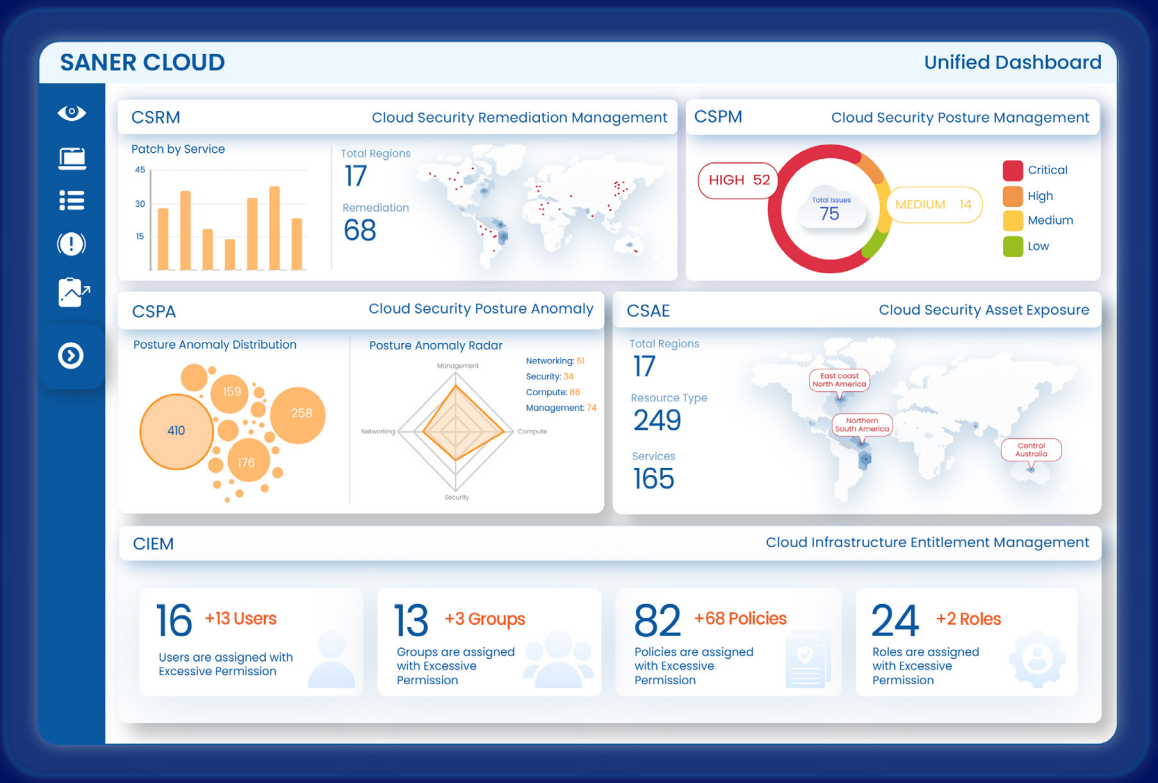
secpod

SANER CLOUD



AI-powered CNAPP Suite for unified visibility, compliance, and remediation

www.secpod.com

Why Cloud Security is Failing?

Visibility is partial, remediation is delayed.

Cloud adoption has transformed the way businesses operate, but it has also introduced new layers of risk. Every virtual machine, container, identity, and policy creates an expanding surface that attackers can exploit.

Organizations often rely on multiple tools for asset discovery, compliance checks, identity governance, and remediation. The use of siloed tools often leads to wider gaps in your cloud security posture. Further, this fragmented approach leaves blind spots, slows response, and increases the chance of a breach.

Offer limited visibility and leave blind spots.

Lack integrated remediation, delaying fixes.

Rely on static compliance checks without anomaly detection.

Struggle with identity sprawl and excessive entitlements.

Misconfigurations, exposed assets, identity misuse, and costly breaches remain constant threats.

Saner Cloud can change it.

It brings all aspects of cloud security together into one AI-powered platform delivering complete visibility, continuous compliance, and automated remediation in a single, unified workflow.

