solutions should be accessible directly via a browser and scale easily to handle new devices, users, and locations.

v230113