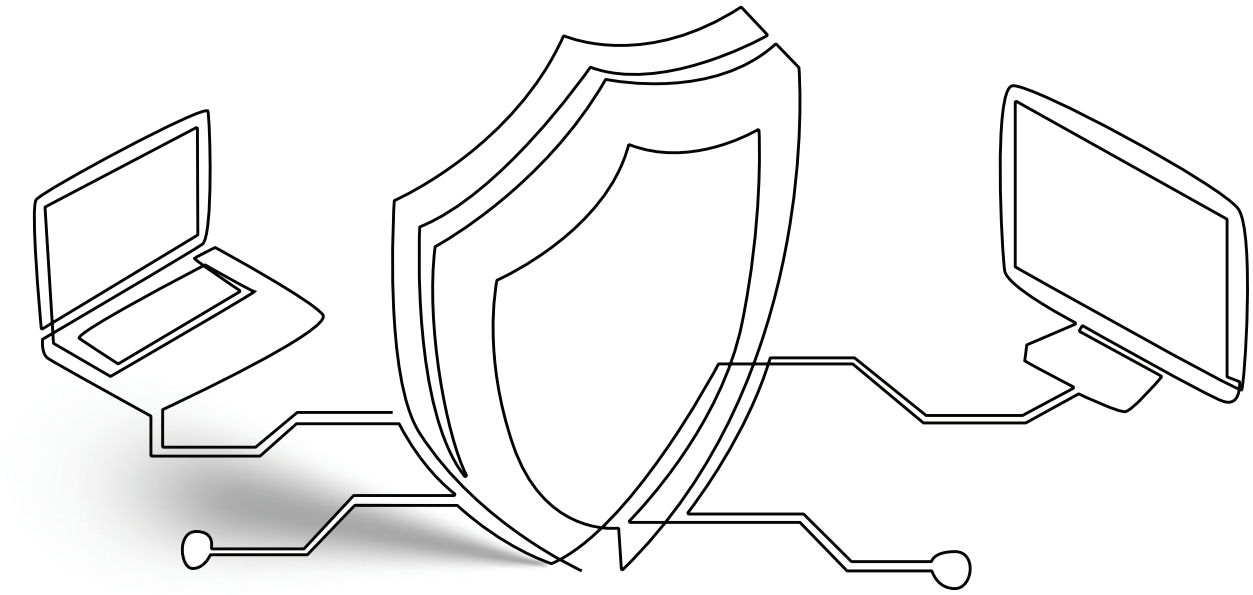
secpod

SANER CVEM



Prevention-first Vulnerability and Exposure Management for unified visibility, prioritization, compliance, and remediation

Saner CVEM unifies asset exposure, posture anomaly detection, vulnerability assessment, compliance management, risk prioritization, patching, and endpoint actions in one dashboard.

Saner CVEM is built to help teams continuously detect, assess, prioritize, and remediate vulnerabilities and other security risks from a unified console.

www.secpod.com

DISCONNECTED SECURITY. INEFFECTIVE WORKFLOWS. WIDER GAPS

When vulnerability management depends on separate scanners, patching tools, compliance tools, and endpoint workflows, visibility narrows, remediation slows, and teams lose time deciding what to fix first. The gap between detection, prioritization, and action grows, which increases operational inefficiencies and leaves more room for cyberattackers to exploit.

Traditional vulnerability management tools

Offer fragmented visibility across assets and software

Endpoint and non-endpoint devices, OS applications, third-party apps, and infrastructure changes are harder to track when vulnerability data sits in separate tools.

Miss out on Risks beyond CVEs

Cyberattackers don't just exploit CVEs. Misconfigurations, exposures, deviations and anomalies need equal visibility that traditional tools just don't provide.

