secpod

A SanerNow Solution for
Vulnerability Management

Discover, Normalize, Prioritize Vulnerabilities & Misconfigurations

www.secpod.com

Maximize Visibility. Assess Risk Exposure. Overcome Security Risks

Organizations need a seismic shift in the way they manage vulnerabilities. Though there are plenty of tools and a buzz of opinions on how to address vulnerabilities, there is a shortage of an integrated platform to orchestrate vulnerability management tasks by unifying and automating asset discovery, asset standardization, holistic vulnerability discovery, compliance, and risk prioritization continuously. This approach is critical to spurring efficiencies in security operations, sharpening decision-making in discovering assets, assessing, and prioritizing vulnerabilities to control risk exposure.

Why do organizations need such a platform?
Currently, organizations have deep-seated challenges that prevent them from staying ahead of attacks.

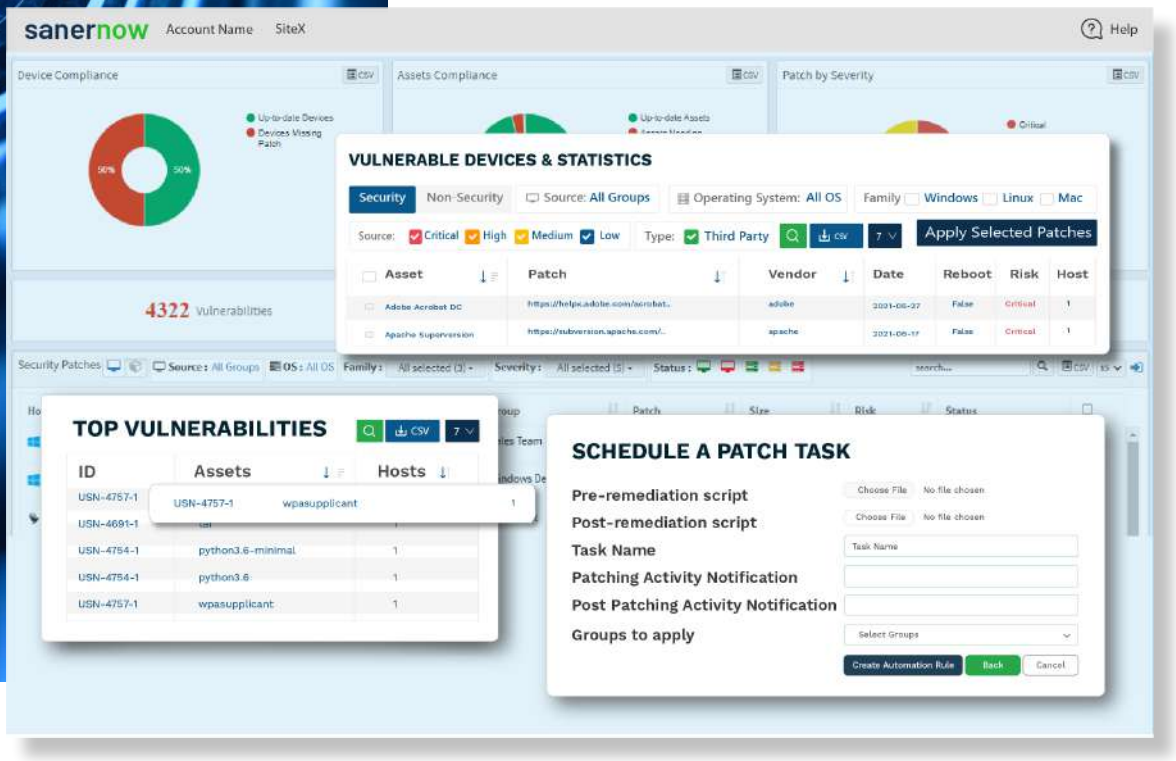
Some of them include: do vulnerability scanners cover the entire IT asset inventory, with no asset left behind? Are the scanners quick enough to find new vulnerabilities? With many tools in my security ecosystem, what is the speed at which organizations can contextualize, prioritize, and consolidate vulnerabilities? Is it possible to automate and enable continuous vulnerability management?
Traditional solutions will find it hard to provide answers.

SecPod's risk-based vulnerability management solution, with its interplay of steady but interconnected modules, can resolve the burgeoning challenges and questions in vulnerability management.

The Guarantee Success in Vulnerability Management

The solution is a show stealer, as it wins over the existing tried and tested tools having siloed configurations. It significantly speeds up vulnerability management with its proactive, automated, and continuous scanning capabilities to meet the growing risk landscape. From asset discovery to compliance, it can reshape an entire array of actions to enable the cause of integrated vulnerability management.

