SANER CLOUD

Cloud Security Posture Management (CSPM)

DATASHEET

SANER CLOUD
Cloud Security Posture Management (CSPM)

Managing an organization's cloud security posture is one of the most complicated tasks in the world of cybersecurity. With lack of visibility into data security posing as the primary challenge, closely followed by the complexity of modern security tools and a shortage of skilled cloud professionals, the world is in dire need of an effective CSPM solution.

With Saner CSPM, get ready to address your most pressing cloud security posture and compliance issues with a level of simplicity and speed like never before experienced.

The Most Advanced Cloud Security Posture Management Tool

SecPod Saner CSPM identifies misconfigurations across cloud infrastructures by benchmarking configurations against the SecPod Default Benchmark. It brings together best practices from HIPAA, PCI DSS, SOC 2, NIST, and CIS.

We've merged them into predefined policies that map cloud configurations to established standards to help organizations bolster their security strategies with maximum convenience.

For Compliance Officers and Risk Managers, SecPod promises complete visibility across AWS, Azure, and others via a centralized security console.
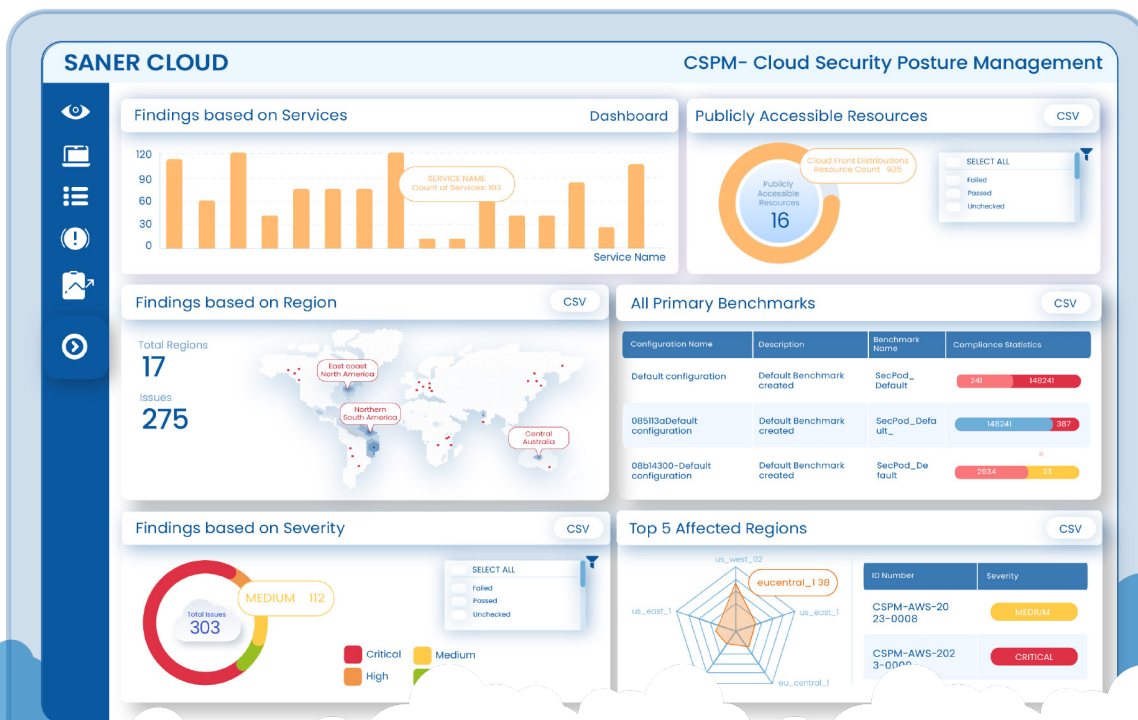
Future-Proofing Your Cloud Security Posture

CONTINUOUS CLOUD MONITORING

Performs scans in short intervals across all supported cloud environments. Continuous monitoring detects misconfigurations, public exposures, & outdated security settings, providing a persistent view of risk indicators and cloud posture.

UNIFIED CLOUD INTELLIGENCE

Consolidates data from AWS, Azure, and other environments into a single dashboard. This central view eliminates information silos and offers comprehensive insight into asset security, compliance metrics, and emerging trends.

AUTOMATED RISK RESPONSE

Executes preconfigured workflows that recalibrate identity access settings, adjust encryption parameters, and modify network configurations as soon as vulnerabilities are detected. Automation cuts down on manual processes and shortens the time between detection and remediation.

AI-DRIVEN RISK RANKING

Utilizes advanced analytics to assess vulnerabilities based on exploit potential, overall impact, and remediation urgency. Smart prioritization focuses team efforts on addressing the highest-risk issues first.

LOCALIZED BENCHMARKING PRECISION

Customizes security assessments by aligning benchmarks with regional compliance standards. Tailored evaluations reflect both global best practices and local regulatory mandates, offering relevant insights for different geographic areas.

CONFIGURABLE SEVERITY CONTROLS

Provides granular control over risk thresholds. Customizable settings allow organizations to pinpoint high-impact issues across diverse environments, focusing remediation efforts where they matter most.

