SANER CLOUD – CNAPP UNPACKED

The cloud moved fast, risk moved faster

www.secpod.com

The Cloud Reality Check

The Cloud Changed Everything - So Did the Risk

Cloud adoption skyrocketed. But security didn't keep pace.
Now, everything from exposed identities to unpatched workloads creates an open door for attackers.

- *76% of cloud breaches exploit misconfigurations*
- *Over 90% of cloud identities are over-permissioned*
- *Most CNAPP tools detect problems, but don't fix them*

"Your cloud is already being scanned - by attackers."

Why CNAPP Isn't Enough Anymore

Most CNAPPs Detect. Few Protect.

The CNAPP market is filled with stitched-together solutions.
They monitor. They alert. But they can't act. Saner Cloud is different - it was designed to prevent, not just observe.

- *Integrated Remediation*
- *One platform, one view*
- *Real-time posture correction*

"Alerts don't stop breaches. Action does."

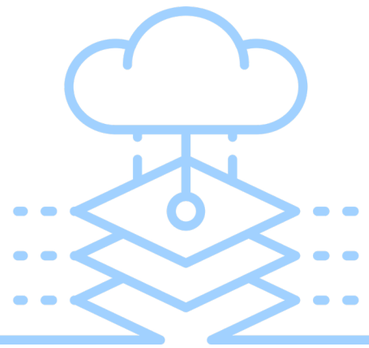
Meet Saner Cloud

The Industry's First Prevention-First CNAPP

Saner Cloud is an AI-powered Cloud-Native Application Protection Platform (CNAPP) that brings every layer of cloud security into a single solution. It helps organizations discover assets, monitor posture, detect anomalies, govern identities, and automate remediation, all from one unified dashboard.

OUR CORE PROMISE:

- *Continuous Security*
- *World's first CISA-SSVC Prioritization*
- *Zero-Touch Remediation*



"Security isn't a feature. It's a lifecycle. Saner Cloud runs it end to end."

VISUALIZE & NORMALIZE

Discover, normalize, and inventory cloud assets
(Modules: CSAE, CWPP)

DETECT & PRIORITIZE

Spot vulnerabilities, misconfigurations, anomalies, and beyond
(Modules: CSPA, CSPM, CSRP, CIEM)

REMEDIATE & MITIGATE

Act with precision - patch, fix, and configure instantly
(Modules: CSRM, CWPP)

LEARN & ADAPT

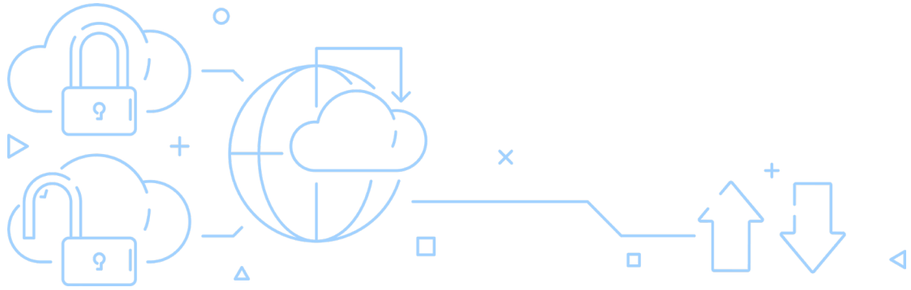
Feed threat intel and user context into the risk engine
(System-wide ML + behavior-driven re-ranking)

REPORT & ALERT

Notify, log, and visualize compliance posture and status
(Modules: Reporting Layer, Alerts, Audit Logs)

