secpod

SANER CLOUD

Cloud Identity Entitlement Management (CIEM)

DATASHEET

SANER CLOUD

Cloud Identity Entitlement Management (CIEM)

Cloud identities with excessive permissions pose a significant risk, as they can be exploited to gain access to sensitive data. CIEM continuously audits and reviews these access rights, applying automated adjustments to lower the chance of unauthorized operations. With a well-rounded CIEM, organizations gain the ability to maintain a strict control over cloud access, support compliance with regulatory frameworks, and reduce overall exposure to potential security breaches. But it's not easy to find a CIEM solution that effortlessly touches all bases.

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

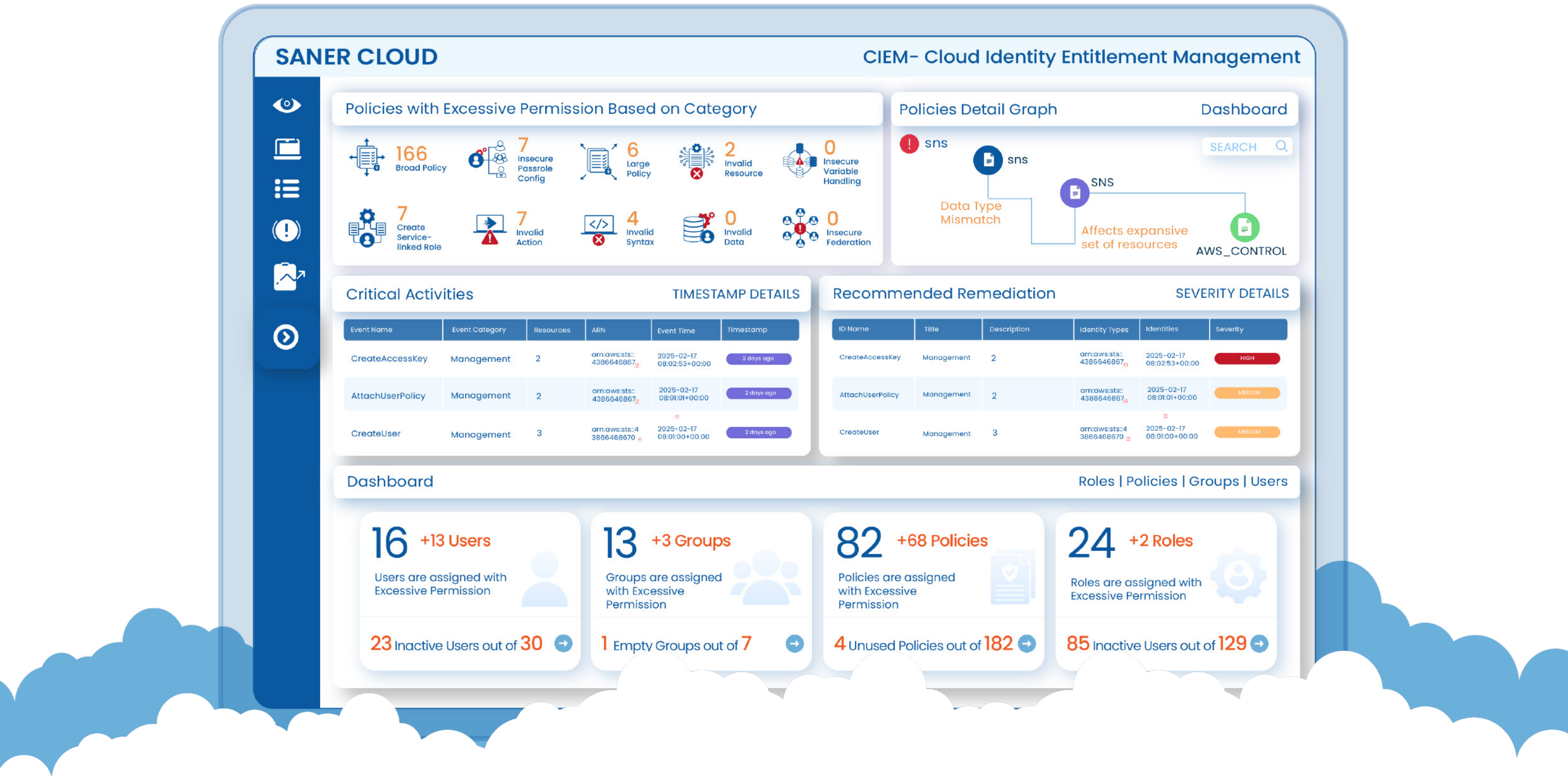
Handle Cloud Entitlements Completely Stress-Free

SecPod Saner CIEM provides a detailed perspective on cloud identity and entitlement management through continuous auditing and analysis of access permissions across diverse environments.