INSTANT COMPLIANCE INSIGHTS

Tracks security posture in real time with built-in compliance monitoring. Downloadable CSV reports and audit-ready metrics simplify periodic reviews and streamline preparation for audits.

INTERACTIVE DATA VISUALIZATIONS

Displays findings through intuitive visual tools, including service-specific bar graphs, geographic heat maps, and trend lines that map changes over time. Visual analytics help teams quickly grasp complex data at a glance.

INTEGRATED REMEDIATION WORKFLOWS

Connects with CI/CD pipelines and development workflows to automatically apply remediation policies during deployment. Pre-set workflows correct misconfigurations during the rollout process, reducing the need for manual fixes.

ADVANCED IDENTITY & ACCESS OVERSIGHT

Monitors identity and access management activities to flag unusual access patterns, overprivileged accounts, or deviations from standard permission models. Built-in alerts support strict access control and help mitigate insider risks.

Workflow Diagram
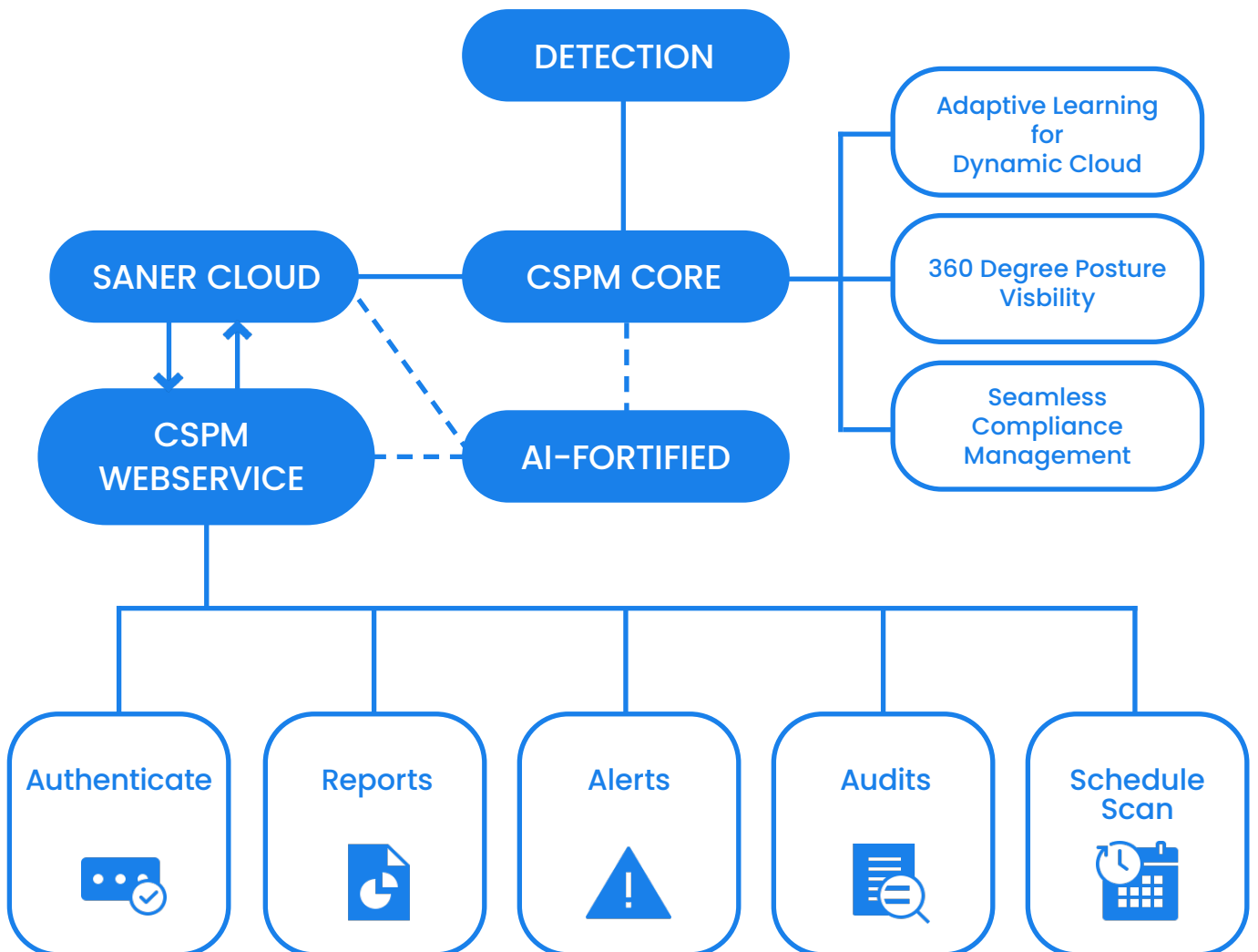
Unparalleled Benefits of Saner CSPM

RAPID DETECTION AND RESPONSE

Real-time scanning identifies configuration errors within minutes, significantly reducing the window for potential attacks. Fast detection leads to quicker remediation, minimizing exposure to emerging threats.