The Saner Cloud Difference

Saner Cloud is an AI-powered and Machine-Learning based Cloud-Native Application Protection Platform (CNAPP) that brings every layer of cloud security into a single solution. It helps organizations discover assets, monitor posture, detect anomalies, govern identities, and automate remediation, all from one unified dashboard.

PREVENTION-FIRST SECURITY

1. Detects vulnerabilities, misconfigurations, asset exposures, deviating security controls, and anomalies before attackers can exploit them.
2. AI-driven insights help prioritize risks, so teams focus on what truly matters.
3. Integrated remediation that ensures continuous compliance.

UNIFIED VIEW ACROSS CLOUD ASSETS

1. One dashboard for AWS, Azure, and cloud environments.
2. Visualize every asset, identity, and configuration in with rapid on-demand scans.
3. No more juggling multiple disconnected cloud consoles.

AUTOMATION THAT SCALES

1. From discovery to remediation, Saner Cloud eliminates manual, repetitive tasks.
2. One-click remediation to shrink exposure windows from weeks to minutes.
3. Automated compliance checks to ensure standards like PCI-DSS, HIPAA, NIST, and CIS are continuously enforced.

AI AT THE CORE

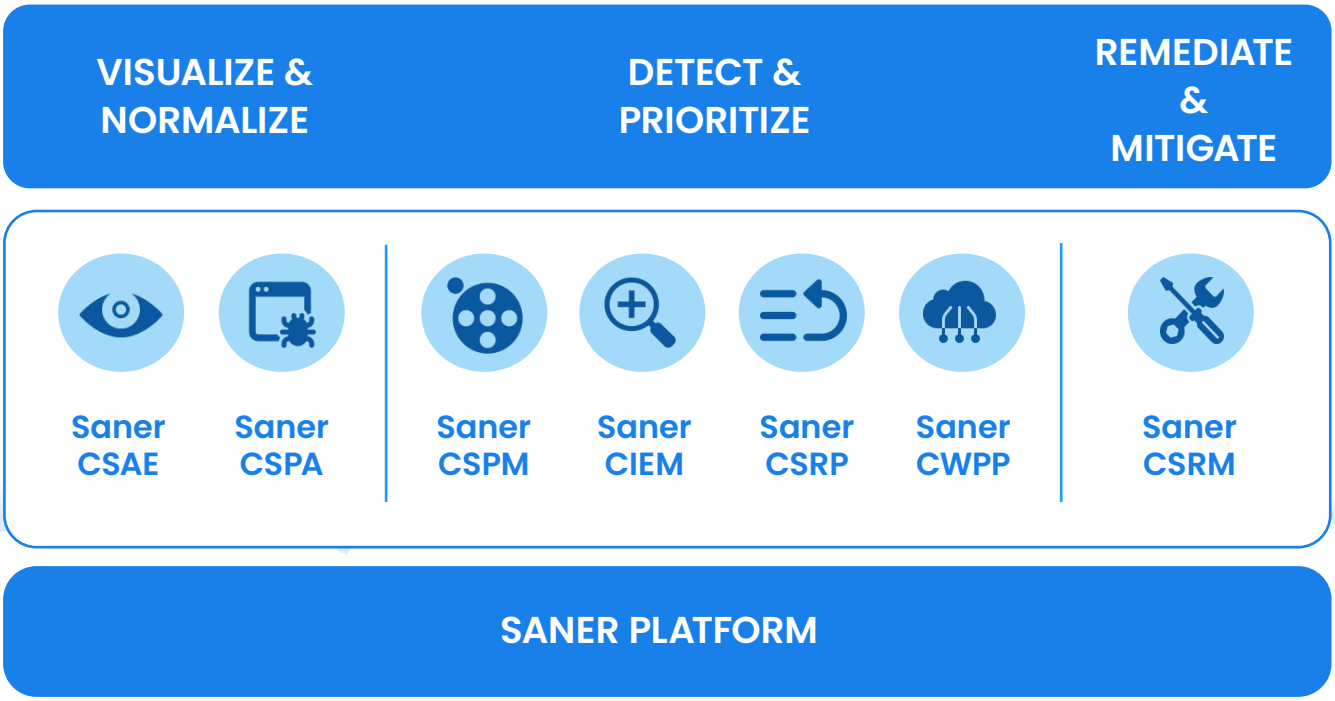
1. Discover and learn your environment along with latest security intel for effective recommendations.
2. Context-aware assistant built into every dashboard.
3. Summarizes complex posture data into simple, actionable insights.
4. Allows natural queries for faster answers.

