secpod

The Partner Opportunity:

Delivering Cloud Security through Saner CNAPP

www.secpod.com

The Cloud Hygiene Gap in Modern Security Stacks

Enterprise security stacks often include firewalls, endpoint protection, SIEMs, and more. Yet a critical layer is frequently missing: Cloud hygiene.
Cloud hygiene refers to continuously maintaining a secure and compliant cloud environment by eliminating misconfigurations, remediating vulnerabilities, and enforcing least-privilege access. Without dedicated cloud hygiene measures, even well-defended organizations remain exposed. Consider these alarming trends:

Widespread Cloud Breaches

80% of organizations have experienced a cloud security incident in the past year. Misconfigurations are a leading cause.15% of breaches begin with cloud misconfigurations, making it the third most common attack vector in 2024. In fact, Gartner predicts 99% of cloud security failures will be due to customer errors by 2025.

Data at Risk

82% of data breaches in 2023 involved data stored in the cloud, and more than half of cloud environments contain exposed sensitive data on servers or storage. These exposures often stem from overlooked configuration mistakes or unpatched systems, issues that basic security tools miss.

Skill and Tooling Shortfalls

Nearly 45% of organizations report struggling with cloud misconfigurations due to training and awareness gaps. Many IT teams lack the specialized tools or expertise to continuously audit cloud settings, monitor workloads, and manage cloud identities. Traditional security products don't fully address cloud-specific risks, leaving a dangerous gap.

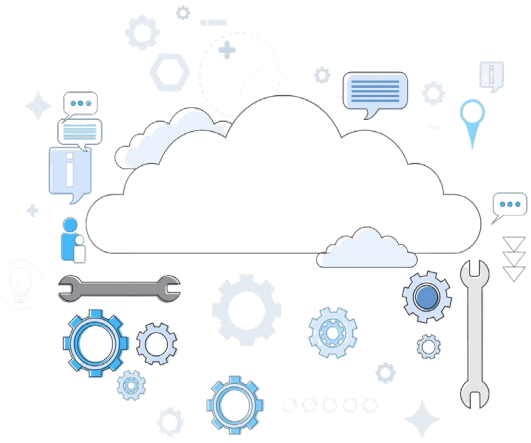
In short, most security stacks aren't equipped for the unique challenges of cloud security posture management. This gap manifests as unnoticed misconfigured storage buckets, overly permissive identity roles, forgotten unpatched VM instances, and other ticking time bombs. For managed service and security providers (CSPs, MSPs, and MSSPs), resellers, and distributors, this gap represents a clear opportunity to step in with a solution that keeps cloud environments clean and safe. Filling this void not only mitigates breaches but also adds significant value to any security offering.

Saner Cloud: Filling the Cloud Hygiene Gap with an AI-Powered CNAPP

SecPod's Saner Cloud is an AI-powered Cloud-Native Application Protection Platform (CNAPP) with integrated Cloud Workload Protection (CWPP) capabilities, purpose-built to tackle cloud hygiene challenges head-on. It provides a unified, continuous approach to securing cloud infrastructure and workloads that complements and completes any security stack. Saner Cloud proactively finds and fixes weaknesses across multicloud environments (AWS and Azure), going beyond what legacy tools cover. Leveraging automation and artificial intelligence, it guarantees that misconfigurations, excessive permissions, and unpatched vulnerabilities don't slip through the cracks.

Saner Cloud's cloud hygiene approach means security is preventive and systematic rather than reactive. The platform continuously scans cloud resources, configurations, and identities against industry benchmarks and best practices. When issues are found, it alerts and guides, or even automatically performs remediation, from tightening an overly broad access policy to patching a critical vulnerability.

The result is a dramatically reduced attack surface and strengthened compliance posture across the board. Partners can confidently position Saner Cloud as the missing piece that hardens clients' cloud environments end-to-end, delivered through an easy-to-manage SaaS platform. The next sections outline Saner Cloud's powerful capabilities that enable this comprehensive cloud hygiene.



