What is Advanced Vulnerability Management?

We all are aware of what vulnerability management is and how important it is for us to safeguard our IT environment. But when everything in the IT landscape is constantly changing, have we ever wondered if vulnerability management needs any upgrade? What was there in the IT environment two decades ago is not there today, and the security hemisphere has become even more complex post the pandemic. However, the vulnerability management process has almost remained the same with no innovation.

Suppose you still have convinced yourselves that siloed approach, relying on different tools for remediation, and focusing only on CVEs are enough to protect your network; it is the same as locking the main door and leaving all the windows in the house wide open and believing you are safe. Modern IT security teams need an advanced vulnerability management solution that automatically manages vulnerabilities and numerous security risks from a centralized console that strengthens the overall security posture.

Pitfalls of Traditional VM: Why Advanced Vulnerability Management?

There are numerous reasons why traditional vulnerability management cannot cope with the modern security landscape. Let us look at the three major reasons which present an inevitable need for Advanced vulnerability management.

Not Managing Vulnerabilities Beyond CVEs

Conventional tools focus only on CVEs or software vulnerabilities leaving behind other crucial security risks

Lack of Integrated Remediation

Traditional tools still lack integrated remediation, leaving IT security teams in a dilemma of which tool to use for remediation.

Relying on Siloes and Multiple Tools

For different steps of vulnerability management, traditional processes depend on multiple tools, causing chaos and confusion while correlating and assessing the vulnerabilities for mitigation.

What is Advanced Vulnerability Management?

Advanced Vulnerability Management reinvents the traditional process with a broader approach to vulnerabilities, integrated patch management, end-to-end automation, multiple security controls for remediation, and alignment with regulatory compliance from a single centralized console. It enables IT security teams to combat the existing vulnerability management challenges and go beyond traditional methods. With a continuous, automated, and advanced vulnerability management solution in place, you can easily prevent cyberattacks and achieve continuous security risk and compliance posture.

How Advanced Vulnerability Management differ from Traditional Vulnerability Management

Different Between Vulnerability Management and Advanced Vulnerability Management	
Vulnerability Management	**Advanced Vulnerability Management**
Siloed interfaces & multiple-point solutions approach	Unified, single-solution approach to visibility, detection, assessment, prioritization, and remediation
Rely on a separate tool for remediation	Integrated and seamless patch management capability for timely remediation
Discover only CVEs or software vulnerabilities	Detect vulnerability, misconfigurations, asset exposures, missing critical security patches, and security posture anomalies within a single console
Lack of remediation controls to fix security risk exposures	Remediation controls beyond patching to fix the vulnerability and other security exposures
Lack of risk prioritization based on threat intelligence	Threat intelligence-based risk prioritization, risk prediction, and remediation
Detection is not performed with threat focus and from the attackers' point of view	Attacker and threat-focused detection and mitigation
Manual methods and irregular processes	Built for automation, achieving continuous compliance
Irregular scans and no clarity on real-time risk posture	Continuous scan and up-to-date risk posture assessment
Lack of controls to establish real-time communication with devices	Ability to communicate with devices in real-time
Inaccurate vulnerability coverage	Timely and accurate coverage for vulnerability

Prolonged Patch Management Lifecycle taking months to complete	Rapid, continuous, and automated patch management lifecycle
Lack of capabilities to build queries to detect and respond to security risks	Build custom queries to detect security risks and deploy instant response
OS and device-specific support	Heterogeneous and device-agnostic support
Multiple agents	Single, light-weight, multifunctional agent
Lack of API support & eco-system integration	Native API support and eco-system integration
Segregated security & IT goals	Unified security and IT goals

How SanerNow Advanced Vulnerability Management works?

SanerNow provides a centralized solution to implement continuous, automated, and advanced vulnerability management. Here is how SanerNow AVM reinvents the existing vulnerability management process and adds a new spin to it.

