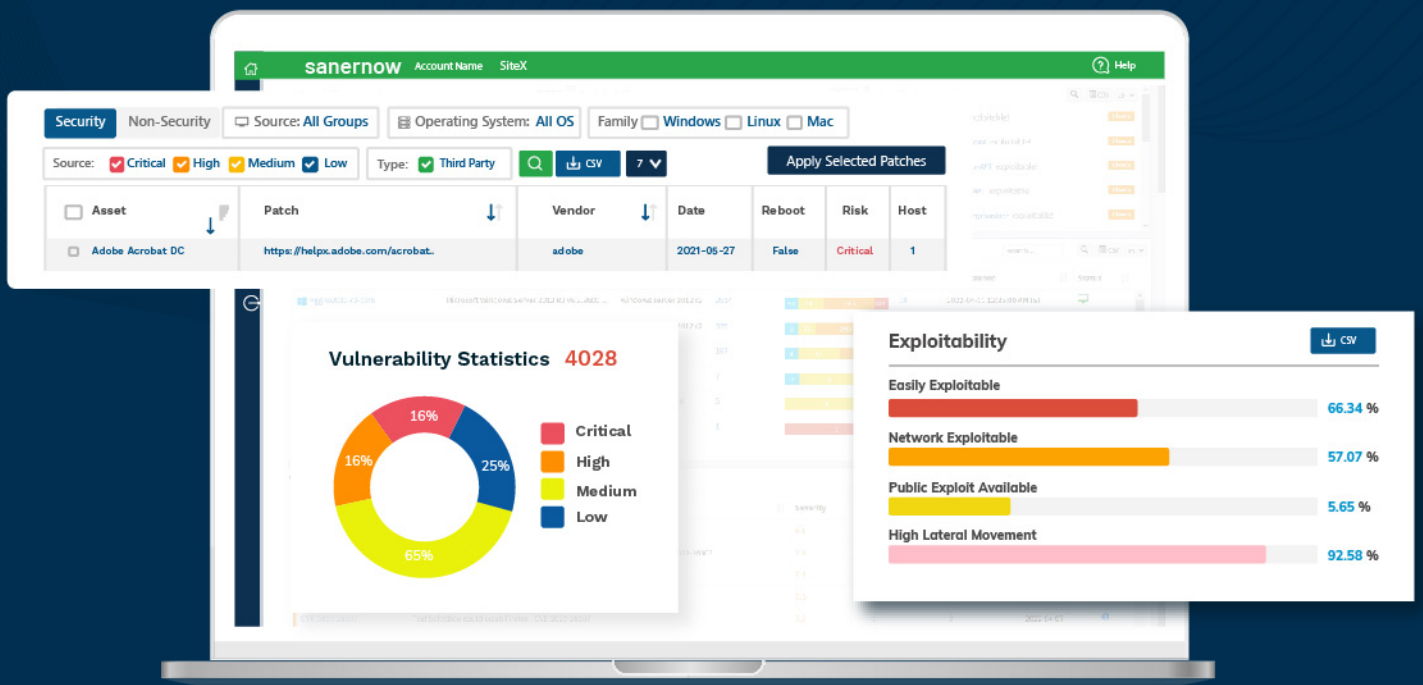


REINVENTING VULNERABILITY MANAGEMENT



SanerNow Continuous Vulnerability & Exposure Management
for Modern IT Security Teams to Achieve Continuous Security
Risk and Compliance Posture

Attack surfaces have become massive, and the security landscape is significantly different from how it was in the past. Yet, vulnerability management has not undergone any reinvention in the last two decades. The traditional vulnerability management solutions still depend on siloed interfaces and focus only on software vulnerabilities, missing out on other crucial security risks. These conventional solutions provide only superficial visibility into infrastructure with insufficient actionable insights. They also lack the capability to remediate vulnerabilities, leaving security and IT teams in dilemma of who will remediate.

For today's complex security landscape, managing software vulnerabilities is good but not sufficient to combat the rising cyberattacks. And relying on multiple tools for managing vulnerabilities makes it an even more complex and a challenging process. To add to this, around 50 to 70 new vulnerabilities are discovered every day, expanding the horizon of vulnerabilities. And 90% of preventable cyber attacks are still happening as prevention processes like vulnerability management is not continuous and automated.



Multiple Solutions and Siloed Interfaces



Lack of Integrated Remediation



Superficial Visibility to IT with poor insights



Vulnerabilities beyond CVEs are being overlooked

IT security teams need a continuous vulnerability and exposure management solution that automatically manages vulnerabilities, exposures, anomalies, and security risks from a centralized console to achieve continuous and automated prevention of cyberattacks at a radical speed.