Saner Cloud's Core Capabilities

Saner Cloud offers a rich set of capabilities that together empower organizations to achieve continuous cloud hygiene. Below are its core features and benefits:

CONTINUOUS CLOUD POSTURE MANAGEMENT (CSPM)

Saner Cloud continuously monitors cloud configurations and compliance posture in real-time, giving immediate visibility into risks across accounts and regions. Its main capabilities include:

Unified Posture Dashboard

Provides a live, interactive view of your cloud environment's security posture and compliance status across frameworks like NIST, HIPAA, CIS, PCI DSS, and SecPod's own benchmark. With this, you can instantly gauge overall risk and regulatory compliance.

Risk-Based Prioritization

All findings are categorized by severity — High, Medium, Low — to help prioritize remediation effectively. Critical issues, such as exposed sensitive data, or critical compliance failures, stand out immediately for quick action.

Exposure Identification

The platform automatically identifies resources exposed to public networks, like open storage buckets or VMs with public Ips, so you can secure any publicly accessible assets before attackers find them. These at-a-glance indicators of exposure greatly reduce cloud blind spots.

Geographic and Trend Insights

Saner Cloud visualizes security findings on an interactive world map, highlighting affected cloud regions. It also tracks trends over time, so you can see if security issues are spiking or receding after mitigation efforts. Such insights help focus attention on trouble spots and measure improvement in cloud hygiene.

Built-in Compliance Benchmarks

A predefined SecPod Default Benchmark combines best practices from standards like NIST, CIS, PCI, and HIPAA, automatically checking your cloud resources against these controls. This out-of-the-box compliance auditing simplifies meeting regulatory requirements and makes sure cloud configurations align with industry standards.

All these posture management features operate continuously across AWS and Azure accounts, with data updating after each automated scan. Instead of periodic manual audits, organizations get an up-to-date, single pane of glass for cloud risk.

Misconfigurations and compliance violations are surfaced immediately, prioritized intelligently, and linked to guided remediation options. Saner Cloud's CSPM capability basically acts as a diligent cloud security auditor that never sleeps, which is a game-changer for maintaining cloud hygiene.

INTEGRATED VULNERABILITY AND PATCH MANAGEMENT (CWPP)

Cloud workloads — VMs, containers, and other compute instances — often introduce vulnerabilities that need prompt remediation. Saner Cloud includes full vulnerability assessment and patch management as part of its Cloud Workload Protection Platform, ensuring cloud VMs and other assets are secure and up to date:

Continuous Workload Scanning

Saner Cloud continuously assesses cloud-hosted servers and workloads for missing patches, vulnerabilities, and misconfigurations. It provides visibility into any cloud instances that are misconfigured or deviating from secure baselines, so no workload goes unmonitored.

Automated Patching

The platform identifies missing patches and enables one-click remediation of vulnerabilities and missing patches directly from the dashboard. This tight integration of detection and patching means partners can swiftly fix issues at scale, drastically reducing exposure time.

Asset Inventory & Exposure Management

A centralized Asset Exposure tool tracks all cloud assets, such as devices, OS versions, applications, third-party software, with full visibility and automated audit reporting. This helps in identifying outdated or unsupported resources and ensuring nothing in the cloud is forgotten or unmanaged.

Risk Prioritization with Machine Learning

Saner Cloud employs SecPod's proprietary ML-driven risk categorization to prioritize vulnerabilities. Risks are tagged into categories like "Act" (urgent action), "Attend," or "Track" based on severity and potential impact. Such intelligent ranking ensures teams focus on patching the most critical vulnerabilities first, optimizing the use of time and resources.

Combining vulnerability scanning, intelligent risk scoring, and automated patching, Saner Cloud's CWPP capabilities keep cloud workloads hardened. CSP/MSPs can use these features to offer managed cloud vulnerability management services, assuring clients that their cloud servers and applications are continuously scanned and patched against the latest threats. Saner Cloud maintains the cyber hygiene of cloud workloads just as diligently as the CSPM module maintains the hygiene of cloud configurations.

IDENTITY AND ENTITLEMENT MANAGEMENT (CIEM)

Another pillar of cloud hygiene is controlling identity and access risks. Saner Cloud includes CIEM to rein in excessive permissions and enforce least privilege across cloud accounts:

Cloud Identity Visibility

The platform automatically discovers all IAM users, roles, groups, and their permissions across the cloud environment. Administrators get a consolidated view of who and what has access to cloud resources, across AWS and Azure, including accounts that may have been forgotten or inactive.

