secpod

REINVENTING VULNERABILITY MANAGEMENT

SANER CVEM Vulnerability Management

VULNERABILITY STATISTICS CSV ⤓

5832

High 3488 59.7%

35%
59.7%

- Critical
- High
- Medium
- Low

EXPLOITABILITY CSV ⤓

Easily Exploitable 55.67%

Network Exploitable 32.30%

High Lateral Movement 58.89%

HIGH FIDELITY ATTACKS CSV ⤓

10.71% devices are **4 assets** exploitable **Fortinet Products Active Exploits**

3.57% devices are **1 asset** exploitable **Forbook Malware**

3.57% devices are **1 asset** exploitable **Follina**

14.29% devices are **3 asset** exploitable **Firefox Active Exploits**

DETAILS ON EXPLOITABILITY Risk Count on Devices

Host Name	Operating System	Risk Count	Severity Distribution	Assets	Status
windows2022-demo-test1	Microsoft Windows Server 2022 v21H2 archit...	1620		2	☑ ✓
secpod-ubuntu-22	Ubuntu v22.04 architecture x86_64	639		70	☑ ✓
custom-demo-oracle-linux-8-10-s004	Oracle Linux v8.10 architecture x86_64	452	Low 6/ Medium 339/ High 255/ Critical 39	40	☑ 🚀
demo-debian12	Debian v12.6 architecture x86_64	370		67	☑ ✓

VULNERABILITY BY GROUP Vulnerability Count

Groups
- Windows server 2022
- Ubuntu
- Oracle Linux
- General Purpose
- Approved Patch

APPROVED PATCH Vulnerability Count 2751

0   1000   2000   3000

Vulnerabilities

TOP REMEDIATION Fix Patches

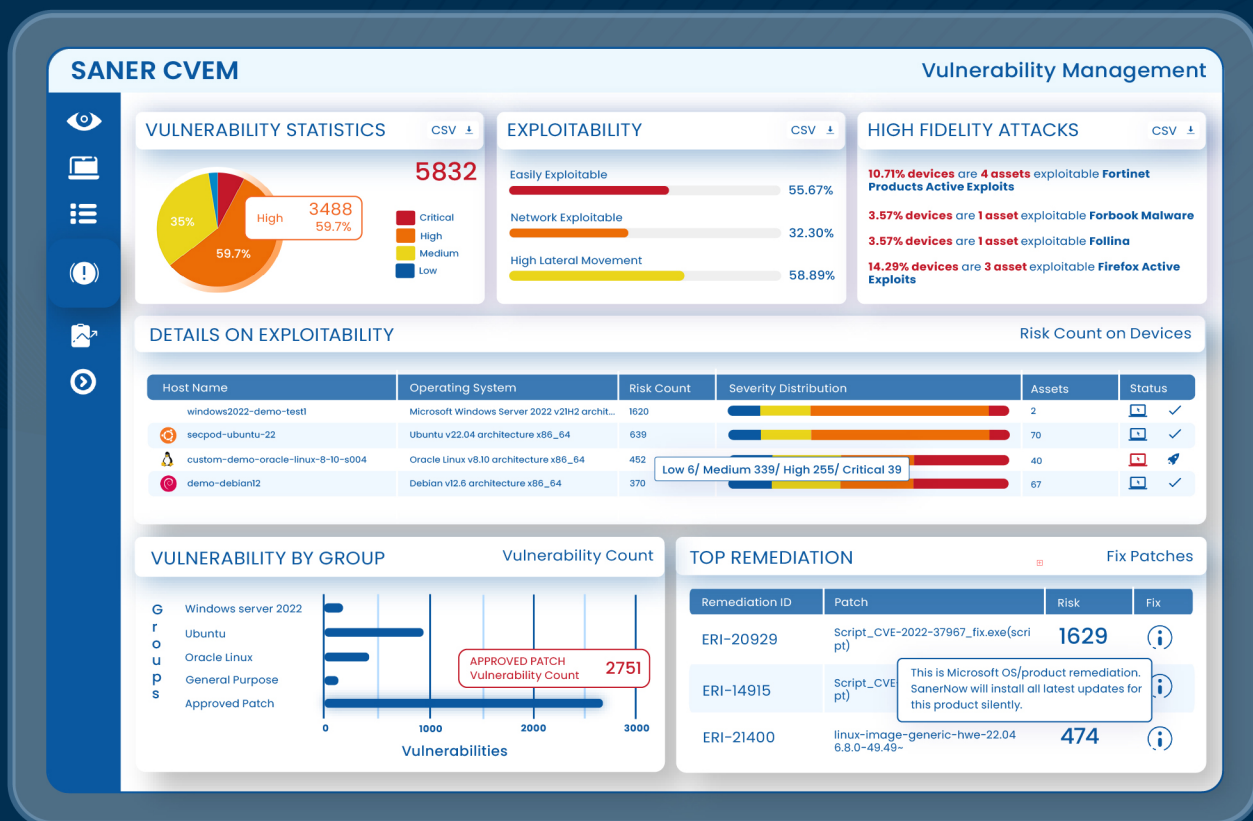| Remediation ID	Patch	Risk	Fix
ERI-20929	Script_CVE-2022-37967_fix.exe(script)	1629	ⓘ
ERI-14915	Script_CVE...pt)	This is Microsoft OS/product remediation. SanerNow will install all latest updates for this product silently.	ⓘ
ERI-21400	linux-image-generic-hwe-22.04 6.8.0-49.49~	474	ⓘ