The New Age Vulnerability Management Solution Built for the Modern Security Landscape

Manage Vulnerabilities and other Security Risks Under One Roof

Manage vulnerabilities, misconfigurations, hidden IT assets, deviation in security controls, and numerous security risks under one roof. Eliminate the complexities of traversing across a maze of tools, and oversee everything from one place.

One Powerful, Lightweight, Multifunctional Agent for All Tasks

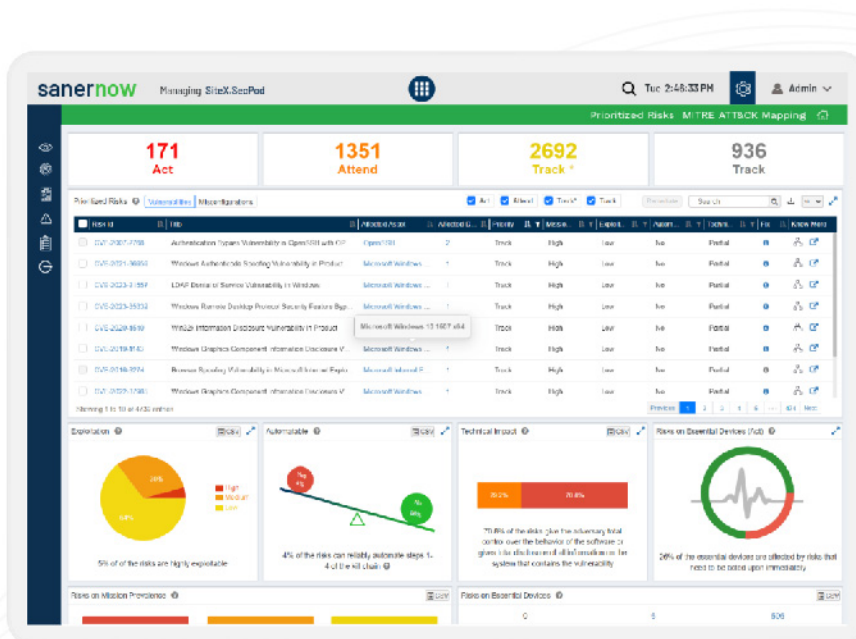
Implement all tasks from detection to remediation with one lightweight, powerful agent. Eliminate the complexities of installing multiple agents to execute different functions. The agent also takes up the role of network scanner and helps save costs on additional hardware.

Best-in-class Vulnerability Management with the Most Trusted Security Intelligence

Powered by our homegrown world's largest security intelligence feed with 175,000+ vulnerability checks.

Experience the Leading Edge of Security Innovation

Leverage machine learning, statistical analysis, and deviation computation methods to get holistic visibility over IT. Automate anything and everything while managing vulnerabilities and risk, and keep your hands free from manual routines.