Using a structured entitlement framework, CIEM categorizes users, roles, and policies according to risk, activity, and compliance requirements. Data is presented through interactive visualizations — including trend graphs, charts, and detailed dashboards — that offer comprehensive insights.

These insights pinpoint excessive permissions, reveal misconfigurations, and track privilege trends over time, enabling teams to enforce least-privilege policies and mitigate access risks with precision.

Targeted at security professionals and IT teams, CIEM delivers a centralized dashboard that consolidates identity and access details from AWS, Azure, and other cloud providers. With features such as deep permission analytics, custom access reviews, and exportable audit logs in various formats, CIEM equips organizations to maintain rigorous control over cloud entitlements, streamline access management, and respond promptly to potential security threats across the infrastructure.



SANER CLOUD
CIEM- Cloud Identity Entitlement Management
Policies with Excessive Permission Based on Category
166 Broad Policy
7 Insecure Passrole Config
6 Large Policy
2 Invalid Resource
0 Insecure Variable Handling
7 Create Service-linked Role
7 Invalid Action
4 Invalid Syntax
0 Invalid Data
0 Insecure Federation
Policies Detail Graph
Dashboard
SEARCH
sns
sns
SNS
Data Type Mismatch
Affects expansive set of resources
AWS_CONTROL

Critical Activities — TIMESTAMP DETAILS

Event Name	Event Category	Resources	ARN	Event Time	Timestamp
CreateAccessKey	Management	2	arn:aws:sts::4386646867	2025-02-17 08:02:53+00:00	2 days ago
AttachUserPolicy	Management	2	arn:aws:sts::4386646867	2025-02-17 08:01:01+00:00	2 days ago
CreateUser	Management	3	arn:aws:sts::43866468670	2025-02-17 08:01:00+00:00	2 days ago

Recommended Remediation — SEVERITY DETAILS

ID Name	Title	Description	Identity Types	Identities	Severity
CreateAccessKey	Management	2	arn:aws:sts::4386646867	2025-02-17 08:02:53+00:00	HIGH
AttachUserPolicy	Management	2	arn:aws:sts::4386646867	2025-02-17 08:01:01+00:00	MEDIUM
CreateUser	Management	3	arn:aws:sts::43866468670	2025-02-17 08:01:00+00:00	MEDIUM

Dashboard — Roles | Policies | Groups | Users

16 +13 Users — Users are assigned with Excessive Permission — 23 Inactive Users out of 30

13 +3 Groups — Groups are assigned with Excessive Permission — 1 Empty Groups out of 7

82 +68 Policies — Policies are assigned with Excessive Permission — 4 Unused Policies out of 182

24 +2 Roles — Roles are assigned with Excessive Permission — 85 Inactive Users out of 129

“SecPod Saner CIEM offers continuous auditing, risk analysis, and visual insights for cloud identity and access management.”

A Holistic Overview of Your Cloud Entitlements

ENFORCE LEAST PRIVILEGE

Saner CIEM continuously audits user, application, and service permissions to verify that each identity operates with only the minimum access required. Excessive or unused privileges are automatically flagged and revoked, significantly reducing the opportunity for unauthorized actions.

DETECT MISCONFIGURATIONS

The solution scans for improper access arrangements that can lead to privilege escalation or unintended data exposure. It identifies risky settings and offers clear recommendations to adjust permissions appropriately.

AUDIT ACCESS

Comprehensive logging provides detailed records of access activities, including who holds which permissions and when changes occur. This complete audit trail supports compliance reviews and streamlines investigations into access-related incidents.