By going beyond traditional vulnerability management, it provides a broader approach to vulnerabilities by covering multiple security tasks, such as giving a holistic view of software and hardware inventory, discovering aberrations, deviation, and outliers in IT infrastructure, spot misconfigurations, prioritize vulnerabilities, run compliance scans, and simplifies compliance reporting.



Manage Attack Surface, Get in-depth Asset Information, and Simplify Compliance

- ✓ Accurately detect global and local IT assets to get a single-pane-of-glass visibility with quick and real-time scans for comprehensive inventory views and asset transparency
- ✓ Discover rarely used and outdated assets or applications to enable decisions on IT asset usage, cost control, and license optimization
- ✓ Drive regular scans to detect any changes in software and hardware
- ✓ Ensure proactive, continuous, automated real-time detection and tracking of assets through a unified cloud-based console
- ✓ Detect malicious software or hardware and block them
- ✓ Automate tracking of OS and third-party applications and drill down into the details of each instance Comprehensive assessment of IT infrastructure and identification of devices different than others using machine learning, statistical analysis, and deviation computation methods
- ✓ Assess risks with comprehensive scans based on SecPod's largest built-in vulnerability database with 175,000+ software vulnerability checks
- ✓ Detect misconfigurations and configuration drifts based on industry benchmarks
- ✓ Assess and ensure 100s of security controls are functioning
- ✓ Lightweight agent-based scanner which can scan and detect vulnerabilities in 5 minutes
- ✓ Perform accurate vulnerability detection and prioritization with insights on vulnerabilities based on severity level, exploitability level and isolate high-risk ones.
- ✓ Detect non-compliant devices by identifying faulty system configurations with fast compliance scans
- ✓ Monitor remote devices easily and simplify compliance reporting across Win, macOS & Linux
- ✓ Drive compliance risk assessments and get insights on risk remediation
- ✓ Customize compliance policies on available system configurations
- ✓ Convert compliance updates into customizable reports

One Platform. One Agent.

Risk-based vulnerability management solution is an ideal choice for attack surface management. With the explosion in distributed IT computing environments, the attack surface is rising. IT teams find it hard to gain a strong footing by keeping track of these assets and who is using them. By using this solution, IT teams can overcome the challenges of legacy tools, which are slow, manual, and error-prone. It works at speed and scale to discover, identify, and prioritize risks across public-facing assets, whether on-prem or cloud workloads.

Scan

Intelligent scanner capable of 5-minute lightning-speed scans. Continuous, on-demand, real-time scans can be scheduled without consuming excessive bandwidth or network resources.

Visualize

Gain 360-degree clarity on software asset exposure, including rarely used/outdated software & its licenses, get unparalleled visibility, monitoring, and access anytime from anywhere with a unified cloud-based console, and track software usage metrics.

Normalize

Discover vulnerable processes making outbound connections, unusual command execution, disabled BitLocker in systems, abnormal events, installation of any unfamiliar applications, and map it with software bill of materials.

Detect

Finds vulnerabilities that can cause high-fidelity attacks. Provides exploitability levels of vulnerabilities, including CVSS information. Ensures near-zero false positives.