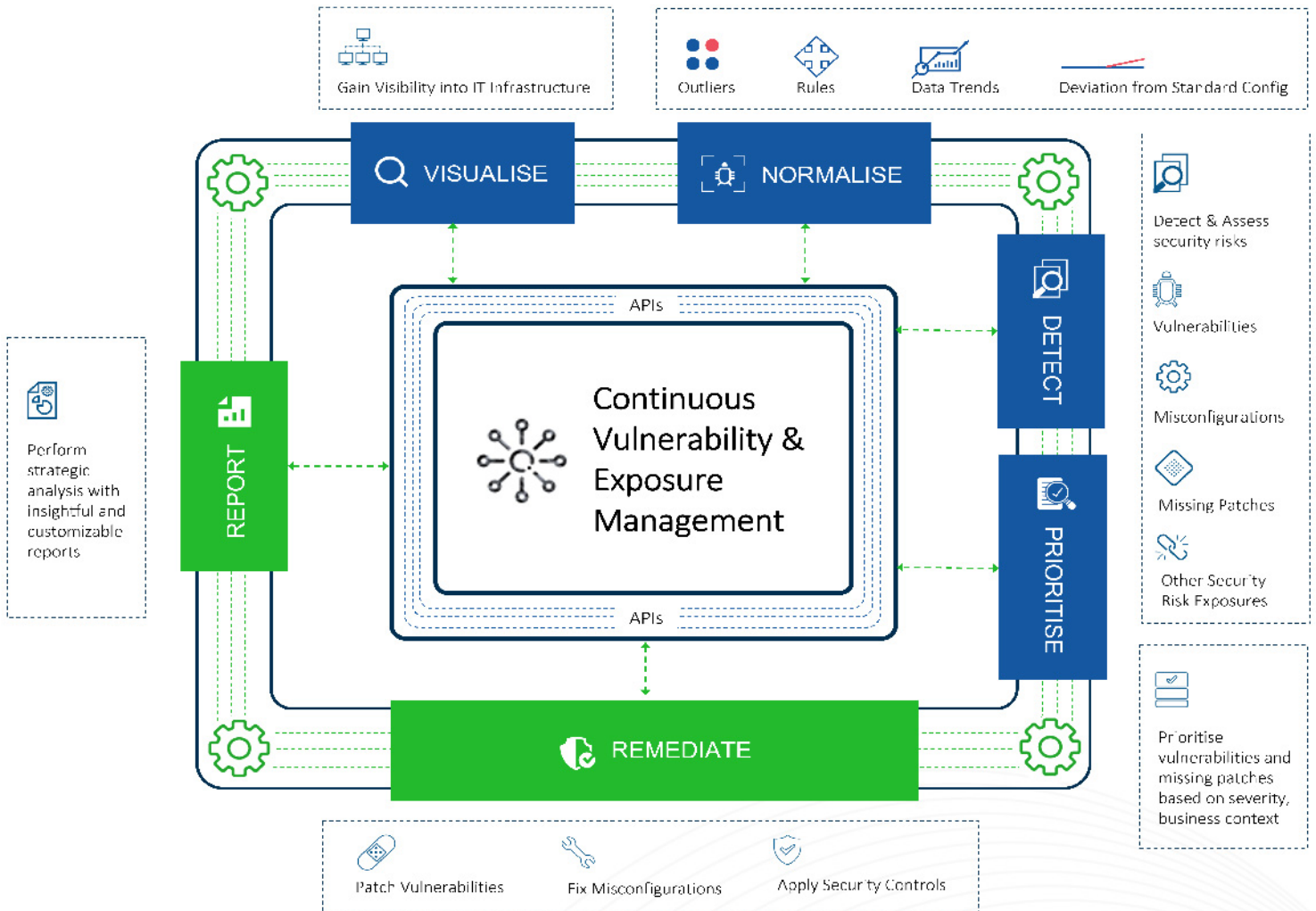
Robust, Natively Built, and Truly Integrated Solution

SanerNow CyberHygiene Platform is completely built in-house to provide a truly integrated solution.



Industry's Fastest and Continuous Scanning

Run the industry's fastest vulnerability scans in under 5 minutes. Rapidly detect exposures, misconfigurations, IT assets, deviations in security controls, and more.



Integrated, Automated, Continuous Vulnerability & Exposure Management for Risk-free IT Operations



👁 Continuous Monitoring of IT Asset Exposure

Perform continuous IT asset scans and gain complete visibility over your computing environment.

🔄 Seamless Security risks prioritization

Manage and prioritize security risks detected based on their business context, exploitability level, and more through advanced vulnerability intelligence.

👁 Take control over Most Obvious Attack Vectors

Manage and prioritize security risks detected based on their business context, exploitability level, and more through advanced vulnerability intelligence.

🔄 Real-time Detection of Vulnerabilities, Exposures, and Security Risks

Continuously detect vulnerabilities, exposures, anomalies, misconfigurations, and security risks in real time and assess them thoroughly.



Timely Remediation with Integrated Patching

Remediate vulnerabilities on time with integrated patching without leaving any security gaps



System Hardening and Conformance with Top Industry Security Policies

Harden system configuration and achieve compliance with major industry benchmarks such as HIPAA, PCI, ISO, NIST and even custom policies.



Remediation Controls Beyond Patching to Eliminate Attack Surface

Go beyond patching and leverage remediation controls to mitigate numerous security risks.



Insightful and Customizable Reports

Utilize a wide range of customizable reports, 50+ trending reports, comprehensive Risk Assessment report, and Insightful Patching Impact report to make reporting and analysis easy.

The screenshot displays the sanernow security dashboard with several key components:

- Top Navigation:** Account Name, SiteX, Help, and buttons for Prioritized Risks and MITRE ATT&CK Mapping.
- Visibility Section:** A 'Device Universe' donut chart showing 78 Total Devices, with a breakdown by OS: Windows, Linux, MacOS, and Network.
- Vulnerable Devices & Statistics:** A filterable table with columns for Asset, Patch, Vendor, Date, Reboot, Risk, and Host.