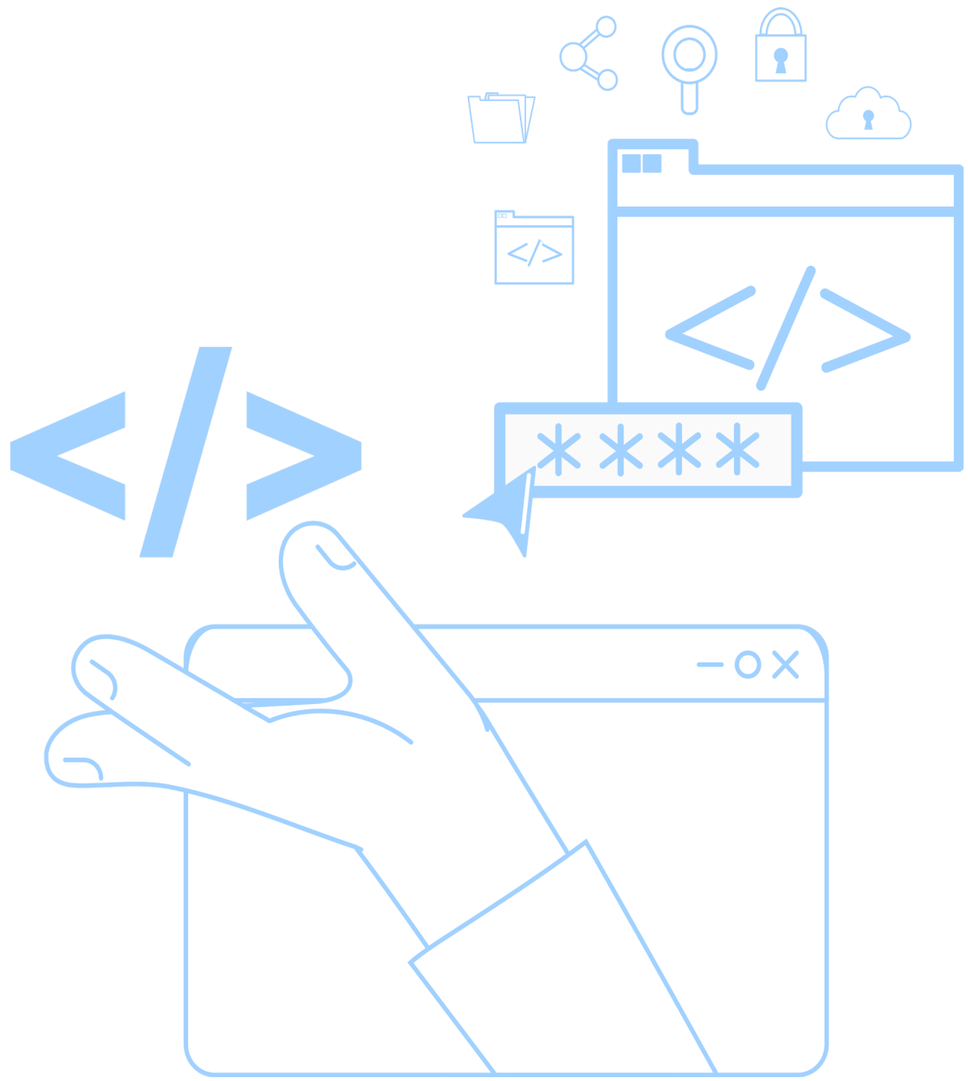
Inside the Saner Cloud Brain

Seven Modules. One Unified Platform.



Saner Cloud delivers full-stack cloud security with six seamlessly integrated modules:

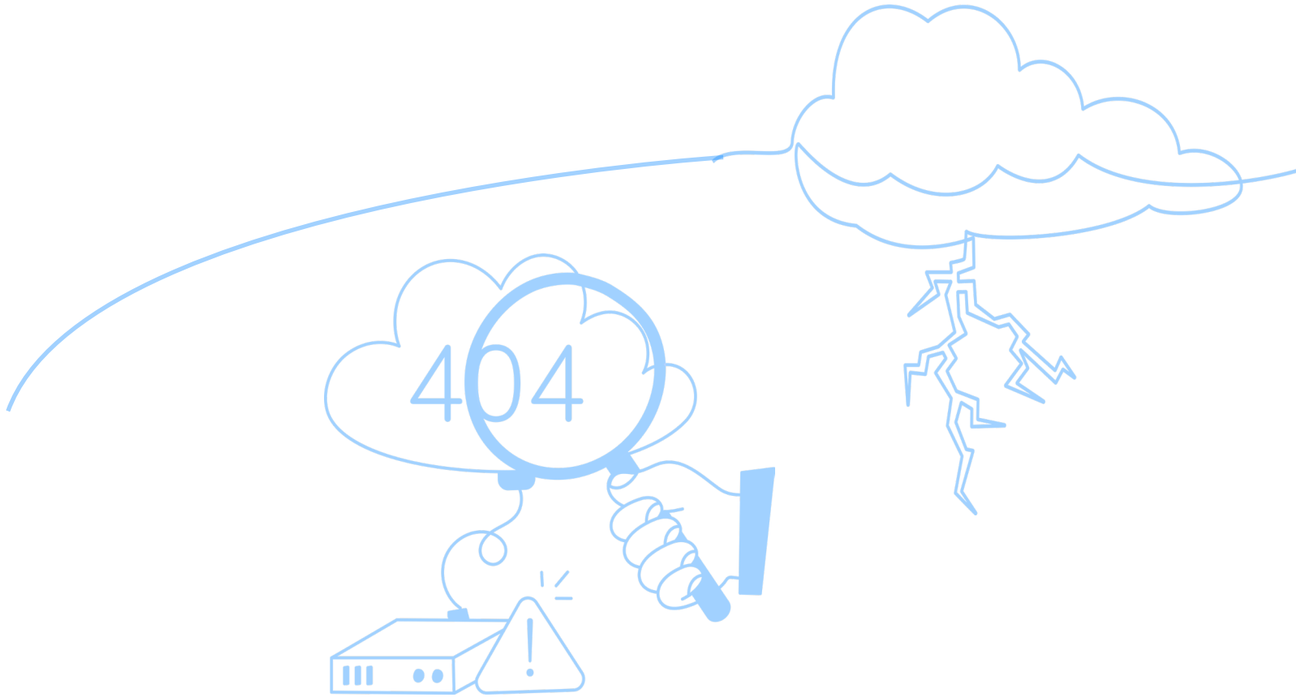
MODULE	WHAT IT DOES	WHO IT HELPS
CSAE	Asset Exposure	Cloud Infra, Security Ops
CSPA	Posture Anomalies	Threat Analysts
CSPM	Misconfiguration & Compliance	Risk & Compliance
CIEM	Identity Entitlements	IAM, DevOps
CSRP	Risk prioritization	IT & Platform Engineers, CloudOps
CWPP	Workload Protection	IT & Platform Engineers
CSRM	Remediation Management	SOC, CloudOps