Provides complete visibility over IT infrastructure

SanerNow AVM provides up-to-date visibility of the IT infrastructure. You can run continuous scans, detect the details of devices, hardware, and software assets in your network and establish complete control over them.

Assesses vulnerabilities and security risks from a single console & insightful reports

SanerNow AVM assesses the vulnerabilities and security risks thoroughly and provides detailed insights in its unified dashboard. SanerNow provides a wide range of customizable reports, including a comprehensive risk assessment report to view and assess various IT security risks in one place.

Prioritizes vulnerabilities & missing patches based on the severity

After a thorough assessment, SanerNow AVM automatically prioritizes the vulnerabilities and missing patches based on their severity level. With this, you can easily identify high-risk vulnerabilities and plan your remediation smartly.

Automates end-to-end tasks from a single centralized console

From detection to remediation, everything can be automated in SanerNow, so that you can implement hands-free vulnerability management. You also eliminate the need to traverse multiple tools and execute all tasks from a single centralized console.

Detects vulnerabilities and security risks with the industry's fastest scans powered by vast security intelligence

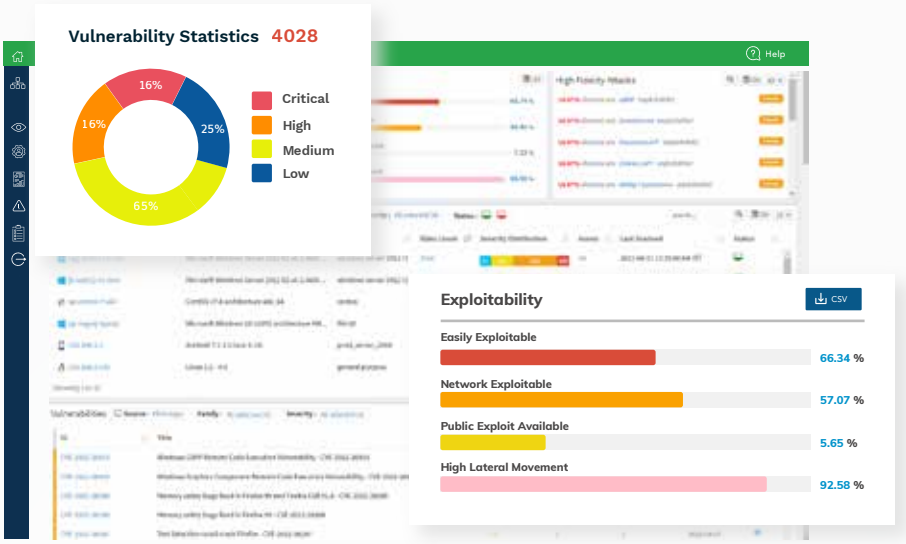
SanerNow AVM runs the industry's fastest scans in less than 5 minutes and detects the vulnerabilities quickly. With rapid scans, you can detect the information of vulnerabilities, IT asset exposures, missing patches, misconfigurations, deviation in security controls, security posture anomalies, and numerous security risks. SanerNow leverages its homegrown world's largest security intelligence library with 160,000+ vulnerability checks. The security intelligence feed is updated continuously to provide accurate detection.

Remediates vulnerabilities on time with integrated patching and other remediation controls

SanerNow AVM provides integrated patch management to aid faster remediation of vulnerabilities. You can also leverage the additional security controls available in SanerNow and remediate the security risk exposures in your network.

Conclusion

To deal with today's dynamic security landscape, a reinvention in vulnerability management is inevitable. SanerNow Advanced Vulnerability Management brings in an all-new perspective to cope with vulnerabilities and security risks and prevent cyberattacks. SanerNow AVM will not only help you keep your IT vulnerability landscape in check, but it will also help you establish a robust security framework that will work seamlessly without you having to bust your head across a maze of tools.



Schedule a SanerNow AVM demo here, and let us show what we tell

Schedule a Demo

CONTACT US

India - (+91) 80 4121 4020 / USA - (+1) 918 625 3023

info@secpod.com / www.secpod.com