secpod

SANER CLOUD

Cloud Security Posture Anomaly (CSPA)

DATASHEET

SANER CLOUD

Cloud Security Posture Anomaly (CSPA)

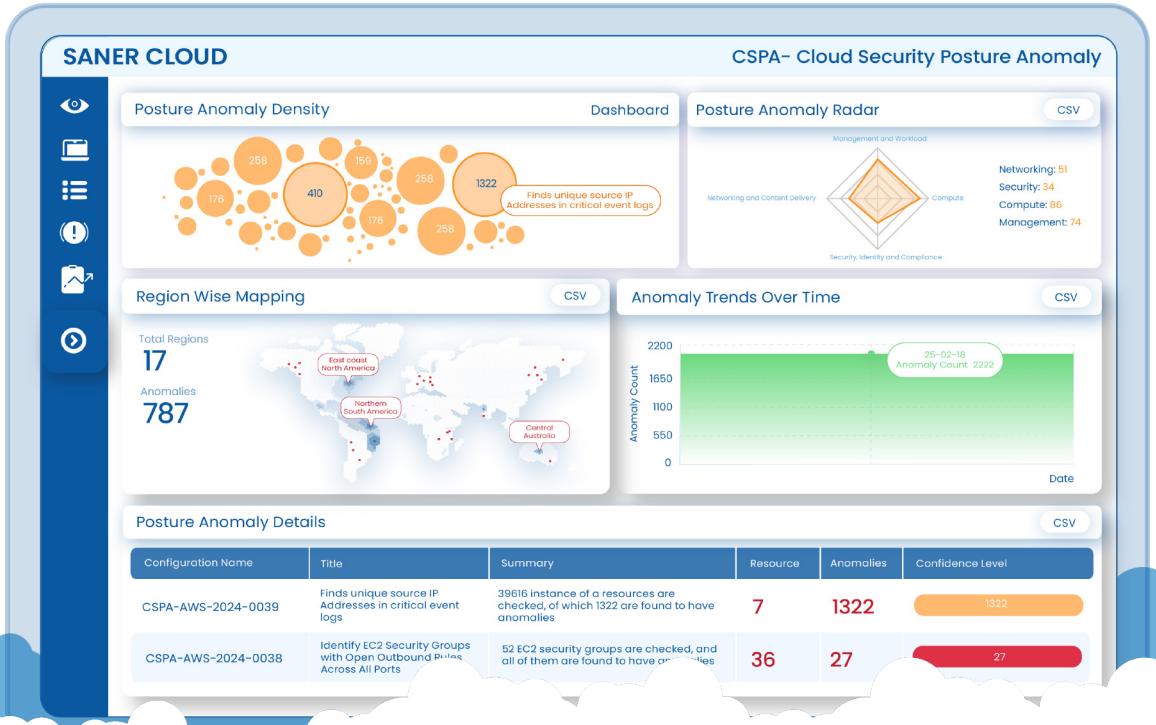
Identifying deviations from expected postures in cloud environments is a process that requires some of the most nuanced analysis practices, which are not easily obtainable in the current market. Once identified, these outliers, if left unaddressed, can introduce vulnerabilities due to misconfigurations or unnecessary permissions. Catching them before they can disrupt your business is a matter of utmost urgency to reduce the attack surface and strengthening cloud security.
The need of the hour is a cloud security solution that helps information security professionals overcome these hurdles with maximum convenience and confidence. Saner CSPA is one such tool that delivers on all expectations.

Maximizing Your Cloud Posture Anomaly Management Capabilities

SecPod Saner CSPA identifies resources that deviate from typical behavior across cloud infrastructures. It uses advanced behavioral analytics and statistical methods to pinpoint outliers among similar resources.

These anomalies may signal misconfigurations, unneeded permissions, or other irregularities that can expose vulnerabilities. CSPA provides actionable paths to address these issues and maintain a stable cloud posture.
Designed for IT teams and security professionals, CSPA offers a unified console that brings together deep insights from multiple cloud platforms.

With a range of visual tools and automated remediation options, CSPA equips teams to monitor, analyze, and adjust cloud configurations in real-time.



Reshaping Your Approach to Cloud Posture Anomaly Management

HEATMAP OF ANOMALIES BY SEVERITY

Presents a color-coded heatmap that categorizes anomalies into high, medium, and low severity levels. This visualization helps teams quickly recognize which deviations require immediate attention and which can be scheduled for routine review.