“Everything cloud security should be. In one place.”

See What You Couldn't Before – With CSAE

Cloud Security Asset Exposure (CSAE)



Visibility Is the Foundation of Security. CSAE Makes It Total.

Most breaches happen because something was left unnoticed — an open port, an outdated image, an unaccounted-for public IP. CSAE brings unmatched visibility into every cloud asset, helping you eliminate shadow IT and catch exposures before attackers do.

KEY CAPABILITIES + HOOKS:

Publicly Accessible Resources
Surface internet-facing assets — even the forgotten ones

"If you can't see it, you can't secure it."

Outdated Resources
Find and flag stale or unsupported assets before they become liabilities

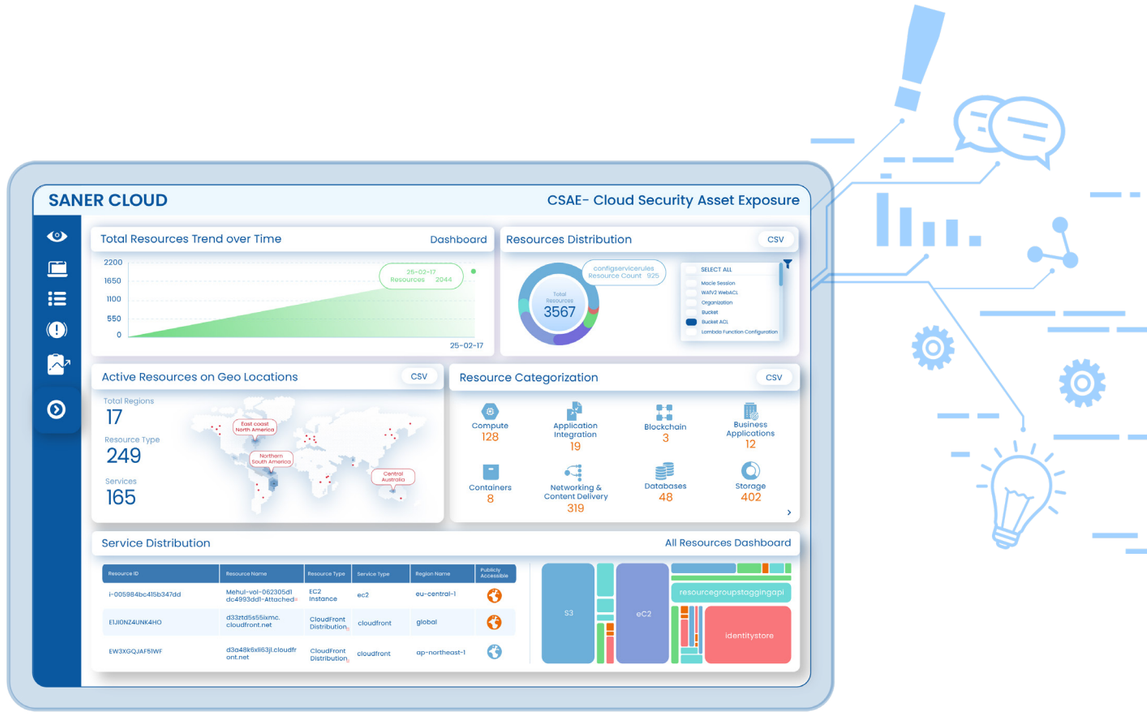
Legacy VMs still running in shadow subnets

Watchlisted Resources
Auto-flag critical assets for priority monitoring

"Spot the crown jewels — and guard them first."