BUILT FOR EVERY ROLE

1. **IT Admins & Sysadmins:** Streamline day-to-day operations and cut time spent switching between tools.
2. **Cloud Security Engineers:** Gain clarity over workloads, entitlements, and configurations.
3. **CISOs & CTOs:** Get high-level visibility, comprehensive audit-ready reporting, compliance assurance, and measurable ROI from security investments.

Intelligent Security Layers

Saner Cloud combines seven powerful modules under a single umbrella to provide, unified, automated and continuous cloud security for your infrastructure. Saner Cloud, built on Sec-Pod's prevention platform, detects risks and ensures that they are remediated with a natively integrated remediation engine for effective security posture.



CLOUD SECURITY ASSET EXPOSURE (CSAE)

Saner Cloud **maps your entire cloud environment** and gives you visibility into every resource, from virtual machines to storage buckets.

- Build watchlists for critical assets categorize resources and track them continuously based on service type, region and more.
- Detect public-facing resources that increase risk.
- Understand resource distribution globally across AWS and Azure.
- Flag outdated or deprecated services before they become vulnerabilities.
- Track costs and usage to make smarter budgeting decisions.

CLOUD SECURITY POSTURE ANOMALIES (CSPA)

Saner CSPA uses AI-driven and machine-learning based anomaly detection to highlight unusual patterns.

- Confidence levels indicate which anomalies require immediate action.
- Dashboards split anomalies into High, Medium, and Low, with visual distributions.
- Whitelist non-relevant anomalies focus efforts on the most critical ones.

CLOUD SECURITY POSTURE MANAGEMENT (CSPM)

CSPM automates cloud configuration checks and aligns them with industry benchmarks.

- Prebuilt SecPod Default Benchmarks aligned with CIS, HIPAA, PCI-DSS, and NIST.
- Fully customizable compliance rules to tailor for your enterprise.
- Fast scans for misconfigurations and compliance gaps.
- Trend analysis to spot recurring posture issues before they spike.
- Real-time drift detection ensures configurations stay compliant

CLOUD INFRASTRUCTURE ENTITLEMENT MANAGEMENT (CIEM)

CIEM gives you a visual map of how identities, groups, and roles connect to permissions across your cloud.

- Policy Map shows relationships between users, resources, entitlements, and permissions.
- Detect excessive or unused permissions in IAM policies for effective role-based access control (RBAC).
- Identify risks tied to privilege escalation users with excessive permissions or unused or inactive roles.
- Activity logs give a clear view of actions, events, and anomalies.

CLOUD SECURITY RISK PRIORITIZATION (CSRP)

CSRP helps teams focus on the vulnerabilities and misconfigurations that needs to be acted upon first.

- Assigns risk scores based on severity, technical impact, exploitability, and mission-critical resources.
- Leverages MITRE Attack and CISA-SSVC frameworks for contextual prioritization.
- Builds Top Risk lists so the most dangerous issues are never missed.
- Correlates risks across CSAE, CSPM, and CSPA for context-aware prioritization.
- Continuously updates as new vulnerabilities or misconfigurations emerge.

CLOUD WORKLOAD PROTECTION PLATFORM (CWPP)

CWPP keeps every workload in your cloud environment secure and visible, ensuring they stay resilient against vulnerabilities and misconfigurations.

