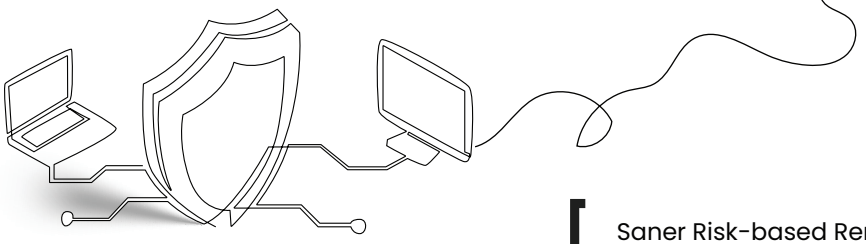
secpod

SANER

RISK-BASED REMEDIATION



Prevention-first remediation for complete attack surface reduction and mitigation

Saner Risk-based Remediation combines risk mitigation capabilities of Saner Platform into a single solution to mitigate risks, close potential gaps and minimize your attack surface. For you cloud AND endpoint infrastructure.

Detecting vulnerabilities and misconfigurations is only the beginning. Saner Risk-based Remediation help teams continuously remediate risks, mitigate weaknesses, close gaps and prevent cyberattacks from a unified console.

www.secpod.com

SILOED REMEDIATION. WIDER GAPS. IMPENDING CYBERATTACKS.

When remediation is disjointed and visibility is incomplete, gaps in your security posture grows. Letting these risks linger in your network increases the chance for cyberattacks.

But what is the real cost of disconnected and ineffective remediation

Fragmented tools delay action

When patch management, compliance enforcement, endpoint controls, and cloud remediation live in separate tools, remediation slows down and accountability gets stretched thin across teams.

Severity ratings alone don't guide decisions

Without deeper context — exploitability, asset criticality, exposure in the wild — teams patch what looks urgent rather than what matters most, wasting limited remediation capacity.

Compliance drift goes undetected

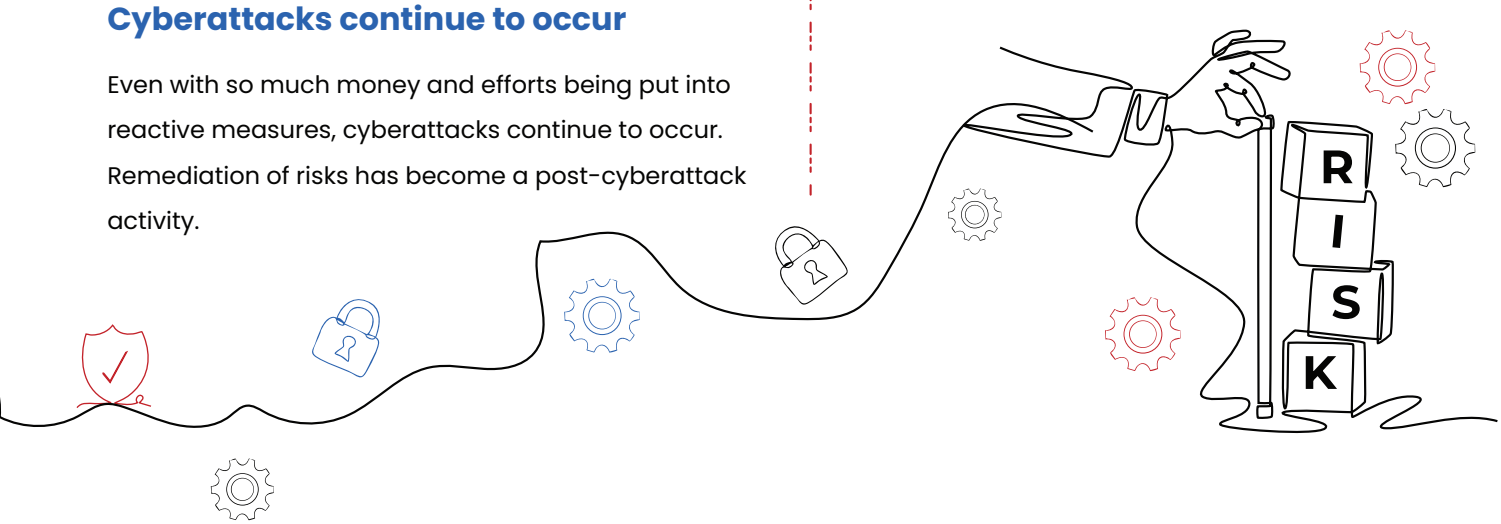
Configuration baselines shift over time. Without continuous checks and automated remediation tied to compliance frameworks, non-compliant systems can linger for weeks or months before audits surface them.

