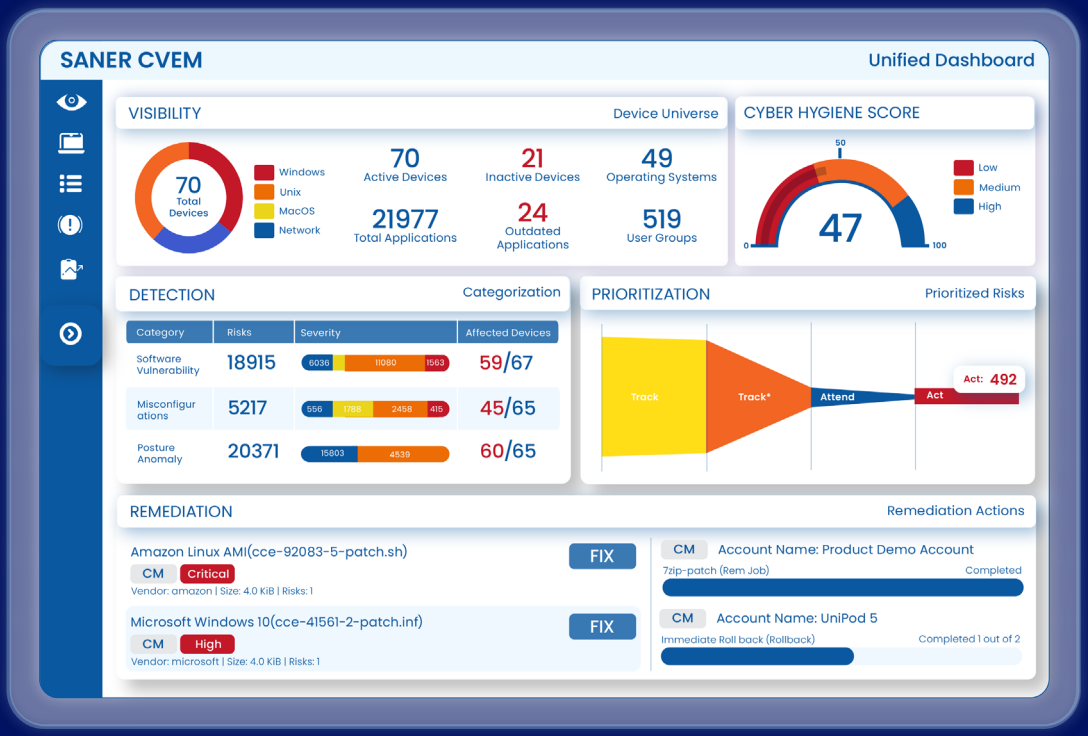
secpod

SANER CVEM



Continuous Vulnerability & Exposure Management to unify asset visibility, normalize posture, prioritize risks, remediate CVEs & Non CVEs, audit ready compliance, and manage endpoints

www.secpod.com

Siloed tools weaken security posture

They can’t prevent attacks

Enterprise environments are powered by thousands of endpoints and servers spread across hybrid infrastructures. These systems are the backbone of business operations and the prime targets for attackers. Yet, vulnerability management for them hasn’t evolved at speed.

Legacy solutions can’t keep up

Traditional vulnerability management tools rely on siloed interfaces and detect only software-level issues. They miss critical risks like misconfigurations, weak credentials, and outdated system components that often become easy entry points for attackers.

Limited remediation. Fragmented workflows

Legacy tools offer little automation and no built-in remediation, leaving security and IT teams unclear on ownership and next steps.

Limited visibility. More risk exposure

Traditional tools provide shallow insights into endpoint and server exposure. They force IT and security teams to use multiple tools to scan, prioritize, remediate, and comply, leaving systems exposed.