Saner 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

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

Saner CVEM Cyber Hygiene Platform is completely built in-house to provide a truly integrated solution.
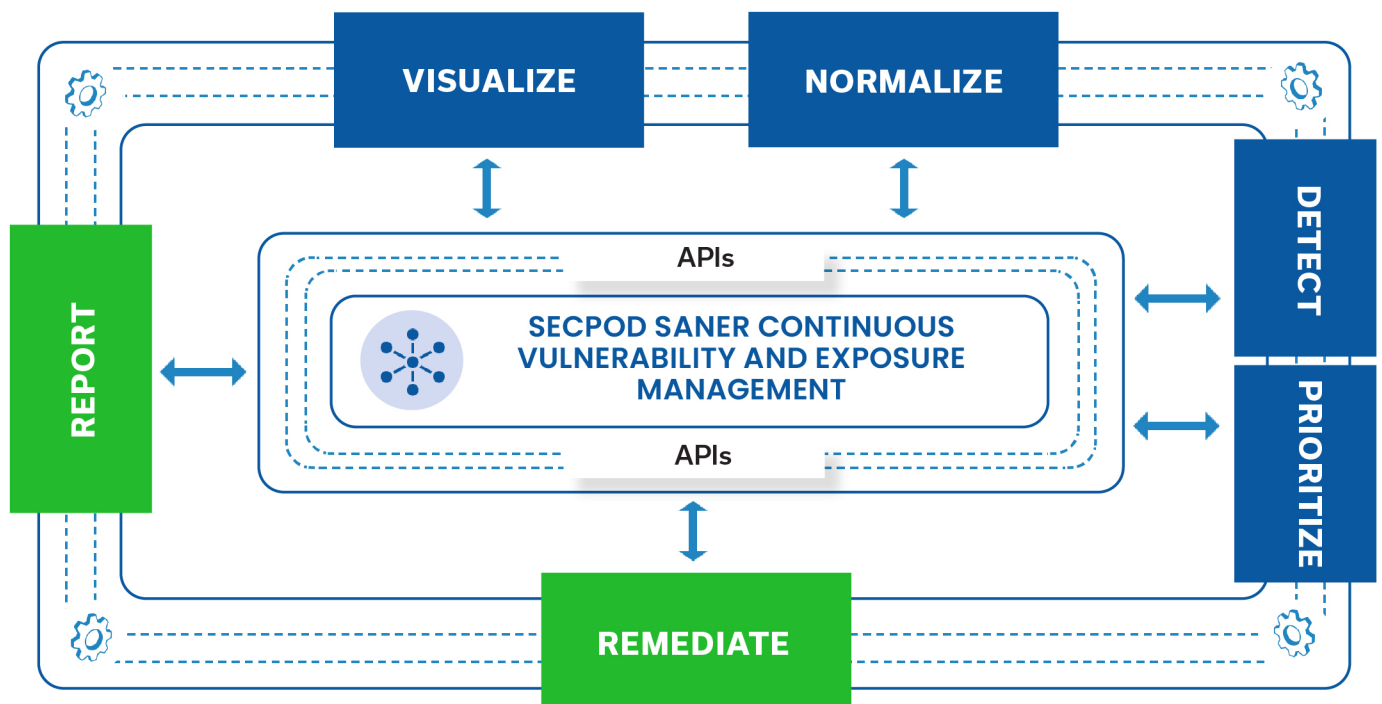
Industry's Fastest and Continuous Scanning