BUBBLE CHART FOR ANOMALY DISTRIBUTION BY CATEGORY

Displays anomalies in a bubble chart format, where each bubble represents a specific security category. The size and density of the bubbles reveal the volume and concentration of irregularities, allowing teams to pinpoint areas with a high occurrence of deviations.

MAPPING OF ATTACK CATEGORIES VIA ANOMALY COUNT

Associates detected anomalies with potential attack vectors. The system gives insight into which types of threats the cloud environment may be more susceptible to by counting anomalies per attack category, supporting proactive adjustment of security measures.

IN-DEPTH ANALYSIS USING DATA SCIENCE TECHNIQUES

Each identified anomaly is scrutinized with advanced data algorithms. The process is designed to filter noise and extract actionable information, presenting detailed context such as impact estimation and probable causes to assist in precise decision-making.

DETECTION AND REPORTING OF PUBLICLY ACCESSIBLE RESOURCES

Identifies resources that are exposed to the public and explains the configuration settings leading to this exposure. Detailed reports allow teams to review why an asset is open and address any settings that could lead to unauthorized access.

TIMELINE VISUALIZATION OF ANOMALY TRENDS

Tracks anomalies over time with a timeline-based graph, revealing patterns and shifts in the cloud posture. This historical view assists teams in monitoring improvements or recurring issues, and in understanding how changes affect the overall environment

GEOGRAPHIC DISTRIBUTION OF ANOMALIES

Provides a map-based visualization that shows the regional dispersion of anomalies. Identifying the geographical hotspots, teams gain insights into location-specific configurations and regional compliance matters.

CUSTOM WATCHLIST FOR EXPECTED ANOMALIES

Allows teams to mark known or acceptable deviations that do not require further action. Once whitelisted, these anomalies are removed from ongoing remediation prompts so that focus remains on unexpected findings.

ONE-CLICK REMEDIATION FUNCTIONALITY

Saner Cloud CSAE offers a streamlined option to address individual anomalies or apply fixes to all flagged issues in one operation. This feature minimizes manual intervention by triggering preconfigured remediation workflows that correct misconfigurations.

WHITELIST MANAGEMENT FOR ENTIRE ANOMALY GROUPS

Provides the option to exempt an entire category of anomalies from remediation suggestions. This particular capability helps refine the alert system, focusing attention only on deviations that truly represent a security concern.

COMPREHENSIVE ANOMALY INSIGHT SUMMARIES

Every anomaly comes with a detailed summary that includes historical trends, regional data distribution, and a breakdown of affected versus unaffected resources. These summaries empower teams to assess the overall impact and decide on the appropriate remediation strategy.

GRID VIEW FOR ALL ANOMALIES

Presents a complete tabular listing of detected anomalies, clearly distinguishing between items requiring action and those with acceptable configurations. The grid view facilitates quick scanning and sorting for the simplified management.