Fragmented risk. Contextless prioritization & compliance drift

Siloed tools offer separate vulnerability, posture, and compliance data. They offer context-unaware risk prioritization that ignores asset criticality, exploitability, and business impact. IT, security, and compliance teams have to collate findings across tools, creating duplicate work, unclear ownership, and audit gaps. That leaves them chasing low-impact issues while high-risk ones remain unaddressed.

With new vulnerabilities surfacing daily, and 90% of preventable breaches still exploiting known weaknesses, reactive and tool-fragmented approaches no longer work.

Saner CVEM

Prevent Attacks Continuously. Reduce Risks at Scale.

IT security teams need an integrated, continuous vulnerability and exposure management platform to manage risks and threats through a centralized cloud console.

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.

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.

Predictable vulnerability management with the most trusted security intelligence

Powered by SecPod's unified security intelligence with over 200,000 security checks

Smarter security with AI and ML

Leverage artificial intelligence, machine learning, statistical analysis, and deviation computation methods to get holistic visibility over IT. Automate managing vulnerabilities and risks, and keep your hands free from manual routines.

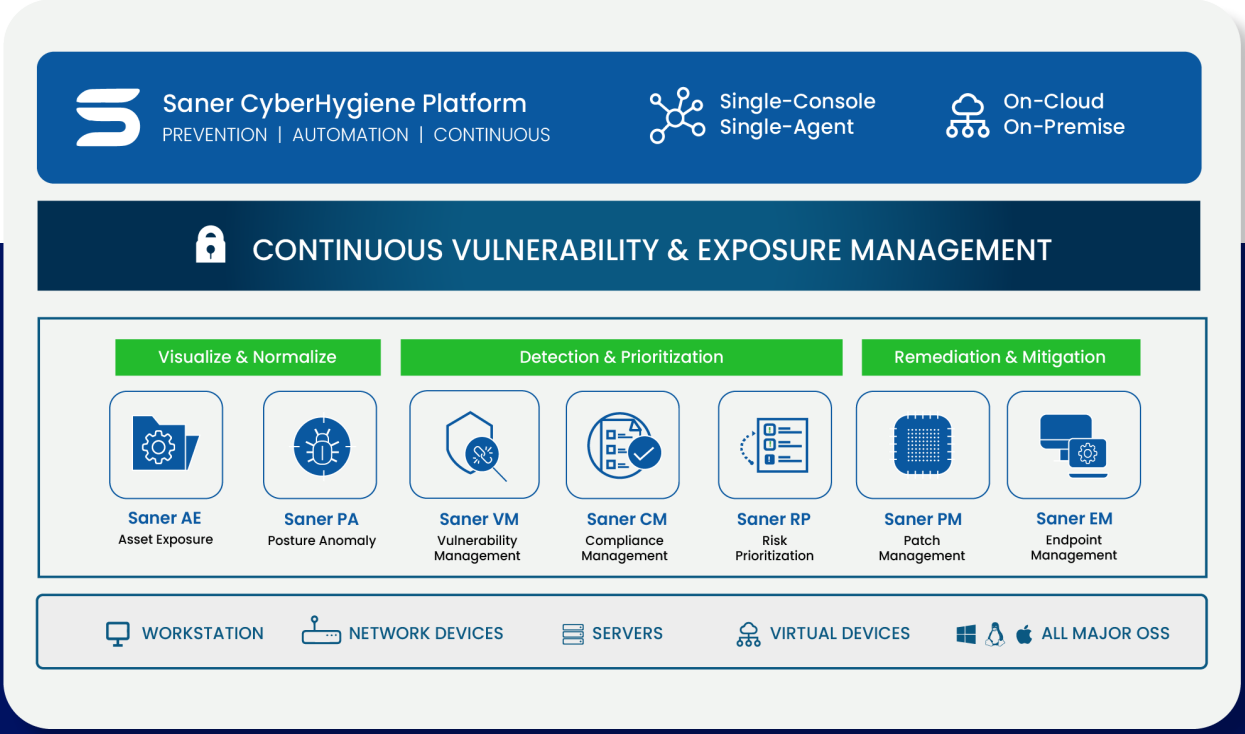
Robust, natively built, and truly integrated solution

The Saner CVEM Cyber Hygiene Platform is developed natively and completely in-house to deliver a truly integrated experience, eliminating silos, for enterprise-grade cyber hygiene and risk management.