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

Saner Continuous Vulnerability and Exposure Management Framework

The Saner CVEM framework adopts a "weakness perspective." It continuously scans your organization's network, identifying and addressing vulnerabilities in real time. Further, Saner CVEM provides unmatched visibility into your network, enabling swift action to reduce and prevent potential attacks.

Improved Scope of Risk Coverage

With the Weakness Perspective, CVEM scans for all potential risks in your network, drastically increasing the scope and width of risk coverage. The coverage includes software vulnerabilities, misconfigurations, asset exposures, posture anomalies, and other potential risks.
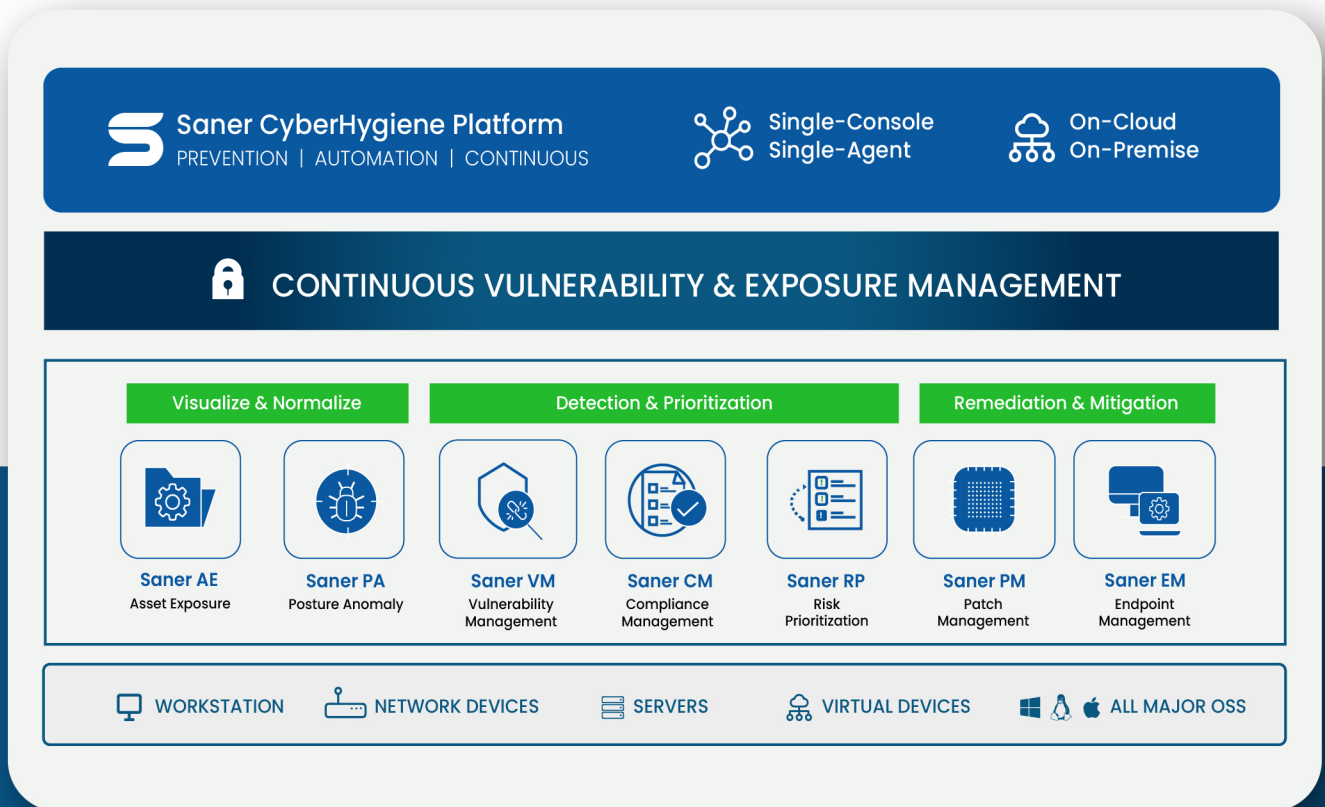
Integrated Prioritization, Remediation and Mitigation

