secpod

SANER CLOUD

Cloud Workload Protection Platform (CWPP)

DATASHEET

SANER CLOUD

Cloud Workload Protection Platform (CWPP)

Modern cloud environments are constantly evolving and expanding, requiring a centralized view of workloads, vulnerabilities, and configurations to operate efficiently. Organizations relying on providers such as AWS and Azure face significant challenges in discovering, classifying, and monitoring distributed workloads across hybrid and multicloud setups. Without a unified perspective, unnoticed security gaps may persist, increasing the risk of breaches or compliance complications.

The need of the hour is a cloud security solution that helps information security professionals overcome these hurdles with maximum convenience and confidence. Saner CWPP is one such tool that delivers on all expectations.

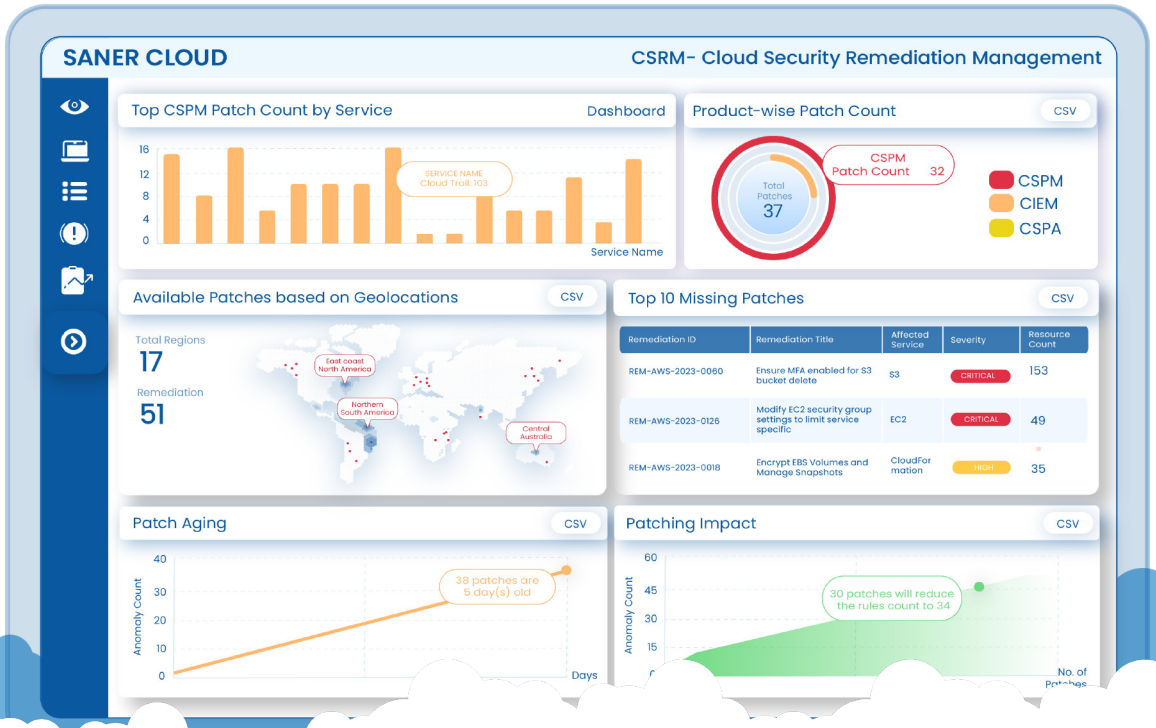
Unified Security for Cloud Workloads, Managed Under One Roof

SecPod Saner's CWPP delivers a unified framework that merges seven advanced security capabilities to protect cloud workloads.

It brings together Vulnerability Management (VM), Compliance Management (CM), Posture Anomaly Management (PA), Asset Exposure (AE), Risk Prioritization (RP), Patch Management (PM), and Workload Management (WM).

SecPod's approach continuously identifies vulnerabilities, monitors configurations, deploys timely patches, restricts unauthorized access, and manages workload behavior.

Designed for IT and security teams, CWPP provides a centralized console that unifies diverse security functions to address cloud workload challenges efficiently.