Rely on severity-based prioritization without deeper context

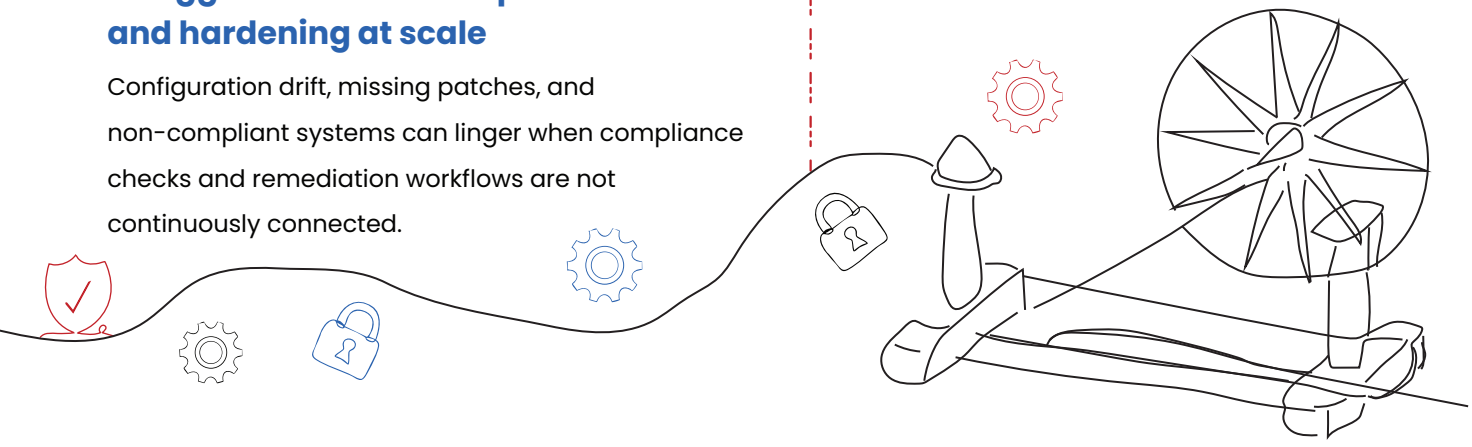
Thousands of findings can pile up fast, and without contextual prioritization, teams may patch what looks urgent instead of what matters most.

Lack integrated remediation, delaying closure

Scanning alone does not reduce risk. When patching and mitigation controls are disconnected from detection, remediation takes longer and ownership gets stretched across teams.

Struggle to sustain compliance and hardening at scale

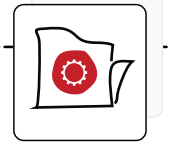
Configuration drift, missing patches, and non-compliant systems can linger when compliance checks and remediation workflows are not continuously connected.



The Saner CVEM Difference

Saner CVEM combines seven powerful modules under one umbrella to provide continuous, automated, and unified vulnerability and exposure management for modern IT environments. It brings visibility, detection, prioritization, and remediation together in one console, with support for cloud or on-premise deployment and remediation across Windows, Linux, macOS, and AIX devices through the Saner Agent.

SANER CVEM



SANER AE

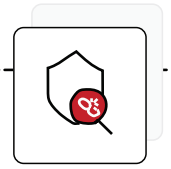
Asset Exposure

Tracks endpoint and non-endpoint assets, OS applications, and third-party applications from a centralized view, helping teams manage asset inventory, and license information.

SANER PA

Posture Anomaly

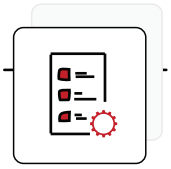
Monitors thousands of device parameters to spot outliers, aberrations, deviations, and unusual security posture that can stay hidden in standard checks.



SANER VM

Vulnerability Management

Runs continuous scans to identify vulnerabilities on devices, organize findings, and support faster assessment and remediation from a centralized console.



SANER CM

Compliance Management

Maps systems to benchmarks such as PCI, HIPAA, ISO 27001, NIST 800-53, and NIST 800-171, monitors deviations, and supports manual or automated fixes.

SANER RP

Risk Prioritization

Uses SSVC-based decisioning to rank the vulnerabilities and misconfigurations that need attention first, with deeper exploitation analysis powered by SecPod's machine-learning algorithm.