By integrating vulnerability scanners, prioritization methods, and remediation solutions, CVEM drastically improves the speed of detection, prioritization, and mitigation of risks. This further enhances the overall effectiveness and speed of your weakness/risk management process.

Continuity and Automation

Vulnerabilities and risks pop up daily, so continuous and real-time monitoring and response are necessary. By using natively integrated modern scanning and remediation tools, CVEM drastically improves the effectiveness of the detection and remediation process. Furthermore, it also upgrades your organization's ability to respond to newly detected risks.

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

Saner CyberHygiene Platform
PREVENTION | AUTOMATION | CONTINUOUS

Single-Console Single-Agent

On-Cloud On-Premise

CONTINUOUS VULNERABILITY & EXPOSURE MANAGEMENT

Visualize & Normalize		Detection & Prioritization			Remediation & Mitigation	
Saner AE Asset Exposure	**Saner PA** Posture Anomaly	**Saner VM** Vulnerability Management	**Saner CM** Compliance Management	**Saner RP** Risk Prioritization	**Saner PM** Patch Management	**Saner EM** Endpoint Management

WORKSTATION   NETWORK DEVICES   SERVERS   VIRTUAL DEVICES   ALL MAJOR OSS

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

Gain holistic visibility over IT infrastructure. Discover and eliminate posture anomalies that threaten security.

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.
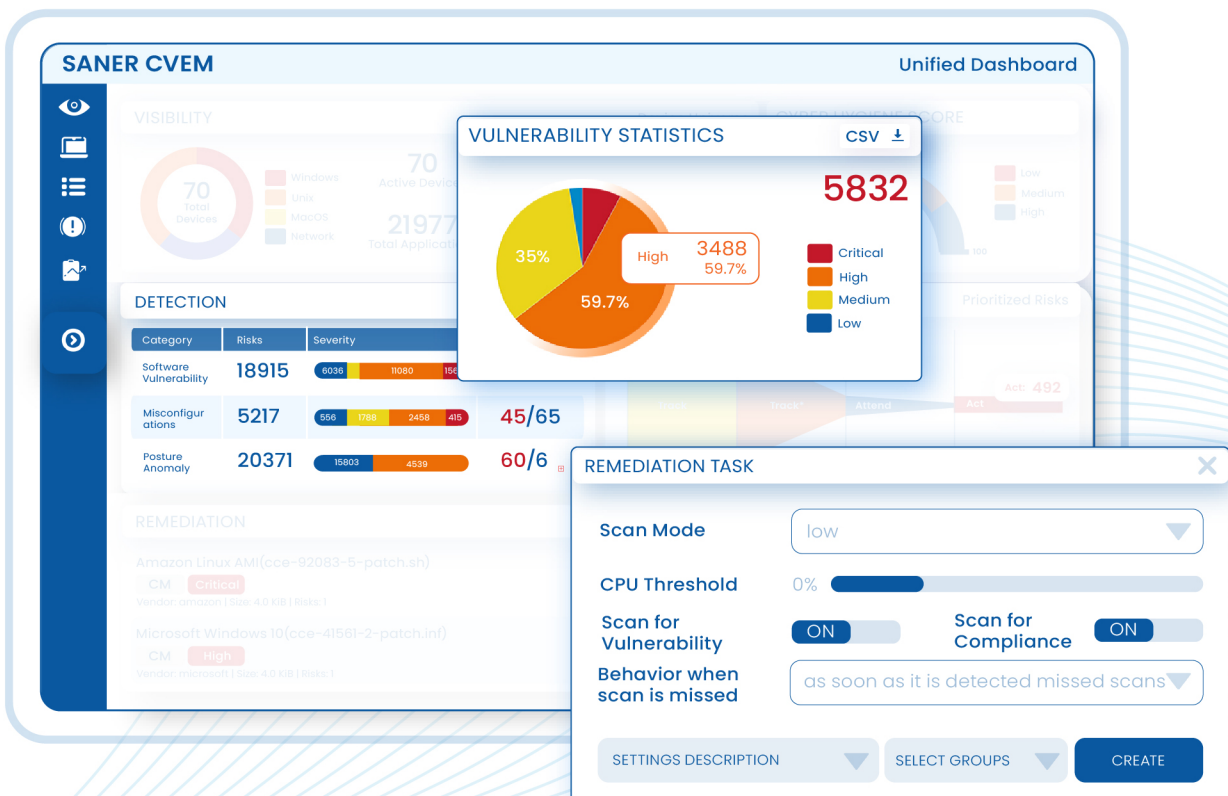
"SanerNow is an all-in-one tool for ITOps/ Security professionals. It has a huge list of features that make every IT Ops and Security guy happy. Moreover, it is more than affordable compared to other tools coming from "big" guys. It has multi-OS & 3rd Party Centralized Patch Management (Win, macOS, Linux-multiple 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 Features