"SecPod Saner's CWPP integrates security capabilities like vulnerability, compliance, patch, and workload management to protect cloud workloads."

Maintaining Steady Security Across Your Cloud

UNIFIED WORKLOAD DEFENSE

Automated systems continuously scan and assess cloud workloads, providing consolidated visibility across hybrid and multicloud environments.

INTEGRATED SECURITY FUNCTIONS

Combines vulnerability management, configuration reviews, patch deployment, anomaly detection, and workload control into one seamless platform.

REAL-TIME COMPLIANCE MONITORING

Ongoing audits and configuration checks produce audit-ready reports and support regulatory requirements without extra steps.

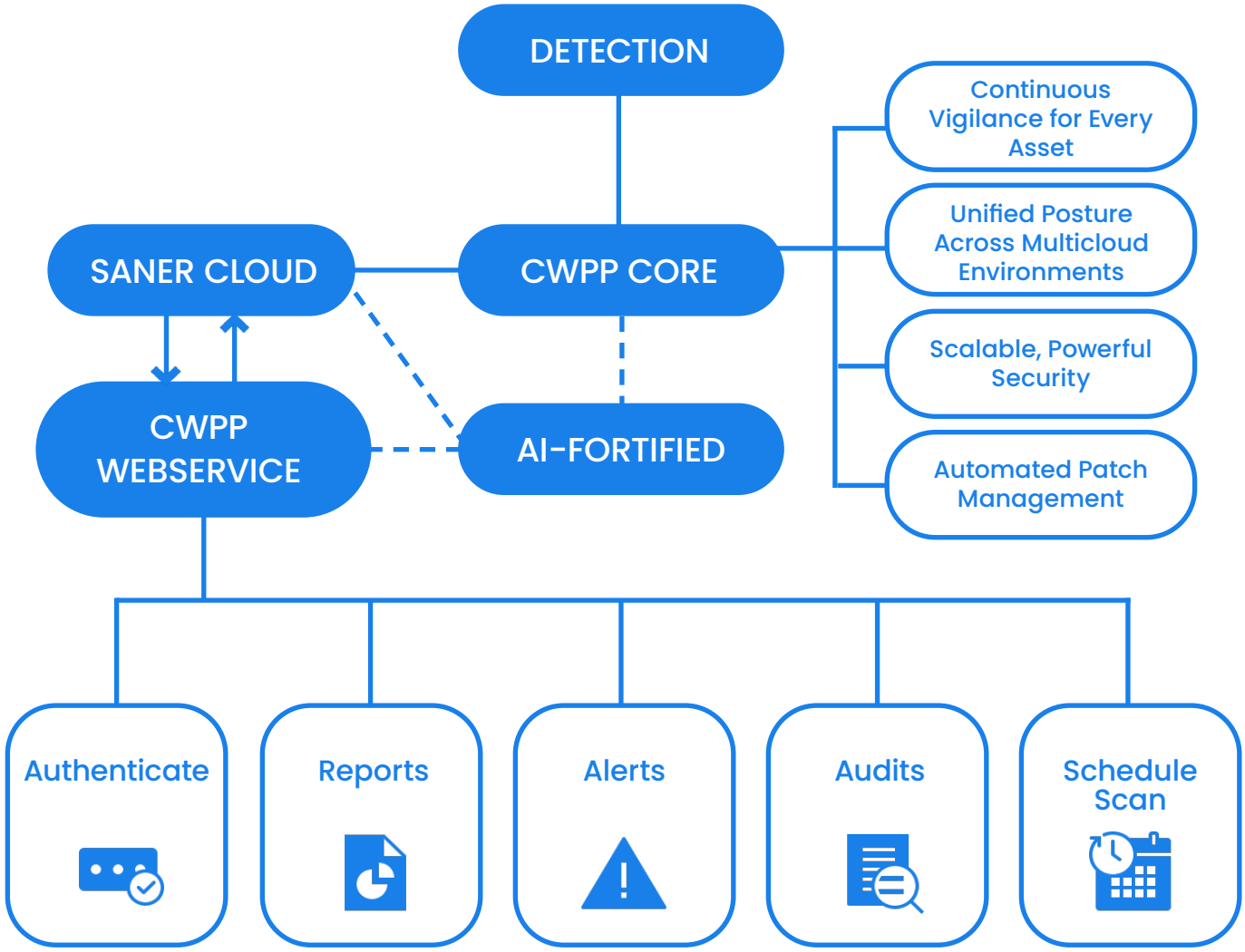
ACCELERATED REMEDIATION

Automated Patching and risk prioritization considerably reduce the time between issue detection and correction.

