

The background is a solid blue color. It features a pattern of binary code (0s and 1s) in a lighter blue shade, scattered across the upper and middle sections. At the bottom, there is a stylized, layered pattern of light blue clouds.

**secpod**

# **SANER CLOUD**

**Cloud Security Remediation  
Management (CSRM)**

---

**DATASHEET**

# **SANER CLOUD**

## **Cloud Security Remediation Management (CSRM)**

---

The importance of CSRM in today's cloud security management cannot be understated. The task of addressing vulnerabilities, anomalies, entitlements issues, and compliance gaps efficiently is laborious, and organizations need all the help they can get. And once vulnerabilities are identified and analyzed, the next natural step is patching. It's a process that guarantees that security risks are mitigated promptly to maintain a desirably strong security posture. However, finding the ideal CSRM solution is easier said than done.

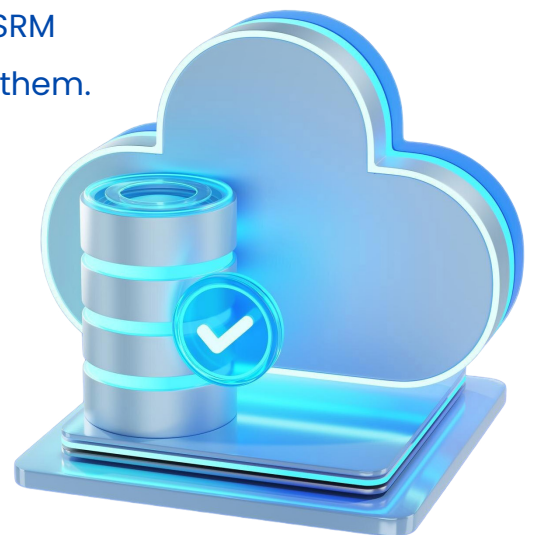
The need of the hour is a cloud security solution that helps information security professionals overcome these hurdles with maximum convenience and confidence. Saner CSRM is one such tool that delivers on all expectations.

## **Hassle-Free Cloud Security Incident Remediation**

SecPod Saner CSRM addresses vulnerabilities, anomalies, entitlement issues, and compliance gaps through efficient patch management.

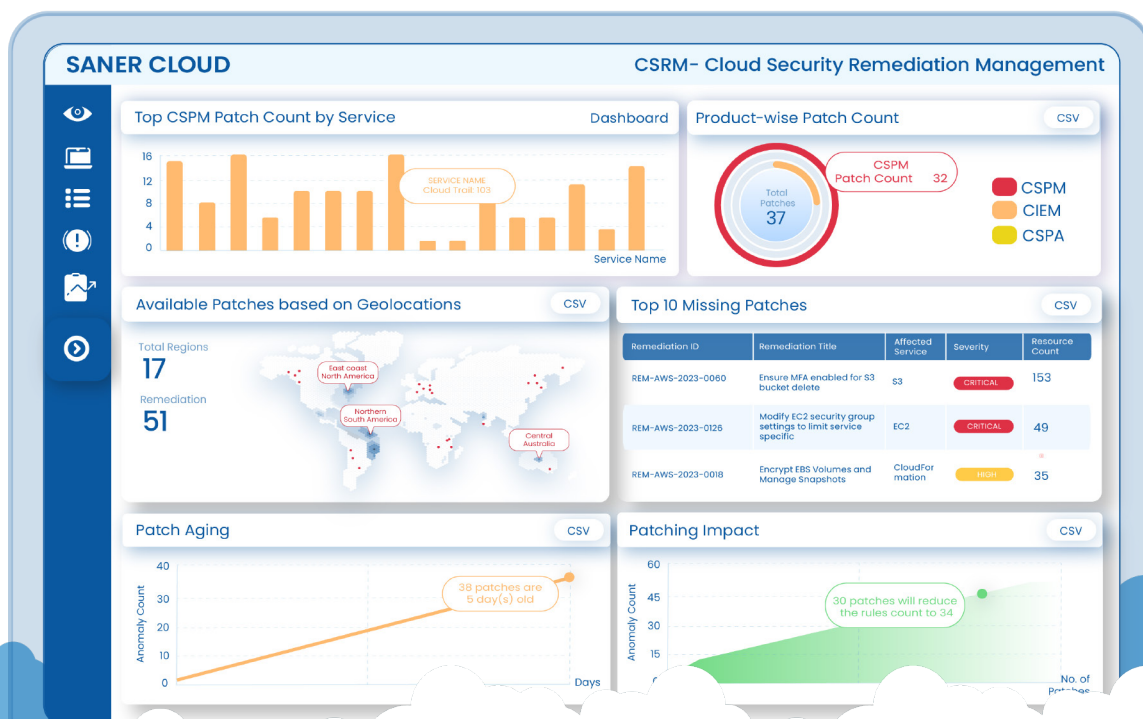
After security issues are detected and analyzed, CSRM takes the next step by applying patches to resolve them.