Excessive Privilege Detection

Saner Cloud evaluates and highlights over-privileged identities and risky policies. It flags users or roles with permissions beyond what they actually use or need, as well as accounts that have been inactive or service accounts with unused keys. Policies that grant more access than necessary are clearly identified so they can be reviewed and adjusted to uphold least-privilege principles.

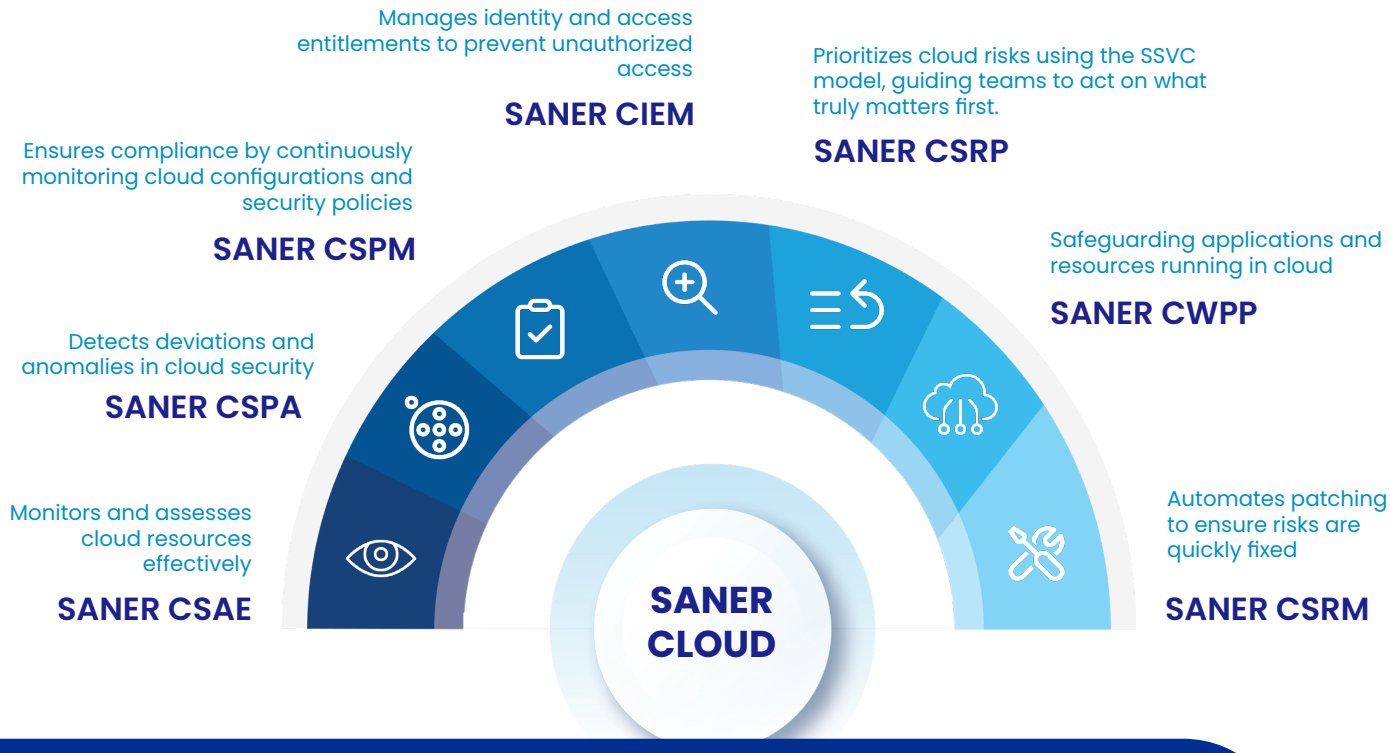
Guided Remediation

The CIEM dashboard provides recommended remediation steps for each finding, helping administrators right-size permissions easily. For example, if a user has an admin role they never utilize, the platform might suggest revoking that role. This guidance makes cloud entitlement cleanup much more straightforward. All such security & compliance issues are presented in one consolidated view, alongside other cloud vulnerabilities and misconfigurations, to simplify holistic remediation efforts.