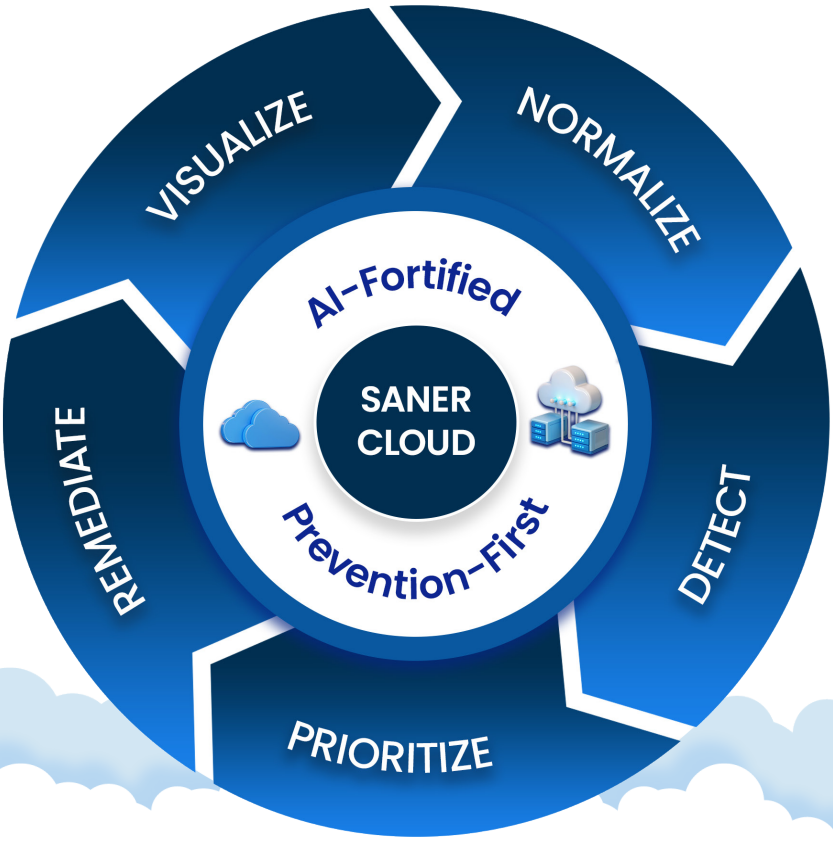
- Proactive risk assessments and holistic cloud workload protection with integrated remediation engine.
- Detect workload misconfigurations and anomalies before attackers exploit them.
- Track OS, applications, and third-party software for complete workload visibility.
- Apply patches and configuration fixes automatically or on demand.

CLOUD SECURITY REMEDIATION MANAGEMENT (CSRM)

CSRM automates patching and remediation across all modules.

- Top 10 missing patches ranked by security impact.
- Create remediation tasks with scheduling for enhanced automation.
- Leverage approval workflows to approve or reject remediation jobs for validated remediation.
- Patch Aging dashboards to show how long vulnerabilities remain unpatched.
- Patching Impact charts prioritize and deploy the most impactful fixes and exponentially reduce attack surface.

Saner Cloud is the premier AI-fortified Cloud-Native Application Protection Platform (CNAPP), based on SecPod's Prevent Framework, delivering continuous visibility, compliance, and risk mitigation.



Benefits at Glance

- Unified dashboard with real-time updates and interactive visuals for a single source of truth
- Complete asset visibility with watchlists, exposure detection, region-based categorization, deprecated services, and cost analysis
- AI-driven anomaly detection with confidence levels, severity distribution, whitelisting options, and one-click remediation
- Continuous posture management with built-in benchmarks, quick misconfiguration checks, trend tracking, and drift detection
- Risk prioritization with scoring, top-risk lists, and context across assets, posture, and anomalies to focus on which risk to remediate first.
- Identity and entitlement governance with policy maps RBAC, resource groups excessive permission detection, and activity logging
- Enhanced Remediation with scheduling and approval workflows, Top 10 patches, patch aging, most-impactful-patches charts, and grouped remediation.
- Smart tagging for fast filtering across thousands of resources and audit logs with tool-specific job codes for full traceability
- Multi-cloud coverage across AWS and Azure with a prevention-first workflow

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 preemptively block cyber threats. The platform includes:

1. **Saner Cloud –** An AI-fortified Cloud-Native Application Protection Platform (CNAPP) that delivers continuous visibility, security compliance, and risk mitigation for cloud environments.

2. **Saner CVEM –** A Continuous Vulnerability and Exposure Management (CVEM) solution that delivers continuous visibility, identifies, assesses, and remediates vulnerabilities across enterprise devices and network infrastructure.

With its suite of cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

Take control of your cloud security posture today.

Saner Cloud is your single, AI-powered defense to discover, govern, and remediate cloud risks faster.