It supports two approaches: Job-based patching, where patch tasks are created and scheduled according to security findings, and automated patching, which applies fixes whenever specific issues recur.



Remediation actions are organized into three primary domains – Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), and Cloud Security Protection & Automation (CSPA) – and fall into two categories: Predefined Patches, which operate fully automatically, and Custom Patches, which may require user configuration for aspects such as allowed IPs or port settings.

Designed for SOC teams, DevOps, response teams, and IT administrators, CSRM provides a centralized view to monitor, manage, and track all remediation activities across your cloud environment.



**“SecPod Saner CSRM addresses vulnerabilities and compliance gaps through job-based or automated patch management to resolve security issues.”**

# The Most Comprehensive Cloud Remediation Platform

## VISUALIZE PRODUCT-WISE PATCH COUNT DISTRIBUTION

An intuitive display shows the number of patches applied across various products, giving teams a quick snapshot of remediation activity and overall security posture.

## TOP CSPM PATCH COUNT BY CLOUD SERVICE

A bar graph categorizes CSPM patches by cloud service — such as AWS, Azure, or others —revealing which platforms require more remediation effort and focused attention

## PATCH COUNT BASED ON GEOLOCATION

For CSPM, CIEM, and CSPA, Saner Cloud CSRM visualizes maps patch distribution across different regions, helping teams identify areas with elevated risk and prioritize location-specific remediation measures.

## PRIORITIZE BASED ON TOP MISSING PATCHES

Identifies the ten most significant patch gaps across CSPM, CIEM, and CSPA by applying a weighted score that considers both severity and the number of affected resources, guiding teams to address the most impactful vulnerabilities first.

## TABULAR LISTING OF REMEDIATION TASKS AND STATUS

A structured table lists all remediation tasks along with their current status — whether pending, completed, or failed — accompanied by relevant metadata to support tracking and follow-up.



## **PATCH AGING ANALYSIS**

A time-based line plot correlates the number of pending patches with their age in days, enabling teams to prioritize older patches that may pose greater risk.

## **PATCHING IMPACT VISUALIZATION**

A graphical representation plots the number of security rules fixed against the number of patches applied, offering clear insight into the effectiveness of remediation efforts.

## **PATCH JOB ORCHESTRATION WORKFLOW**

Outlines a simple, step-by-step process: select affected resources, review patch selections (with the option to skip uncertain fixes), enter scheduling details, assign a unique job name, and confirm job creation. This workflow simplifies the process from detection to remediation.

## **APPROVAL-BASED EXECUTION**


At the final stage of patch task creation, users with the appropriate permissions can authorize immediate execution or set the task aside for later approval, ensuring that only validated tasks proceed.