Critical Activity Monitoring

Saner Cloud also monitors critical IAM activities and logs, like changes to policies or unusual login events, in a dedicated feed. Doing so helps partners and security teams catch suspicious behavior. For instance, if a dormant account suddenly starts making privilege changes, it can indicate compromise. By filtering and searching these activity logs, responders can quickly investigate and take action.

Partners can help clients eliminate dangerous permission creep and shadow admin accounts that often go unnoticed by leveraging Saner Cloud's CIEM capabilities. Enforcing proper cloud identity hygiene reduces insider risk and limits what attackers can do even if credentials are compromised. It's an integral part of a complete cloud security strategy, and Saner Cloud provides these insights and controls out-of-the-box.



AI-Driven Insights and Automation

A standout aspect of Saner Cloud is how it uses artificial intelligence and automation to amplify security teams. Cloud hygiene maintenance has never been this efficient and less error-prone.

Generative AI Assistant

Saner Cloud has a built-in AI assistant that can interpret complex graphs, tables, and large data sets from its dashboards, producing human-readable summaries and insights. Instead of manually parsing raw data, users can rely on generative AI-powered analysis to understand key points in plain language. These AI-generated insights can be copied into reports or presentations, adding value for partners who need to clearly communicate findings to clients.

Automated Remediation Actions

The platform supports one-click remediation for many issues. For example, from the findings view, a technician can click a “Fix” wrench icon to instantly apply a recommended fix or patch. This tight integration between detection and remediation, powered by automation scripts, ensures that maintaining cloud hygiene can happen at the swift pace cloud environments demand, without waiting for lengthy manual fix cycles.

Continuous Learning and Updates

SecPod continuously updates Saner Cloud’s security intelligence, including its benchmarks, vulnerability feeds, and rules, and uses machine learning to improve anomaly detection confidence. The system’s ML algorithms assign confidence levels to detected posture anomalies (high, medium, low) to prioritize which alerts truly need immediate attention. Over time, this means fewer false alarms and more focus on real risks. In short, the platform’s AI/ML components help filter noise, highlight the most critical issues, and even take action on them automatically.

By automating analysis and remediation, Saner Cloud allows partners and IT teams to manage cloud security at scale without proportionally scaling up headcount. It is a game changer for CSP/MSP/MSSPs who must secure multiple client environments efficiently. The AI-driven capabilities enhance both the technical credibility of the solution and the tangible value delivered to customers, with faster time-to-fix and clearer reporting, for instance. In the competitive field of cybersecurity, offering an AI-powered cloud security service like Saner Cloud can be a real differentiator.

The Partner Opportunity: Delivering Cloud Hygiene-as-a-Service

For CSP/MSPs, MSSPs, resellers, and distributors, cloud hygiene represents a high-growth service opportunity. As organizations scramble to secure their cloud deployments, they increasingly turn to trusted partners for help. In a recent survey of IT leaders at large organizations, 57% said they plan to increase reliance on CSP/MSPs for managing and securing cloud environments. Notably, 92% of those using CSP/MSPs entrust them with ensuring cloud security and 88% with cloud compliance tasks. Businesses clearly need the specialized expertise and tools that partners can provide to keep their cloud infrastructure safe.

By adding Saner Cloud to your portfolio, you can fill the cloud hygiene gap for clients and differentiate your services in a few key ways:

Comprehensive Cloud Security Service

Saner Cloud allows you to offer cloud security posture management, workload protection, and identity management as a unified service. This means you can proactively secure customers' cloud assets on an ongoing basis, rather than just react to incidents. Given the spike in cloud breaches, this proactive service is in high demand.

Faster Incident Prevention and Compliance

With continuous monitoring and automated remediation, you help clients prevent misconfiguration-related incidents that could lead to costly breaches or compliance fines. This not only saves clients money and downtime but also cements your role as a critical advisor for their risk management. Partners can use Saner Cloud's rich compliance reporting to regularly demonstrate value to customers in audits and reviews.