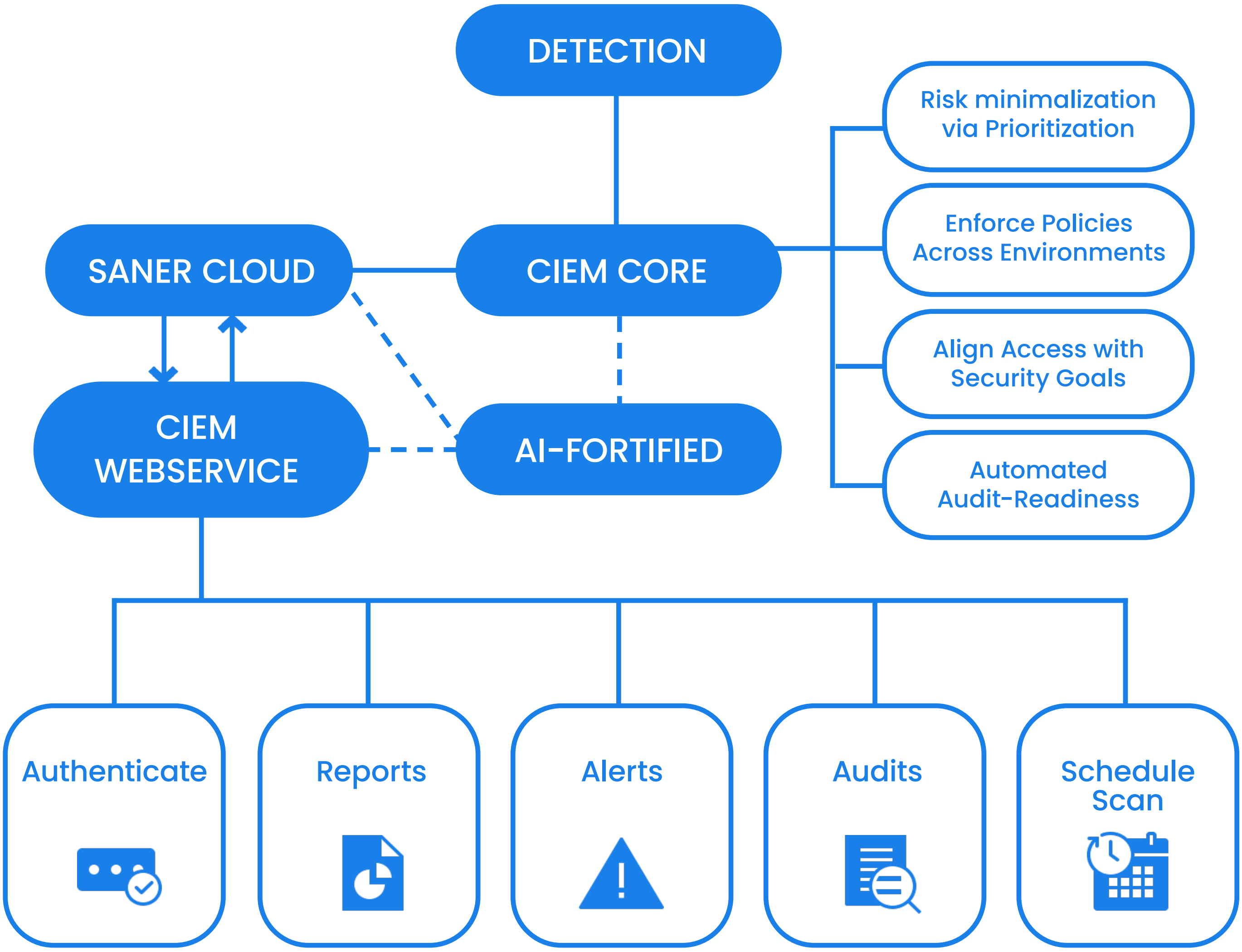
REMEDIATE RISKS

Automated recommendations and one-click remediation workflows empower teams to correct risky entitlements swiftly. CIEM identifies over-permissive roles and inactive accounts, prompting immediate actions to minimize potential exposure.

PROVIDE VISIBILITY

A centralized dashboard aggregates identity and access data from multiple cloud providers, presenting interactive charts and reports that deliver an at-a-glance view of cloud entitlements. It’s a consolidated perspective that enables informed decision-making and prompt adjustments to access controls.

Workflow Diagram


DETECTION
SANER CLOUD
CIEM CORE
CIEM WEBSERVICE
AI-FORTIFIED
Risk minimalization via Prioritization
Enforce Policies Across Environments
Align Access with Security Goals
Automated Audit-Readiness
Authenticate
Reports
Alerts
Audits
Schedule Scan

Unparalleled Benefits of Saner CIEM

AUTOMATICALLY DETECTS OVERLY PERMISSIVE POLICIES

CIEM continuously scans for users and roles that have more access than needed, flagging them as potential risks. Its automated routines examine permission configurations and highlight deviations from best practices.

USES PRE-BUILT POLICIES TO DETECT RISKY PERMISSIONS

By applying a set of predefined security rules, the system assesses access settings to pinpoint permissions that may expose vulnerabilities. Its rule-based approach simplifies the identification of risky configurations.