Cost & Usage Analysis
Connect security risk with real cost impact

High-risk, low-usage assets draining budgets



Anomalies Aren't Errors – They're Warnings.

Cloud Security Posture Anomaly (CSPA)

CSPA Detects the Unexpected. And Fixes It Instantly.

Misconfigurations don't always look like vulnerabilities. CSPA brings Machine Learning-based posture assessment to cloud security — surfacing unexpected changes and making it easy to respond before risk turns into damage.

KEY CAPABILITIES + HOOKS:

Detailed Anomaly Insights
Context-rich anomaly feeds for faster triage

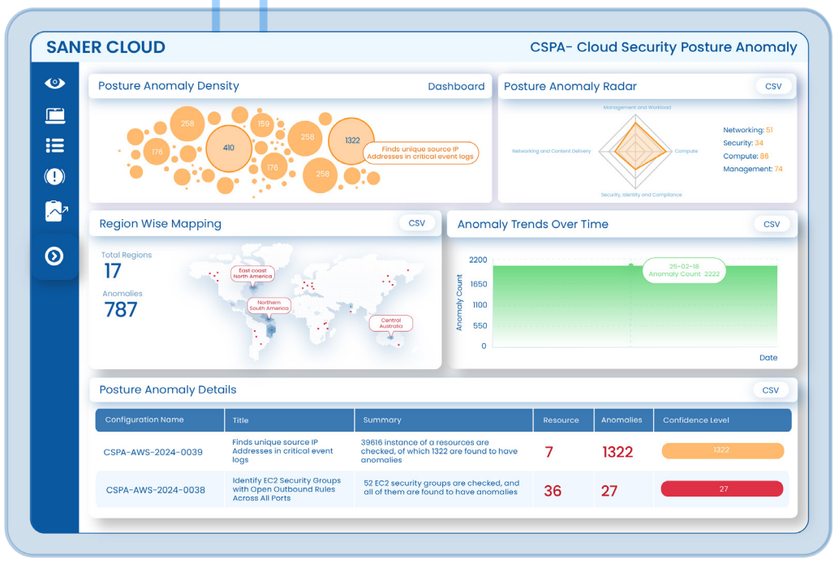
Detect configuration drift in newly provisioned workloads

Anomaly Category Bubble Graphs
Visualize where your posture is breaking

One-Click Remediation
Resolve issues straight from detection

"If it's not normal, fix it before it's fatal."

Custom Whitelists
Filter out noise, stay focused on what matters



Prevent Misconfigurations From Becoming Breaches

Cloud Security Posture Management (CSPM)

CSPM Enforces Best Practices. Even When No One's Looking.

Security is about doing the right thing every time, not just when someone's watching. Saner Cloud's CSPM module runs continuous compliance and configuration checks across all your cloud accounts - AWS, Azure, hybrid, and beyond.

KEY CAPABILITIES + HOOKS:

Benchmark-Based Audits (NIST, CIS, PCI-DSS)

"Always audit-ready — even when the audit is a surprise."

Geo-Distribution Heatmaps

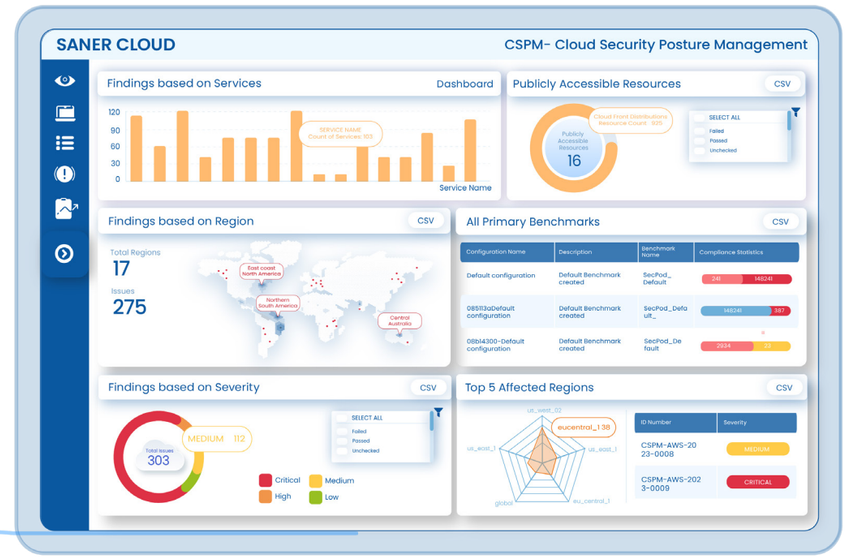
Visualize non-compliance by region and provider

Custom Benchmarks + One-Click Fixes

Compliance teams create internal policies and remediate at scale

Trend Over Time View

Know if you're improving or slipping



CIEM - Fix the Most Dangerous Permissions in the Cloud

Every Identity Is a Risk - Unless It's Controlled

Identity is the new perimeter - but in the cloud, it's also the most overlooked attack vector. Over-permissive roles, abandoned credentials, and unknown privileges expose you to silent, invisible threats.
Saner Cloud's CIEM module unmasks and corrects dangerous identity configurations so you can enforce least privilege, reduce risk, and pass audits with confidence.