Multi-Tenancy and Scalability

Saner Cloud's SaaS platform is designed for scale, allowing partners to manage multiple customer environments from a single interface with proper segregation. This multi-tenant efficiency means you can expand your client base without linear growth in overhead. The cloud-based delivery also ensures you and your clients always have the latest features and updates without maintenance burden.

Cloud hygiene services powered by Saner Cloud enable new revenue streams and stronger customer retention. You can bundle cloud security monitoring with existing offerings or provide it as a standalone managed service. Either way, you address a glaring client need, one that competitors may not be tackling at the moment, positioning your business as a leader in modern cloud security.

SECPOD PARTNER PROGRAM BENEFITS AND INCENTIVES

SecPod is committed to partner success, offering a robust partner program with meaningful benefits to accelerate your go-to-market. When you partner with SecPod and offer Saner Cloud, you gain access to:

Flexible Partnership Models

Whether you are a distributor, reseller, CSP/MSP/MSSP, or technology partner, SecPod's program offers flexibility, including options to co-brand the Saner Cloud solution as part of your own services or even offer it as a stand-alone product under your brand. This white-label capability lets you strengthen your brand while leveraging SecPod's technology.

Attractive Margins and Licensing

The program features tailored licensing models with scalable pricing to fit your business needs. You can easily bundle Saner Cloud into subscription packages for clients. Deal registration and volume-based incentives help protect your opportunities and maximize profitability, so you can grow revenue with confidence.

Sales & Technical Training

SecPod provides comprehensive training and certification for your team on both the technical and sales aspects of Saner Cloud. Your engineers and consultants will learn to deploy and support the platform, while your sales team gets the know-how to position and pitch it effectively. Upon completing training, your staff can earn SecPod certifications that bolster your credibility in cloud security.

Marketing and Lead Generation Support

Partners receive a wealth of co-branded marketing materials and support to drive demand, which includes brochures, playbooks, battle cards, case studies, webinars, and more. SecPod actively collaborates on joint marketing campaigns and events to generate leads and elevate you as a thought leader in cybersecurity. Such resources enable you to hit the ground running in educating customers about cloud hygiene and Saner Cloud.

24/7 Technical Support & Resources

When you need assistance, SecPod's experts are available around the clock. Partners get 24/7 premium support access to SecPod's technical teams, ensuring you can meet customer needs promptly. Extensive documentation and a knowledge base are also provided for quick answers and smooth deployments.

Overall, SecPod's partner program is built on collaboration, shared growth, and long-term success. By joining, you gain a true partnership – not just a product to resell. SecPod works closely with partners on go-to-market strategy, provides strategic account support, and continuously innovates its solutions to keep you ahead of the curve. It's a partnership designed to help you expand your cybersecurity portfolio and drive new business with an offering that is timely and highly valued by customers.

Learn more about the SecPod Partner Program and its benefits, and see how you can incorporate Saner Cloud into your offerings.

Strengthening Security Stacks with Cloud Hygiene

Cloud security helps establish a powerful defense strategy. Organizations are actively seeking help to identify hidden misconfigurations, plug cloud vulnerabilities, and manage complex cloud entitlements before they lead to disaster. Cloud hygiene, provided as a service via platforms like SecPod's Saner Cloud, is the missing puzzle piece that completes the modern security stack. It's preventive, continuous, and comprehensive.

For partners, embracing cloud hygiene with Saner Cloud is a chance to differentiate in a crowded market and become indispensable to your clients. You can step up as the expert who keeps your customers' cloud infrastructure not only secure but well-maintained and compliant at all times. The result is a win-win: clients avoid breaches and sleep easier, while you unlock new revenue streams and deepen customer trust.

Don't let your clients operate in the cloud with an incomplete security stack. Take the step to include cloud hygiene in every engagement. With SecPod Saner Cloud, you have the technology and SecPod's full support to deliver this value immediately. It's time to fill the gap and elevate your security portfolio.

Ready to get started? Visit the SecPod Saner Cloud page for more details on the solution, or reach out through the SecPod Partner Program to begin your journey as a SecPod partner. Equip your customers with the cloud hygiene they've been missing and position your business at the forefront of cloud security innovation.

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.

www.secpod.com | info@secpod.com