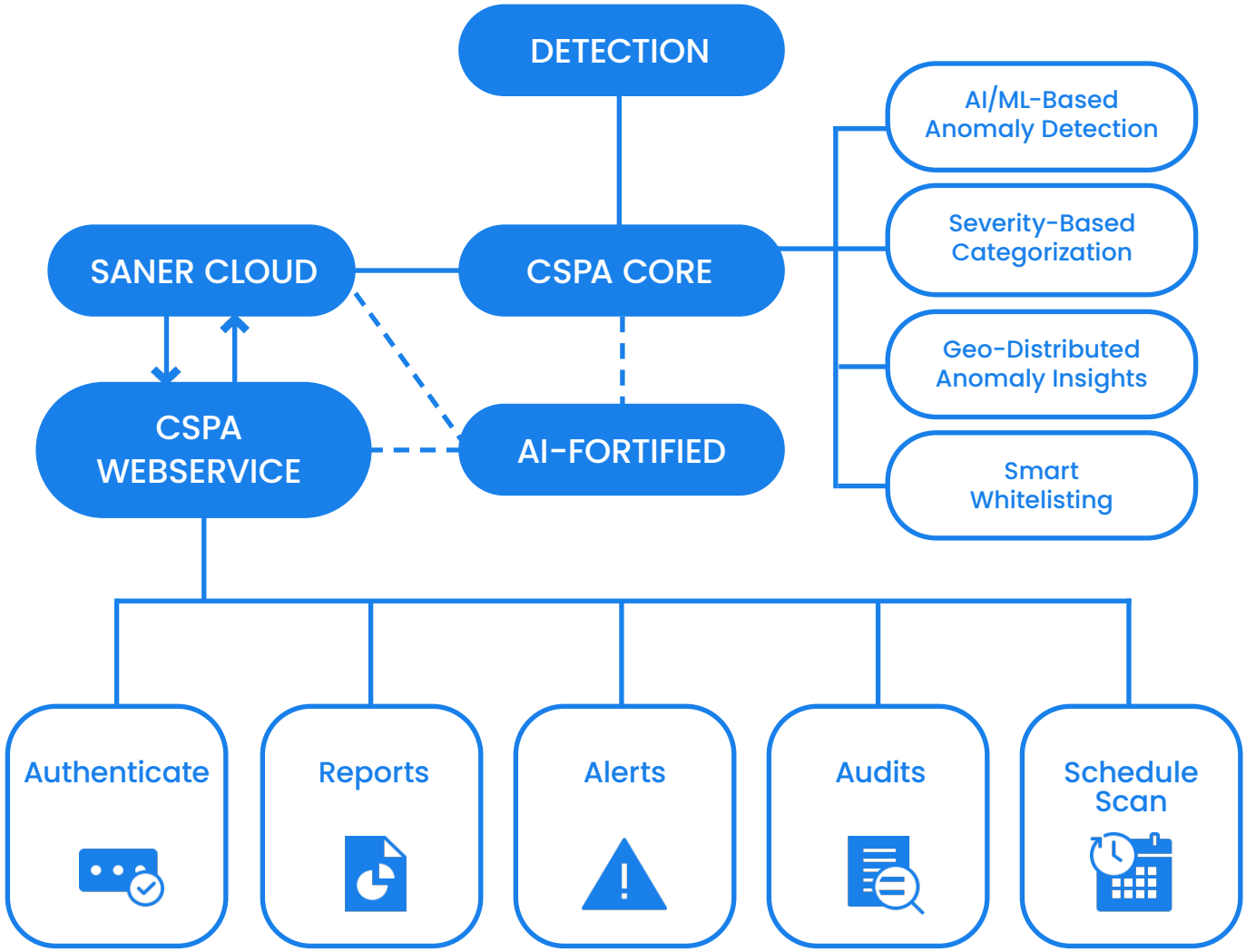
CSV EXPORT FOR OFFLINE ANALYSIS

Supports downloading dashboard data in CSV format for offline review. These reports assist in audit preparation, compliance documentation, and in-depth analysis by external teams.

GENERATIVE AI ANALYSIS FOR VISUALS AND DATA

Incorporates an AI analyzer that converts complex graphs and tables into concise, human-readable summaries. These insights can be directly used in reports or discussions, making data interpretation straightforward.

Workflow Diagram



Unparalleled Benefits of Saner CSPA

RAPID ANOMALY IDENTIFICATION

Real-time detection capabilities reduce the window between misconfiguration and correction, limiting potential exposure time.

PRIORITIZED REMEDIATION

Automated risk scoring and categorization help direct attention to deviations with the highest impact, aiding in faster decision-making.

HOLISTIC VISIBILITY ACROSS CLOUD RESOURCES

A centralized dashboard consolidates anomaly data from multiple cloud providers, giving a clear view of the overall security posture.

ACTIONABLE REPORTING AND CUSTOMIZATION

Customizable reports and whitelist management allow teams to tailor the system to their specific operational needs and regulatory requirements.

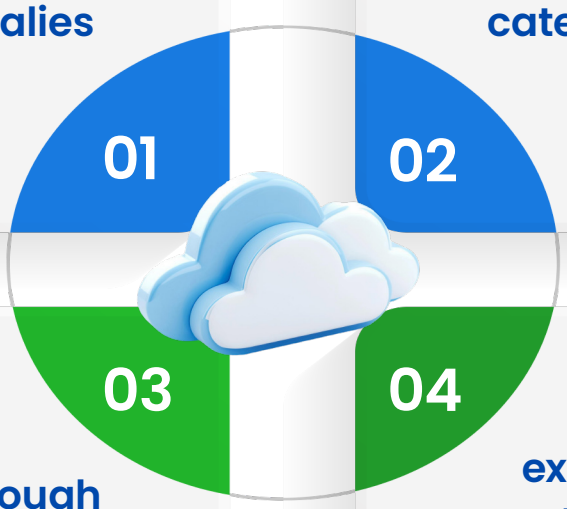
SCALABILITY FOR LARGE ENVIRONMENTS

Designed to monitor millions of resources across diverse cloud infrastructures, CSPA accommodates growth without sacrificing performance.

One-Tool. Multifaceted Impact.

Consolidated view of posture anomalies across cloud platforms.

Detailed categorization with actionable insights.



Streamlined remediation processes through one-click fixes.

Custom reporting and export options for audit and analysis.

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