KEY CAPABILITIES & HOOKS:

Over-Permissive Identity Detection
Detect roles with excessive privileges, and trim them to what's essential.

"Nobody should have God Mode - not even admins."

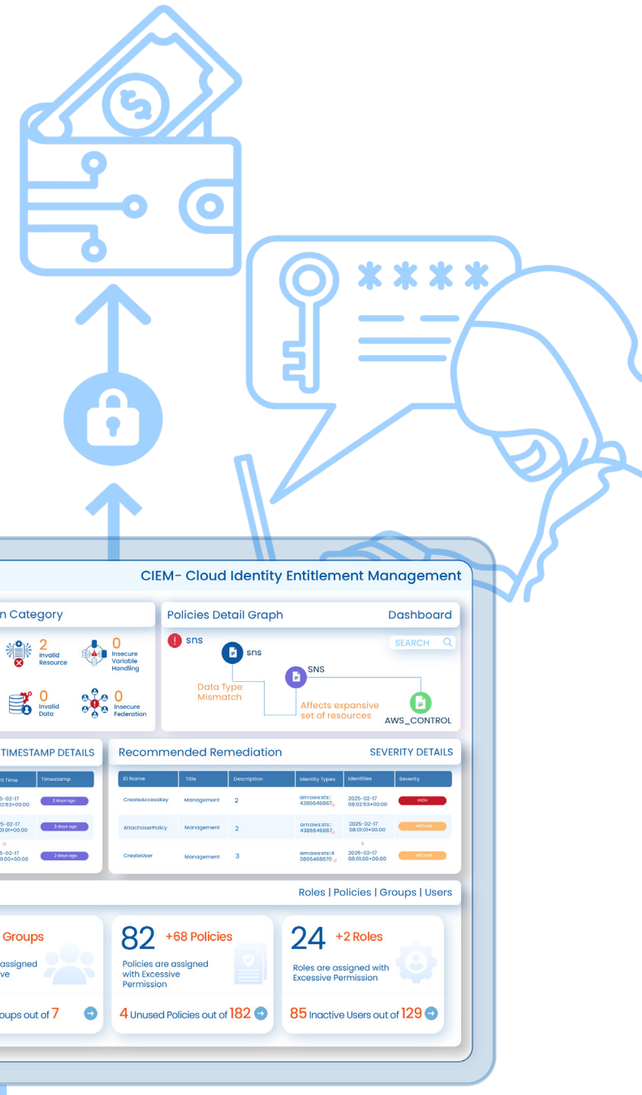
Unused Roles and Groups Detection
Eliminate legacy or orphaned identities before they're exploited.

Critical Activity Logging + Evidence Trails
Full visibility into sensitive actions and privilege misuse.

"See who did what, when - and whether they should've."

Visual Access Graphs for Entitlements
Map users, groups, and resource access in a single view.

Built-In Fix Suggestions and Role Right-Sizing
Replace admin-level access with scoped-down alternatives in one click.



CSRP – Focus on what truly matters in your cloud

Thousands of alerts pour in daily — most aren't worth your team's time. Saner Cloud's Cloud Security Risk Prioritization (CSRP) transforms that noise into a ranked plan of action. It applies CISA's SSVC model and MITRE ATT&CK mapping to classify each risk by exploitability, automation potential, impact, and business criticality. The result: your team acts fast on what could actually be weaponized — and ignores what won't.

KEY CAPABILITIES & HOOKS:

SSVC-based Decisioning
Every risk is labeled Act, Attend, Track, or Track* based on real exploitability and urgency.

Act, Attend, Track or Track — pick the next move, fast.*

Exploitability & Automation Signals
Identify risks already exploited in the wild or easily weaponized at scale.

Technical Impact Insights
See how deep an attacker could go from partial access to complete compromise.

Essential Resource Awareness
Auto-prioritize exposures tied to mission-critical workloads or assets.