COMPREHENSIVE OPERATION OVERSIGHT

A single dashboard aggregates data from multiple modules, offering a clear picture of your cloud workload security.

Workflow Diagram



Unparalleled Benefits of Saner CWPP

ASSET EXPOSURE (AE)

AE delivers a unified inventory that detects unmanaged or unauthorized assets, effectively uncovering instances of shadow IT. It analyzes exposure by pinpointing publicly accessible endpoints, inactive ports, and misconfigured storage that could serve as entry points for attacks. By categorizing assets according to type, usage patterns, and importance, and by monitoring resource utilization to identify redundancies, it helps prioritize remedial actions and reduce unnecessary exposure.

POSTURE ANOMALY MANAGEMENT (PA)

PA uses machine learning to compare current configurations against established baselines, flagging deviations like unauthorized software or irregular workload behavior. Daily evaluations, conducted through over 75 rule-based checks, detect shifts in configurations early on. Automated alerts provide detailed risk insights, and integrated remediation workflows enable direct adjustments or isolation of problematic workloads to maintain a steady cloud posture.

VULNERABILITY MANAGEMENT (VM)

The VM capability continuously scans workloads, containers, and cloud assets using an up-to-date intelligence repository to identify potential weaknesses. It covers both internal and external environments across hybrid and multicloud setups, reaching even the most challenging endpoints. AI-driven models analyze and rank vulnerabilities based on exploit likelihood, impact, and business relevance, while clear remediation instructions and automated workflows facilitate swift application of fixes throughout your environment.

COMPLIANCE MANAGEMENT (CM)

CM employs pre-built policies aligned with standards such as NIST, PCI DSS, and HIPAA, and also supports custom checks tailored to your organization's specific needs. It monitors configurations in real time to promptly identify errors and policy breaches, triggering immediate corrective actions. In addition, comprehensive audit-ready reports consolidate compliance statuses, violations, and remediation activities, simplifying both internal reviews and external assessments.

RISK PRIORITIZATION (RP)

RP helps address the biggest threats first with intelligent risk classification that focuses on the vulnerabilities most likely to impact operational performance. Saner Cloud CWPP prioritizes these risks based on severity, allowing teams to direct resources effectively where they'll have the most significant impact. This structured approach to prioritization supports faster decision-making and ensures an optimized defense strategy, even in dynamic infrastructures where threat levels frequently fluctuate.

PATCH MANAGEMENT (PM)

PM automates the deployment of updates across operating systems, software dependencies, and container images through a centralized process that reduces manual efforts. It offers one-click emergency patching for high-profile vulnerabilities, including zero-day issues, to swiftly reduce exposure. Additionally, it supports custom pre- and post-patch scripting for advanced integration with existing workflows and meticulously records patch activities for thorough audit trails and regulatory compliance.

WORKLOAD MANAGEMENT (WM)

WM empowers you to control applications on cloud workloads through whitelisting and blacklisting, blocking unauthorized software to reduce attack surfaces. It facilitates the rapid isolation of compromised workloads to prevent lateral movement, while automated remediation processes address performance or security issues to minimize downtime. Furthermore, it enforces organizational policies on workload configurations — such as firewall settings and runtime permissions — to maintain a balanced state between security and operational performance.

"Saner CWPP provides a unified cloud security solution for discovering, classifying, and monitoring workloads across hybrid and multicloud environments."

One-Tool. Multifaceted Impact.

Consolidated view of vulnerability, compliance, anomaly, and workload data from multiple cloud environments	Detailed categorization with actionable insights to drive precise remedial actions
Streamlined processes combining automated patching with guided remediation for rapid fixes	Exportable reporting and interactive dashboards to support audits and internal reviews

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.

www.secpod.com