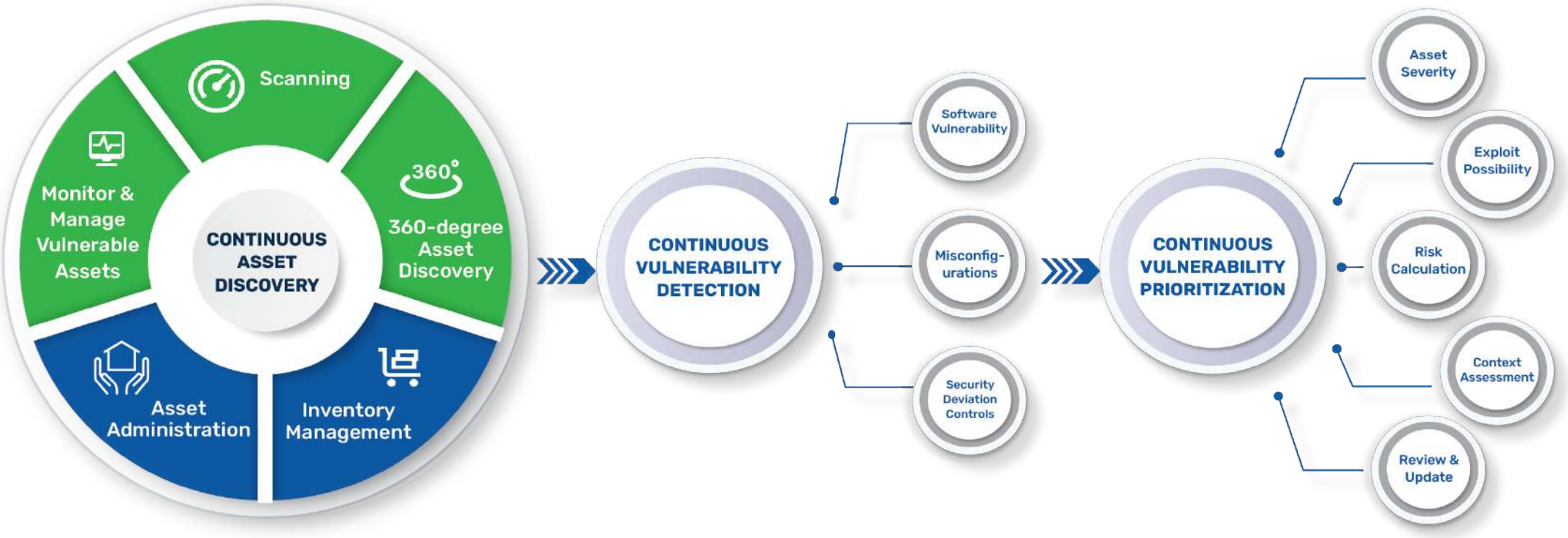
Comply

Compliance manager to identify missing system configurations, monitor remote devices, simplify reporting, and ensure continuous compliance scans to fulfill regulatory needs.

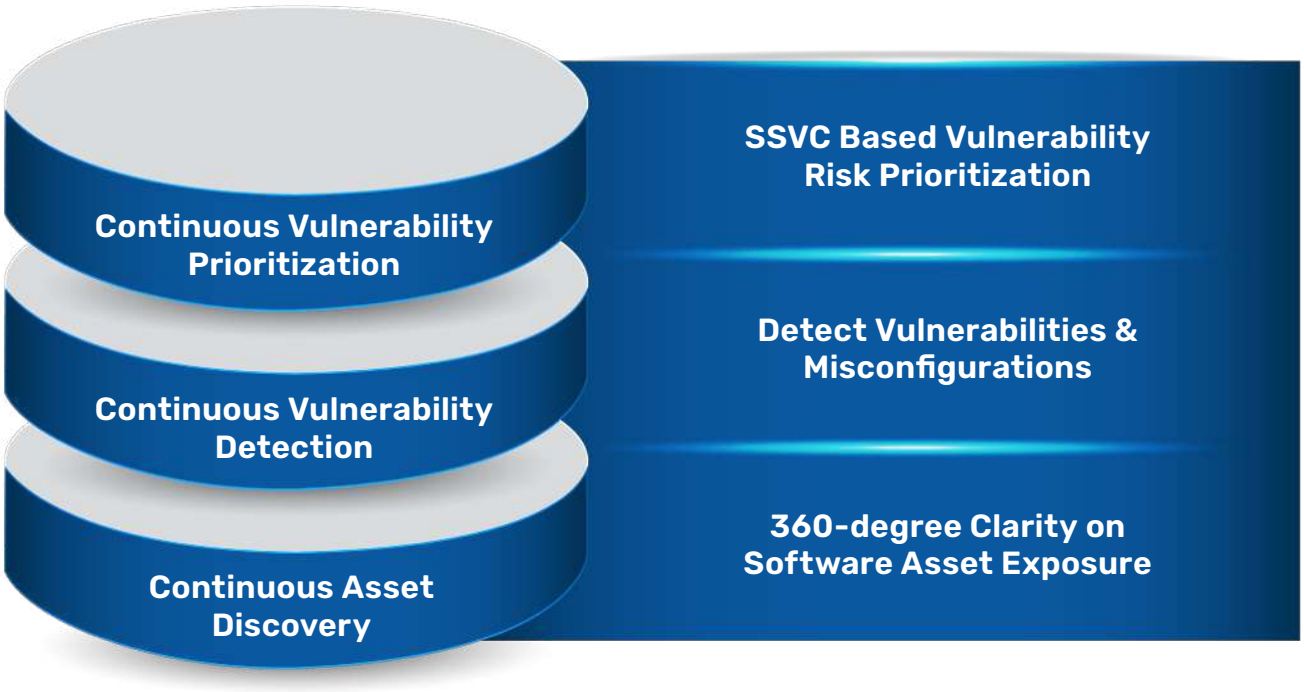
Prioritize

Understand and evaluate millions of vulnerabilities to enable mitigation efforts. Prioritizes risk based on exploitability, business impact, and vulnerability data analysis. Gives exhaustive visibility of risks.

Solution Workflow to Realize Value



SanerNow Modules in the Solution Stack



01 Asset Exposure Module

Ensure continuous visibility and maximize control over IT asset infrastructure by managing software and hardware assets in real time.