Industry's fastest and continuous scanning

Run the industry's fastest vulnerability scans in under 5 minutes. Rapidly detect exposures, misconfigurations, IT assets, missing patches, deviations in security posture across endpoints and network infrastructure.

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



SANER AE – ASSET EXPOSURE

Continuously discovers and normalizes every asset across hybrid environments to expose hidden and unmanaged systems.

- Inventory of endpoints, servers, virtual machines, and network devices across OS platforms.
- Correlates assets with vulnerabilities, configurations, and compliance posture to remove blind spots.

SANER PA – POSTURE ANOMALY

Detects configuration drifts, weak controls, outliers, and security misalignments to maintain a consistent, hardened system posture.

- Continuously benchmarks endpoints against secure configuration baselines and detects privilege escalations or policy violations.
- Enables instant remediation of deviations, unwanted devices, services, connections, or processes, to sustain system integrity.

SANER VM – VULNERABILITY MANAGEMENT

Performs continuous, high-speed scans across all assets to detect and correlate vulnerabilities with unified security intelligence.

- Detects OS and third-party application vulnerabilities using unified security intelligence, world's largest security database with more than 200,000 checks.
- Delivers continuous vulnerability visibility and precise exposure assessment across hybrid infrastructures.

SANER CM – COMPLIANCE MANAGEMENT

Maps system configurations to regulatory benchmarks, delivering continuous compliance visibility and reporting.

- Automates compliance checks against CIS, NIST, ISO, PCI-DSS, CMMC, HIPAA and custom frameworks.
- Provides continuous compliance drift detection, remediation tracking and audit-ready reports.

SANER RP – RISK PRIORITIZATION

Leverages the SSVC risk prioritization framework to correlate vulnerabilities and asset criticality to dynamically prioritize risks

- Combines CVSS, exploit intelligence, asset value, and EPSS data to predict the likelihood of exploitation and rank risks by business impact.
- Applies decision-tree logic to deliver consistent remediation decisions by evaluating exploit status, exposure, and mission relevance.

SANER PM – PATCH MANAGEMENT

Automates patch detection, deployment, and verification across Windows, macOS and Linux operating systems and 550+ third-party applications

- Continuously scans for missing patches and validates successful deployments.
- Supports automated patch rollout with rollback & reduces mean time to remediate.

SANER EM – ENDPOINT MANAGEMENT

Provides unified control for system health and configurations and security status

- Enables centralized command execution, software deployment, remote access and policy enforcement.
- Create and deploy custom scripts for targeted actions such as disabling a service, incident management, blocking applications, managing zero-day vulnerabilities, etc.

Key Features

Continuous monitoring of IT asset exposure

Perform continuous IT asset scans and gain complete visibility over your computing environment. Identify every connected asset, open port, and running service across Windows, Linux, macOS, and AIX to get exposure insights.

Seamless security risk prioritization

Manage and prioritize vulnerabilities based on their business context and exploitability level through unified security intelligence. Enables context-driven vulnerability correlation, ensuring that the most business-critical risks are automatically surfaced and acted upon first.

Take control over the most obvious attack vectors

Gain holistic visibility over IT infrastructure. Discover and eliminate posture anomalies that threaten security. Test-and-deploy workflows and approval controls to ensure only validated remediations are applied, reducing operational risk and blocking potential attacker entry points before they are exploited.

Timely remediation with integrated patching

Remediate vulnerabilities on time with integrated patching without leaving any security gaps. Leverage automation workflows and centralized time scheduling to patch and remediate across global endpoint, aligned with defined SLAs and verified for completeness before deployment.