- ☁ 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

Gartner **peer**insights™ **4.4**/5 | G2 CROWD **4.5**/5 | ◥ Capterra **4.5**/5

GIGAOM RADAR REPORT **LEADER** 2024

High Performer WINTER 2024

Momentum Leader WINTER 2024

Best Est. ROI WINTER 2024

Best Support WINTER 2024

Easiest Setup WINTER 2024

FROST & SULLIVAN GLOBAL VULNERABILITY MANAGEMENT ENTREPRENEURIAL COMPANY OF THE YEAR AWARD 2023

SirionLabs SIEMENS Healthineers POS Aviation Bealls INC. aruba kotak Kaizen AUTOMOTIVE GROUP

pricol amagi marlabs driving digital agility ALZAYANI INVESTMENTS SapphireFoods bKash CreditAccess™ Grameen

mic TANIUM SIGNICAST A FORM TECHNOLOGIES COMPANY Sightsavers India FUSE3 excelra

─── **500+ CUSTOMERS** ───

About SecPod

SecPod is a leading cybersecurity technology company committed to preventing cyberattacks through proactive security. Its mission is to secure computing infrastructure by enabling preventive security posture.

At the core of SecPod's offerings is the Saner Platform - a suite of solutions that help organizations establish a strong security posture to preempt cyber threats against end-points, servers, network and cloud infrastructure, as well as cloud workloads. With its cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

193,641 Total Security Checks Covered	**81855** Total Vulnerabilities Covered	**1143** Publicly Known Exploit Kits Covered
24-48 HRS New Vulnerability Coverage in Every	**552** Operating Systems Supported	**19704** Platforms & Products Supported

SANER CVEM — Unified Dashboard

VISIBILITY — Device Universe

- 70 Total Devices
- Windows / Unix / MacOS / Network
- 70 Active Devices
- 21 Inactive Devices
- 49 Operating Systems
- 21977 Total Applications
- 24 Outdated Applications
- 519 User Groups

CYBER HYGIENE SCORE — 47 (Low / Medium / High)

DETECTION — Categorization

Category	Risks	Severity	Affected Devices
Software Vulnerability	18915	6036 / 11080 / 1563	59/67
Misconfigurations	5217	556 / 1798 / 2458 / 415	45/6
Posture Anomaly	20371	15803 / 4539	60/6

PRIORITIZATION — Prioritized Risks

Track → Track* → Attend → Act — Act: 492

REMEDIATION — Remediation Actions

Amazon Linux AMI(cce-92083-5-patch.sh) — CM Critical — Vendor: amazon | Size: 4.0 KiB | Risks: 1 — FIX

Microsoft Windows 10(cce-41561-2-patch.inf) — CM High — Vendor: microsoft | Size: 4.0 KiB | Risks: 1 — FIX

CM Account Name: Product Demo Account — 7zip-patch (Rem Job) — Completed

CM Account Name: UniPod 5 — Immediate Roll back (Rollback) — Completed 1 out of 2

CONTACT US

info@secpod.com / www.secpod.com