## **TASK STATUS AND APPROVAL DASHBOARD**

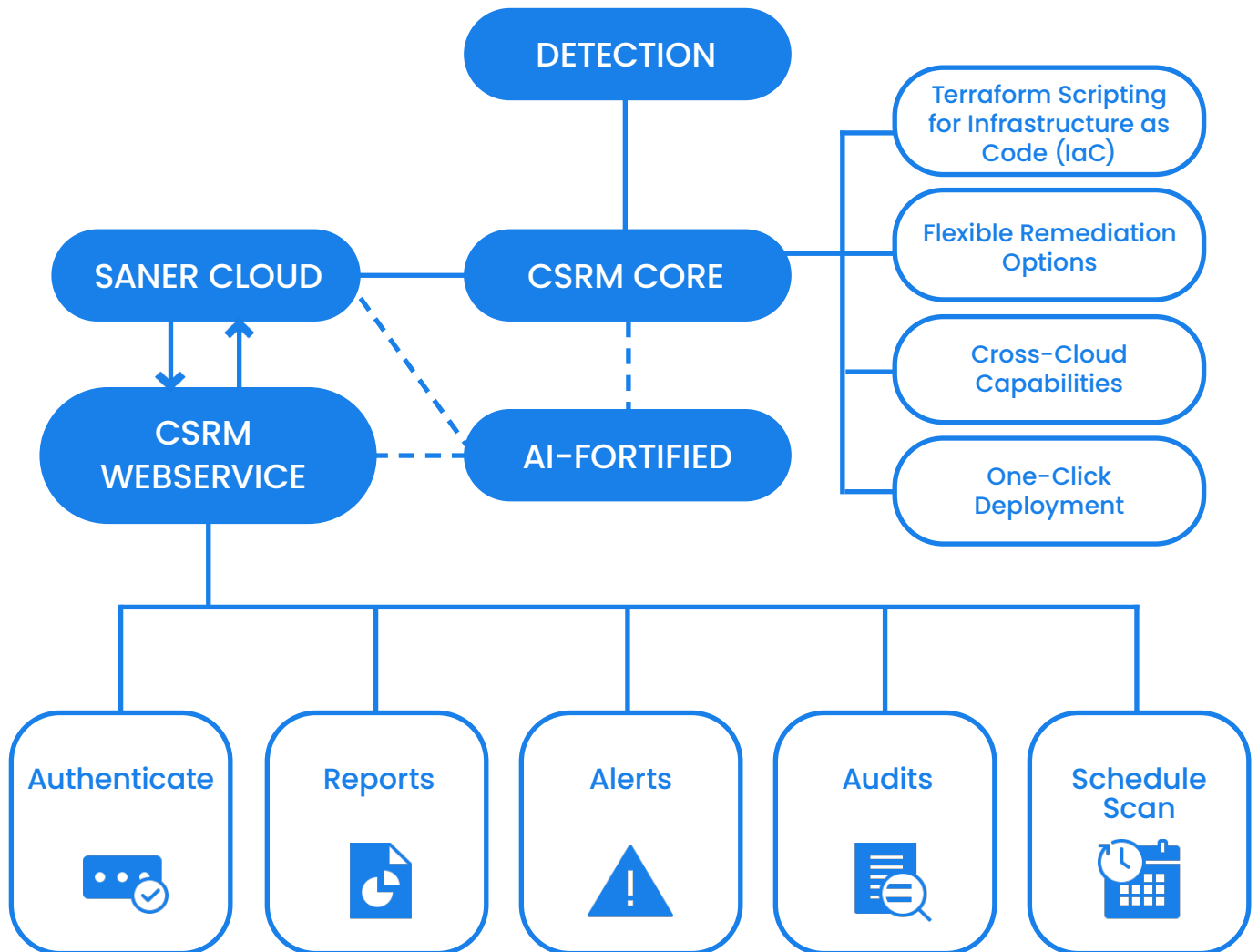
A dedicated dashboard offers real-time monitoring of patch execution and pending approvals, providing teams with a clear view of all ongoing remediation efforts.

## **AUTOMATED PATCHING ON SCHEDULE**

Enables users to configure recurring patching tasks that activate according to a predefined schedule. Once a scan identifies issues, patches are generated and applied automatically, reducing manual intervention and promoting continuous protection.



# Workflow Diagram



## Unparalleled Benefits of Saner CSRM



### RAPID ISSUE RESOLUTION

Automated workflows minimize the gap between vulnerability detection and patch application, significantly reducing the potential window for exploitation.



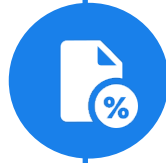
## OPTIMIZED SECURITY MANAGEMENT

Prioritized remediation and comprehensive tracking simplify the management of security fixes, freeing up valuable resources for other tasks.



## HOLISTIC OVERSIGHT ACROSS CLOUD MODULES

A unified dashboard consolidates remediation data from CSPM, CIEM, and CSPA, offering a complete view of your cloud security efforts.



## ACTIONABLE REPORTING FOR COMPLIANCE

Detailed logs and exportable reports support audit processes and help maintain compliance with industry standards



## FLEXIBLE REMEDIATION OPTIONS

The option to choose between job-based patching and automated patching, along with support for both predefined and custom patches, allows organizations to tailor remediation to their operational needs.

# One-Tool. Multifaceted Impact.

**A centralized view of all remediation tasks across multiple cloud services.**

**Detailed categorization with actionable insights to guide patching decisions.**

**Streamlined processes with one-click options and scheduled automation.**

**Exportable data and custom reporting to support audit and compliance efforts.**

## ABOUT SECPD

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](http://www.secpod.com)