SMART ALERT PRIORITIZATION

AI-powered algorithms filter out lower-risk signals and rank alerts based on severity and exploit potential. This targeted approach reduces alert overload and directs attention to the most impactful issues.

COMPREHENSIVE MULTICLOUD VISIBILITY

Data from multiple cloud platforms is aggregated into one centralized dashboard. A single-pane view offers clear insights into security trends, compliance statuses, and configuration anomalies without switching between systems.
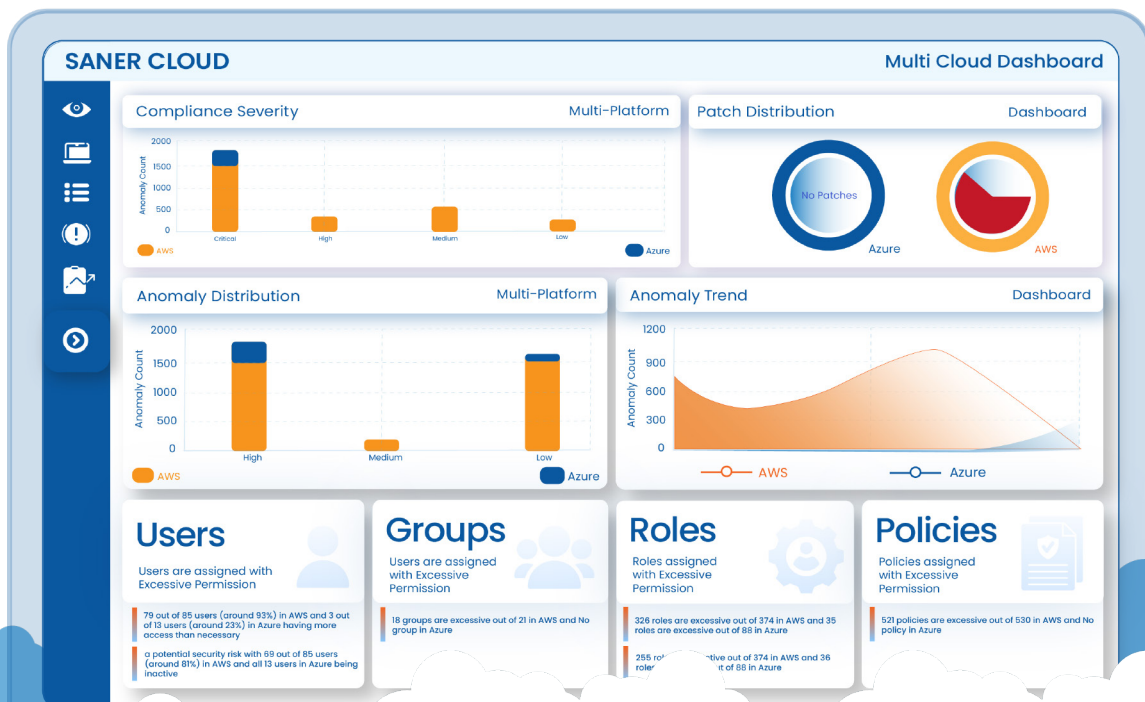
AUTOMATED COMPLIANCE AT SCALE

Ongoing compliance monitoring automatically compiles detailed, audit-ready reports. Continuous application of preconfigured policies aligned with frameworks such as SOC 2, HIPAA, PCI DSS, and NIST 800-53 simplifies audit preparation and regulatory tracking.

ENTERPRISE-LEVEL SCALABILITY

Supports flexible deployment options — agent-based or agentless — to onboard a vast number of cloud assets in minutes. Designed for organizations of all sizes, the solution scales quickly with growing environments.

AI-POWERED ANOMALY DETECTION

Machine learning models review both historical and real-time data to pinpoint irregularities in IAM behavior and resource modifications. Contextual alerts enable teams to address deviations before they develop into larger issues.

SANER CLOUD — Multi Cloud Dashboard

Compliance Severity — Multi-Platform
Patch Distribution — Dashboard
Anomaly Distribution — Multi-Platform
Anomaly Trend — Dashboard

Users — Users are assigned with Excessive Permission
79 out of 85 users (around 93%) in AWS and 3 out of 13 users (around 23%) in Azure having more access than necessary
a potential security risk with 69 out of 85 users (around 81%) in AWS and all 13 users in Azure being inactive

Groups — Users are assigned with Excessive Permission
18 groups are excessive out of 21 in AWS and No group in Azure

Roles — Roles assigned with Excessive Permission
326 roles are excessive out of 374 in AWS and 35 roles are excessive out of 88 in Azure
255 roles ... tive out of 374 in AWS and 36 roles ... t of 88 in Azure

Policies — Policies assigned with Excessive Permission
521 policies are excessive out of 530 in AWS and No policy in Azure

"SecPod Saner CSPM ensures cloud security compliance with centralized visibility across AWS, Azure, and more."

One-Tool. Multifaceted Impact.

Unified view of cloud security posture for Compliance Officers and Risk Managers	**Consistent configuration analysis with real-time, data-driven insights**
Simplified audit processes with automated compliance tracking and report downloads	**Rapid detection and remediation that minimizes exposure across cloud environments**

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