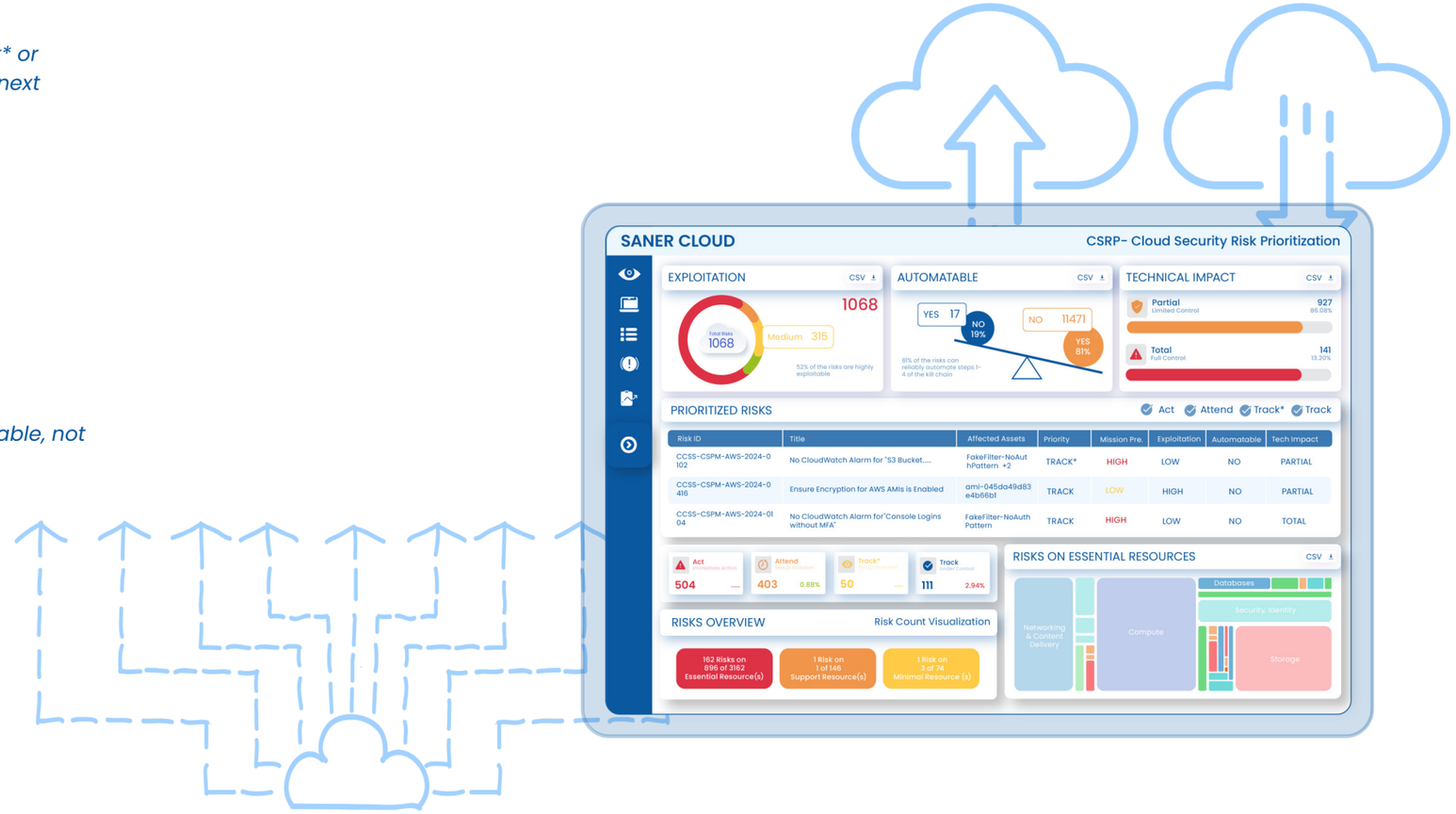
ATT&CK Mapping & Mitigations
Understand adversary intent and instantly view mapped mitigations.

Turn findings into a ranked plan, not another list.

Unified Risk Dashboard
Visualize exploitability, impact, and asset exposure across AWS and Azure.

Remediation Integration
Push prioritized issues directly to Saner Cloud's CSRM for immediate or scheduled fixes.

Fix what's exploitable, not just what's loud



CWPP - Hardening Your Cloud Workloads in Real Time

Your VMs, Containers, and Servers. Secured by Default.

Traditional workload protection tools demand complex setups, heavy agents, and siloed ops. Saner Cloud's CWPP module is built for the cloud — lightweight, scalable, and automated from day one.
It gives you full visibility into workload posture and lets you fix vulnerabilities, misconfigurations, and software gaps at scale — with zero friction.

KEY CAPABILITIES & HOOKS:

Deep Workload Visibility
Scan containers, VMs, OS layers for vulnerabilities and misconfigs.

"Know exactly what's running, where, and how secure it is."

Posture-Aware Patching
Use Case: Detect & patch exploitable vulnerabilities using built-in workflows.

Regulatory Compliance Enforcement
Fix misconfigs that breach compliance automatically.