SANER PM

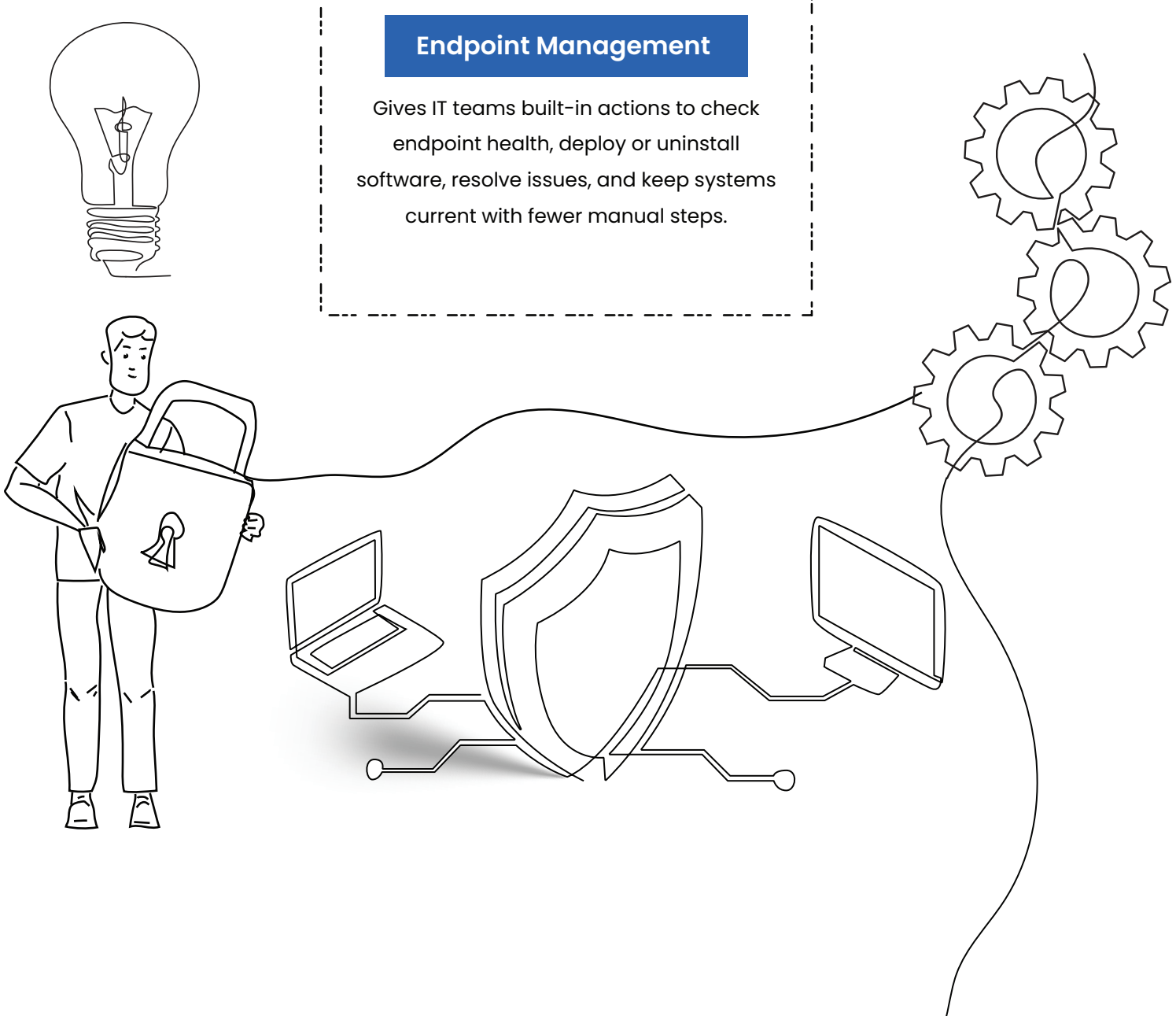
Patch Management

Maps vulnerabilities to tested vendor patches and automates patching from scanning to deployment across major operating systems, firmware, and many third-party applications.

SANER EM

Endpoint Management

Gives IT teams built-in actions to check endpoint health, deploy or uninstall software, resolve issues, and keep systems current with fewer manual steps.



WHY CHOOSE SANER CVEM?

Unified dashboard

with interactive views across visibility, detection, prioritization, and remediation for a single source of truth.

Complete asset visibility

across endpoint and non-endpoint devices, operating system applications, third-party applications, and lifecycle changes.

Continuous risk discovery

with rapid scans, daily-updated risk intelligence, and posture anomaly detection that helps surface outliers and misconfigurations faster.

Continuous compliance management

with built-in templates, customizable profiles, daily checks, and deviation tracking across common frameworks.

Context-driven prioritization

with SSVC categories such as Act, Attend, Track, and Track* so teams can focus on the risks that deserve action first.

Machine-learning-assisted analysis

to identify deeper risk patterns, detect unusual posture, and support smarter remediation decisions.

Integrated patching & remediation

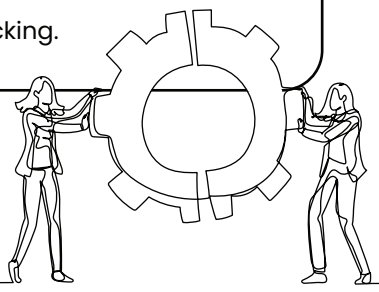
with vulnerability-to-patch mapping, automated deployment workflows, and endpoint actions from the same ecosystem.

Customizable, audit-ready reporting

for security, IT, and compliance teams that need clearer evidence and easier tracking.

Flexible deployment

on cloud or on-premise, with remediation support across Windows, Linux, macOS, and AIX environments.



SecPod is a leading cyber security 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.

Our Clients and Reach

SecPod is trusted by enterprises and MSPs across Finance, Healthcare, IT, Government, and Manufacturing operating across 100+ countries.

Website: www.secpod.com

Email: info@secpod.com

Experience preventive, automated, and intelligent security.