System hardening and conformance

Harden system configurations and achieve compliance with major industry benchmarks such as HIPAA, PCI, ISO, and NIST, as well as custom policies. Remote automation scripting and role-based approvals to enforce hardening policies and control checks across all systems

Insightful and customizable reports

Utilize a wide range of customizable reports, 50+ trending reports, comprehensive risk assessment reports, and insightful patching impact analytics to make reporting and analysis easy. Enhanced reporting APIs and advanced filtering by detection or patch release date to offer deeper insights for audit readiness and governance reporting.

"Saner CVEM 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. Saner CVEM is extremely useful to support environments with a 100% remote workforce."

- Chief Information Security Officer

PLATFORM HIGHLIGHTS

- 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 as Evidence
- Device Tagging

INDUSTRY RECOGNITION, KEY CUSTOMERS AND PARTNERS

Gartner peerinsights 4.4/5 | G2 CROWD 4.5/5 | Capterra 4.5/5

GIGAOM RADAR REPORT LEADER 2024 PATCH MANAGEMENT

SUMMER 2025 Best Est. ROI | SUMMER 2025 Fastest Implementation | SUMMER 2025 High Performer | SUMMER 2025 Momentum Leader | SUMMER 2025 Highest User Adoption

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

exela TECHNOLOGIES | SIEMENS Healthineers | POS Aviation | wipro | HPE aruba networking | kotak

Aster Optimise your enterprise | TVS ELECTRONICS | NATIONAL BANK OF EGYPT | PROFICIO | ansa mcal GROUP OF COMPANIES | bKash

bigbasket | Auxiom OUTSMART CHAOS | SIGNICAST A FORM TECHNOLOGIES COMPANY | Sightsavers India | synergi

Kaizen AUTOMOTIVE GROUP | Newberry Group Peak performance. Achieved. | SBI card

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 endpoints, 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.

380,200
Total number of Risk Exposures covered

81855
Total Vulnerabilities Covered

1143
Publicly Known Exploit Kits Covered

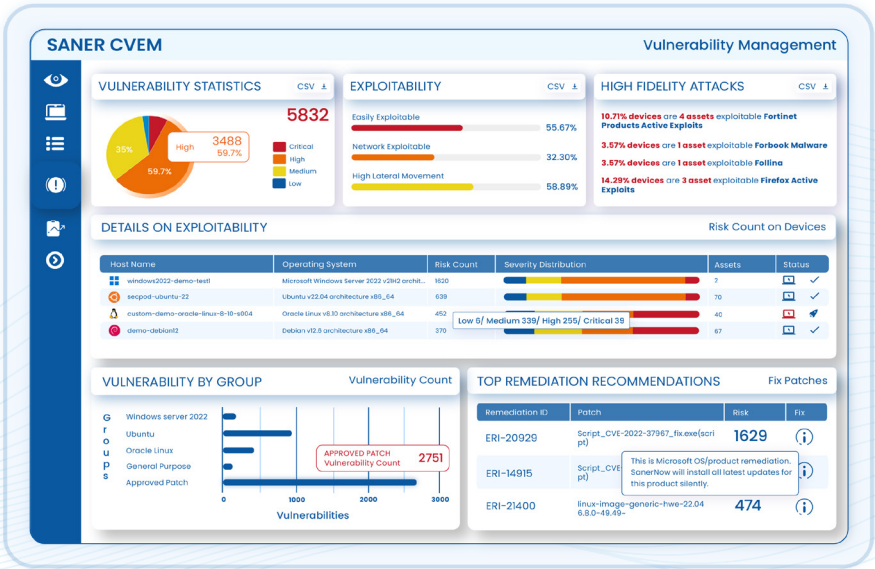
200+
Posture Anomalies Uncovered

24-48 hrs
Speed at which New Vulnerabilities are covered

30000+
Misconfigurations covered

552
Third-party Applications

1189
Platforms & Products Supported



CONTACT US

Contact Us- info@secpod.com | Visit Us- www.secpod.com