- Track software usage metrics & automatically track asset movements in the network
- Runs real-time, live asset scans on enterprise devices to gain a comprehensive 360-degree view of inventory with complete transparency
- Track rarely used & update applications, including software licenses, to optimize asset use
- Manage vulnerable assets and blacklist malicious and outdated apps

02 Continuous Posture Anomaly Management Module

Assess the network to discover deviations or aberrations, spot anomalies in the network from unusual services & processes, abnormal events in event logs, unwanted ports, unsigned applications, unusually executed commands, and hidden risks.

- Get intelligent insights on hidden security loopholes in the network and act on these insights to prevent attacks
- Assess the IT infrastructure and identify the devices that are different from others
- Get instant remediation measures to fix anomalies
- Discover attack vectors in the network and reduce risk exposures

03 Vulnerability Management Module

Operates through a lightweight single agent, which also acts as the single point of management to orchestrate the entire end-to-end process.

- Continuous, periodic scanning using the world's only automated, high-speed scanner to detect vulnerabilities in just 5 minutes.
- All scans based on the continuously updated SecPod's world's largest vulnerability & threat intelligence feed
- Unified cloud console to manage vulnerabilities in decentralized, hybrid IT environments

04 Compliance Management Module

Regulate devices for PCI-DSS, HIPPA, ISO, NIST, RBI, SEBI, or any other compliance standard with the help of the compliance manager to address configuration drifts.

- Run compliance checks & detect non-compliance devices.
- Monitor remote devices & enforce custom industry compliance policies.
- Ensure the IT environment is audit-ready.
- Get customized, insightful reports to meet regulatory needs

05 SSVC-based Vulnerability Risk Prioritization Module

Rapidly prioritizes risk and can handle millions of vulnerabilities with ease. Get exhaustive visibility into risk to reduce exploitable attack surface.

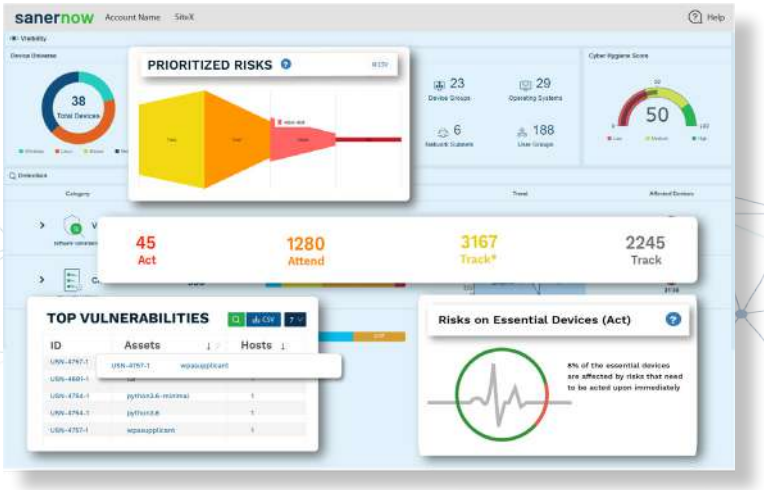
- Automates risk prioritization in real-time by combining SSVC framework with enhanced exploit prediction scoring system, & ML algorithms, & MITRE ATT&CK mapping capabilities
- Gain decisive insights into prioritizing risks & improve security posture
- Customize risk prioritization & configure it into based on org structure to calculate business impact

Manage Vulnerabilities Ingeniously. Enable Smarter Attack Surface Management.

Continuous vulnerability management is critical for continuous security validation. This helps in the continual identification of assets and mapping these assets for critical vulnerabilities. The approach also finds unknown assets, improving asset discovery, both hardware and software, which malicious actors might exploit to infiltrate the attack surface.

With the power of proactive and automated, high-speed scanning capabilities, the time taken to detect vulnerabilities is extremely short and happens in 5 minutes. With automated scans, the data generated is up to date, ensuring better efficiency and accuracy while uncovering vulnerabilities and lowering false positives.

It can enable better visibility & control in reducing vulnerabilities by categorizing them based on severity, asset importance, exploitability, and exposure. The solution improves the accuracy of vulnerability management and prioritizes and identifies the best remediation options to meet compliance regulations and reduce the risk profile of the IT infrastructure.



About SecPod

SecPod is a cyber security technology company. We prevent cyberattacks. We do everything to prevent attacks on the computing environment. Our product helps implement cyber hygiene measures, so attackers have a tough time piercing through. Our SanerNow Cyber Hygiene Platform provides continuous visibility to the computing environment, identifies vulnerabilities and misconfigurations, mitigates loopholes to eliminate attack surface, and helps automate these routines. Our product philosophy is offering simplicity and automation to make the job of security administrators slightly better.

Visit us- www.secpod.com
Write to us- info@secpod.com

Connect with us