Asset	Patch	Vendor	Date	Reboot	Risk	Host
<input type="checkbox"/>	Adobe Acrobat DC	adobe	2021-05-27	False	Critical	1
<input type="checkbox"/>	Apache Supersession	apache	2021-06-17	False	Critical	1
- Top Vulnerabilities:** A table listing vulnerabilities by ID, Assets, and Hosts.

ID	Assets	Hosts
USN-4757-1	USN-4757-1 wpasupplicant	1
USN-4691-1	tar	1
USN-4754-1	python3.6-minimal	1
USN-4754-1	python3.6	1
USN-4757-1	wpasupplicant	1
USN-4691-1	tar	1
USN-4754-1	python3.6-minimal	1
USN-4754-1	python3.6	1
- Schedule a Patch Task:** A form for creating automation rules with fields for Pre-remediation script, Post-remediation script, Task Name, Patching Activity Notification, Post Patching Activity Notification, and Groups to apply. Buttons for 'Create Automation Rule', 'Back', and 'Cancel' are at the bottom.

"SanerNow is an all-in-one tool for ITOps/Security professionals. It has a huge list of features that make every IT Ops and Security guy happy. Moreover, it is more than affordable compared to other tools coming from "big" guys. It has multi-OS & 3rd Party Centralized Patch Management (Win, macOS, Linux-multiple distros), Continuous Vulnerability Management, Compliance Management, Asset Management, Endpoint Management, Endpoint Query, and Response. In addition, ease of use and complete visibility are the top two features that solve most IT security issues. SanerNow is extremely useful to support environments with a 100% remote workforce."

- Chief Information Security Officer

Key Benefits

-  Cloud-based Platform
-  Easy Setup
-  Cost-Efficient & Time Saving
-  Effective Risk Exposure Reduction
-  Improved Resource Efficiency
-  Comprehensive & Customisable Reporting
-  Cyber Hygiene Score
-  Agent-less Support
-  Proof of Detection for Detected Risks
-  Device Tagging

INDUSTRY RECOGNITION, KEY CUSTOMERS AND PARTNERS



500+ CUSTOMERS

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 CyberHygiene 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.

193,641

Total Security Checks Covered

81855

Total Vulnerabilities Covered

1143

Publicly Known Exploit Kits Covered

24-48 HRS

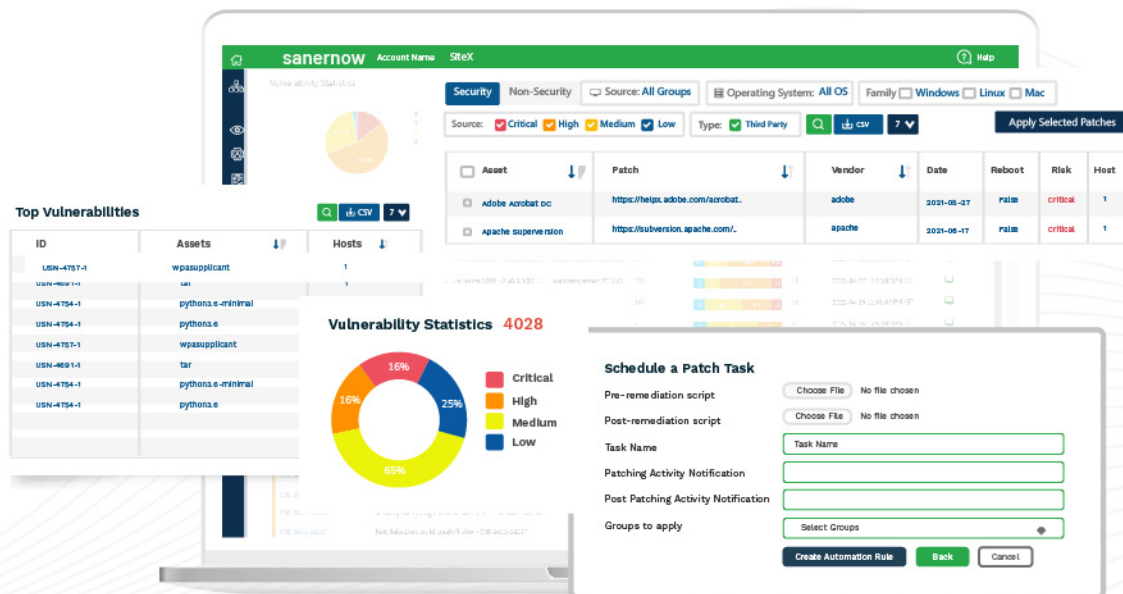
Time Taken to Cover New Vulnerabilities

552

Operating Systems Supported

19704

Platforms & Products Supported



CONTACT US

info@secpod.com / www.secpod.com