Cloud environments require purpose-built workflows

Traditional endpoint patching tools were not designed for cloud infrastructure. Misconfigurations, over-privileged access, and cloud-native vulnerabilities demand dedicated, policy-aware remediation at cloud scale.

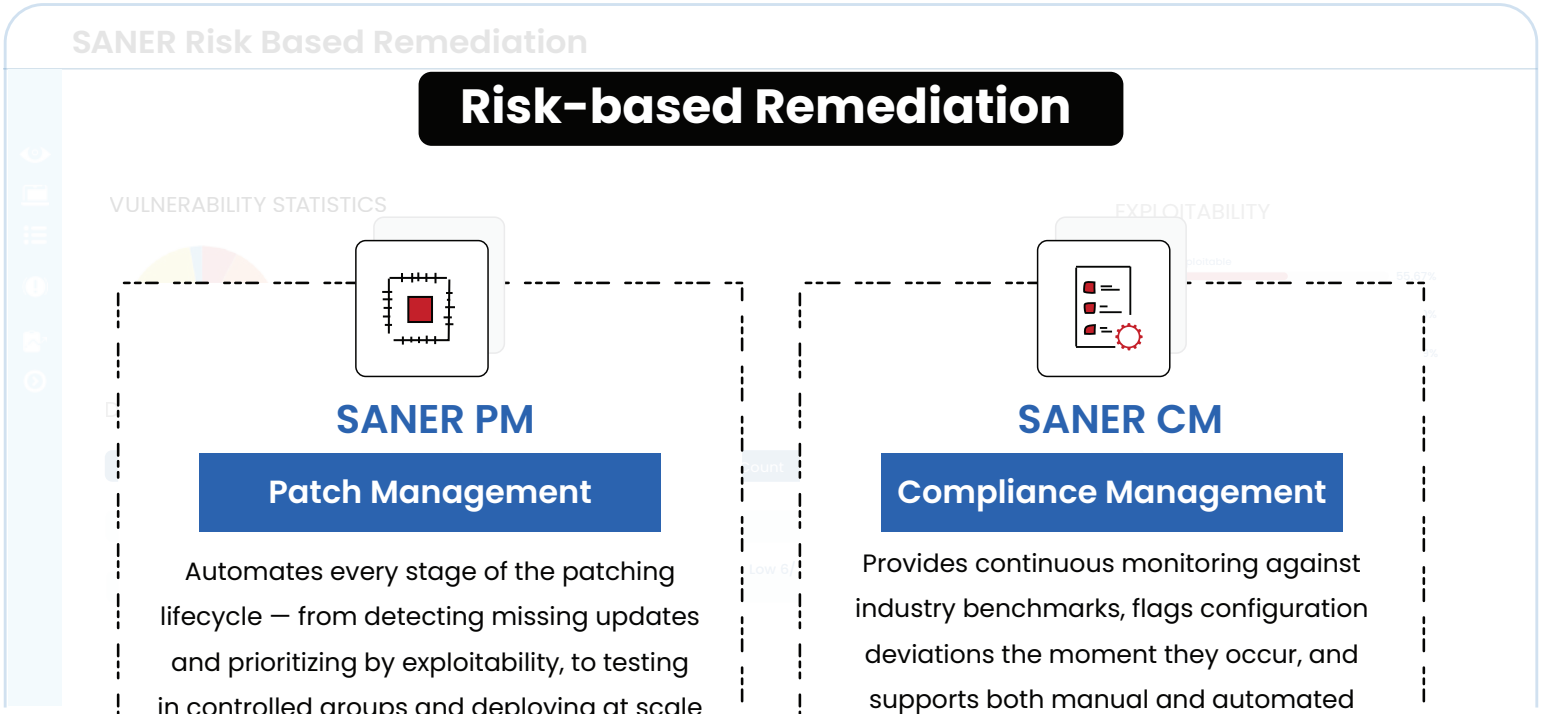
Cyberattacks continue to occur

Even with so much money and efforts being put into reactive measures, cyberattacks continue to occur. Remediation of risks has become a post-cyberattack activity.



The Saner Risk-based Remediation Difference

Saner Risk-Based Remediation integrates Patch Management, Compliance Management, Endpoint Management, and Cloud Security Remediation Management into a single console. This unification eliminates handoffs, reduces tool sprawl, and accelerating time to closure. And more importantly, it prevents cyberattacks.



SANER PM

Patch Management

Automates every stage of the patching lifecycle — from detecting missing updates and prioritizing by exploitability, to testing in controlled groups and deploying at scale across global, distributed environments.

SANER CM

Compliance Management

Provides continuous monitoring against industry benchmarks, flags configuration deviations the moment they occur, and supports both manual and automated remediation — keeping systems hardened and audit-ready at all times

SANER EM

Endpoint Management

Extends remediation beyond patching, giving IT and security teams built-in controls to manage software, block rogue applications, enforce device policies, and troubleshoot endpoints remotely — all from a centralized console.

SANER CSRM

Saner Cloud Security Remediation Management