Frameworks: HIPAA, PCI-DSS, NIST, CIS

Full Workload Management
Install software, push scripts, or initiate remote sessions with one click.

"Fix, update, or tune workloads — without logging into each machine."

Real-Time Action Dashboard
Use Case: Track patch success, workload health, and risk levels across all environments.

CSRM – Your Command Center for Cloud Remediation

Security Isn't a Ticket. It's a Closed Loop.

Saner Cloud's Cloud Security Remediation Management (CSRM) module turns findings into fixes — not just alerts. It stitches together vulnerabilities, posture anomalies, identity misconfigs, and converts them into structured remediation workflows.
With automated enforcement, scheduled fixes, and approval gates, it's the control plane your security team has been waiting for.

KEY CAPABILITIES & HOOKS:

Zero-Click True Remediation
Fixes triggered instantly on detection — across modules.

"No more patching panic. Just precision auto-remediation."

Patch Aging + Impact Graphs
Prioritize older, higher-risk vulnerabilities that haven't been patched in time.

Scheduled Auto-Remediation
Define windows to apply fixes in low-traffic hours.

"Security, while you sleep."

Admin Approval Workflow
Maintain control — only apply changes once

Unified Remediation Across Modules (CSPA, CSPM, CIEM)
Differentiator: One pane to manage fixes across cloud posture, anomalies, and identities.

Remediation Status Dashboard
Track what's been fixed, what's pending, and what's failed — in real time.

The Heart of Automation

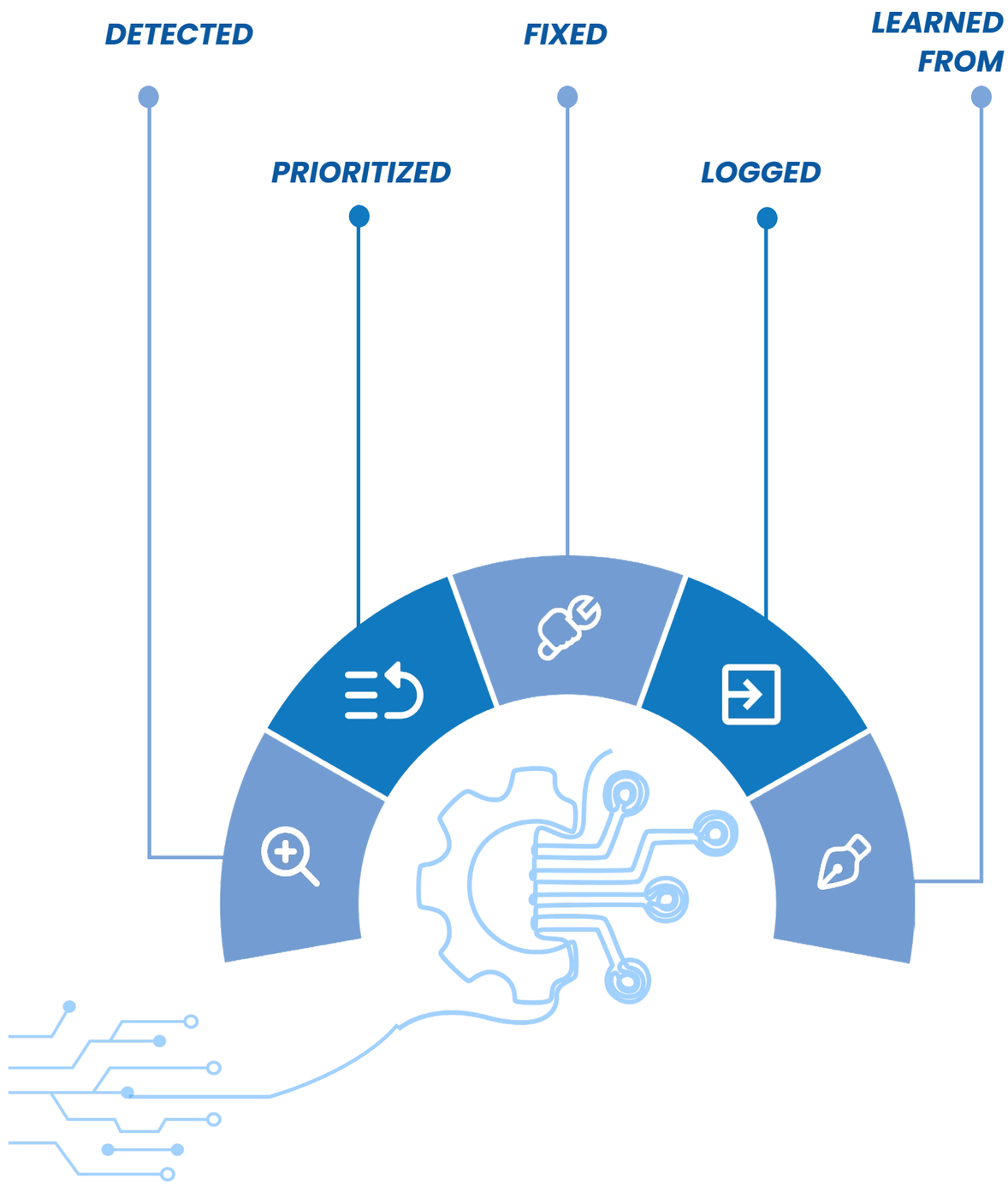
From Detection to Remediation - Without the Delay