PROVIDES AUTOMATED RECOMMENDATIONS

Upon finding excessive or misconfigured access, CIEM offers clear, actionable suggestions that guide teams toward aligning permissions with a least-privilege model. These recommendations help speed up the remediation process.

CENTRALIZES DATA POINTS INTO ACTIONABLE INSIGHTS

CIEM gathers access-related data from diverse cloud environments and presents it through intuitive dashboards and reports. This consolidation turns raw information into clear insights for informed decision-making.

STREAMLINE ACCESS MANAGEMENT

The platform simplifies the review and adjustment of user and role permissions, reducing administrative overhead and accelerating the process of modifying access rights.

COMPREHENSIVE POLICY INVENTORY

Compiles a complete count of AWS policies — including inline, managed, and custom-managed — and classifies them into 15 categories based on their permissiveness. This organized inventory aids in prioritizing remediation efforts.

OVERLY PERMISSIVE AWS POLICIES ANALYSIS

Displays graphical insights into the 15 categories of overly permissive AWS policies, detailing which services and actions contribute to risky configurations and listing the applicable versions in use.

OVERLY PERMISSIVE AZURE ROLES ANALYSIS

Offers a detailed look at five categories of overly permissive roles in Azure, complete with graphics that clarify why these roles may lead to exposure, along with key usage details.

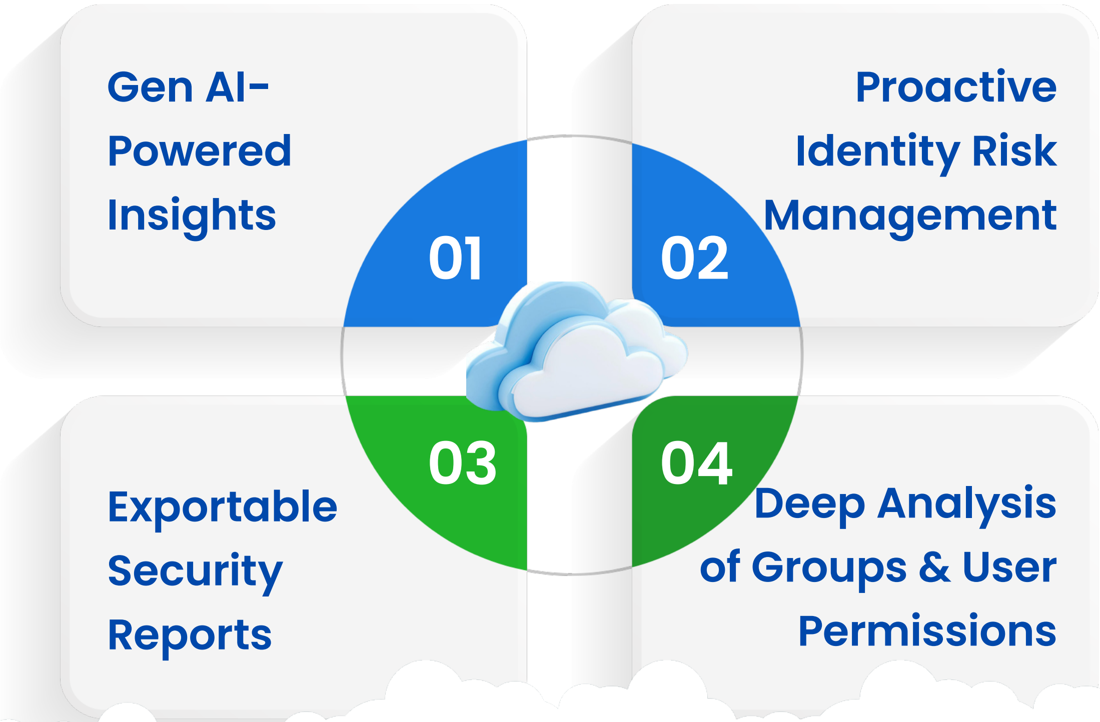
CIEM TREND GRAPH FOR SECURITY INSIGHTS

Tracks changes in cloud access over time with a trend graph that includes numerical indicators of increases or decreases in permissions. The visualization helps simplify the monitoring of access trends.

CRITICAL EVENT ANALYSIS

Monitors significant cloud events, such as failed login attempts and unusual access activities, on a daily basis. This regular review helps detect potential threats early.

One-Tool. Multifaceted Impact.



01 Gen AI-Powered Insights

02 Proactive Identity Risk Management

03 Exportable Security Reports

04 Deep Analysis of Groups & User Permissions

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