Bridges the detection-to-action gap in cloud environments. It integrates directly with Saner Cloud's CSPM, CIEM, and CSPA modules, allowing teams to move from a flagged misconfiguration or over-privileged access issue to a guided remediation workflow in a single click.

WHY CHOOSE SANER RISK-BASED REMEDIATION?

Intelligent Patch Management

Top 10 patch lists, patch aging charts, most-impactful-patches analysis, and grouped remediation turn an overwhelming patch backlog into a structured, prioritized queue.

Context-Driven Prioritization

SSVC-based decisioning (Act, Attend, Track, Track*) combined with risk scoring and ML-assisted analysis ensures teams always fix what matters most — not just what looks urgent.

Integrated Remediation Workflows

Vulnerability-to-patch mapping, automated deployment, approval workflows, and one-click cloud remediation work together in a single ecosystem — eliminating the handoffs that slow closure down.

Continuous Compliance Enforcement

Built-in benchmark templates, daily deviation checks, and automated fix workflows keep systems continuously hardened — not just compliant on audit day.

Broad Platform & Cloud Coverage

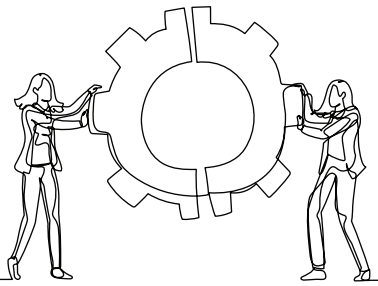
Remediation spans Windows, macOS, Linux, AIX, firmware, 550+ third-party apps, AWS, and Azure — managed from a single console with a shared lightweight agent.

AI-Driven Detection & One-Click Cloud Fixes

Anomaly detection with confidence levels and severity distribution flags risks faster, while one-click remediation and identity entitlement governance close cloud exposure gaps without manual investigation.

Audit-Ready Reporting & Full Traceability

Tool-specific job codes, approval workflows, complete audit logs, and customizable reports give security and compliance teams the evidence they need — and executives the visibility to track progress.



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.