Saner Cloud isn't just another CNAPP with dashboards and alerts. It's built on a deeply embedded automation engine that does what most security tools only promise: act. Automatically. Intelligently. At scale.
This is where our AI-driven core powers zero-touch security - from flagging anomalies to fixing them before your teams even log in.

WHAT POWERS OUR AUTOMATION?

ENGINE	WHAT IT DOES	REAL IMPACT
AI Risk Prioritization	Context-aware scoring based on exploitability, asset value, and privilege misuse	Your team focuses on what matters most — no false alarms
Zero-Touch Remediation	Automatically patch mis-configs and vulnerabilities with no human intervention	Reduce MTTR and stop breaches before they begin
Remediation Intelligence Layer	Ties together findings from CSPM, CSPA, CIEM to drive fix workflows	True multi-module orchestration
Behavioral ML Models	Detect patterns, anomalies, and deviations from security baselines	Prevents configuration drift and detects insider threats

"Why settle for detection dashboards, when you can have a system that fixes things on its own?"



Why Saner Cloud Is Built Differently

Security Doesn't Work in Silos. Neither Do We.

While other solutions stack disconnected tools and dashboards, Saner Cloud is natively integrated from the ground up. It brings together visibility, risk context, automated remediation, and policy enforcement — all within a unified architecture.

WHY IT MATTERS:

- *No dependency on third-party engines or patchwork integrations*
- *Shared intelligence across modules — detection informs remediation in real time*
- *Native remediation built for each layer of the cloud stack*
- *One agentless, high-performance architecture*

"One Platform. Total Security."

The Saner Cloud Advantage - In One View

Five Layers. One Platform. Zero Gaps.

From visualizing misconfigurations to enforcing remediations - Saner Cloud's five-part security loop ensures nothing falls through the cracks.

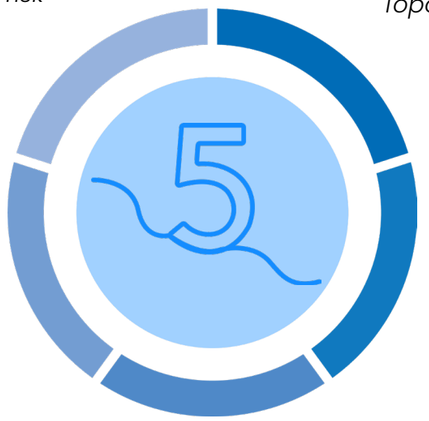
THE FIVE-PART SANER SECURITY LOOP:

Learn & Optimize

- *Trend analysis*
- *Machine learning-based recommendations*
- *GenAI-assisted risk evaluation*

Visualize & Normalize

- *Infra Dashboards*
- *Grouping & Tagging*
- *Asset Inventory & Topology*



Monitor & Enforce

- *Real-time dashboards*
- *Alerting, audit logs*
- *Compliance policy enforcement*

Detect & Prioritize

- *Risk-based posture scoring*
- *AI-powered anomaly detection*
- *Identity misconfig detection*

Remediate & Mitigate

- *True zero-click remediation*
- *Scheduled enforcement*
- *Policy-based access correction*

Who Trusts Saner Cloud

Trusted by Modern Enterprises and Security Teams That Think Ahead

Whether it's a global enterprise, a cloud-native scale-up, or a managed security provider - Saner Cloud powers prevention-first security across hybrid and multi-cloud environments.

USE CASES ACROSS INDUSTRIES:

Financial Services
Remediating misconfigurations in sensitive environments

Healthcare
Ensuring HIPAA and NIST compliance at workload level

Tech & SaaS
Managing thousands of identities and workloads with one console

MSSPs
Running security for multiple clients through a multi-tenant view

Ready to See Saner Cloud in Action?

Don't Just Detect. Remediate. Automatically.

Your cloud environment doesn't need more alerts. It needs a security platform that fixes what it finds - in real time, without noise, and at enterprise scale.

LET'S SHOW YOU HOW SANER CLOUD TRANSFORMS CLOUD SECURITY.

Schedule a personalized demo

Get started with a free trial

Talk to a security expert