secpod

TECHNICAL BRIEF

SANER CLOUD

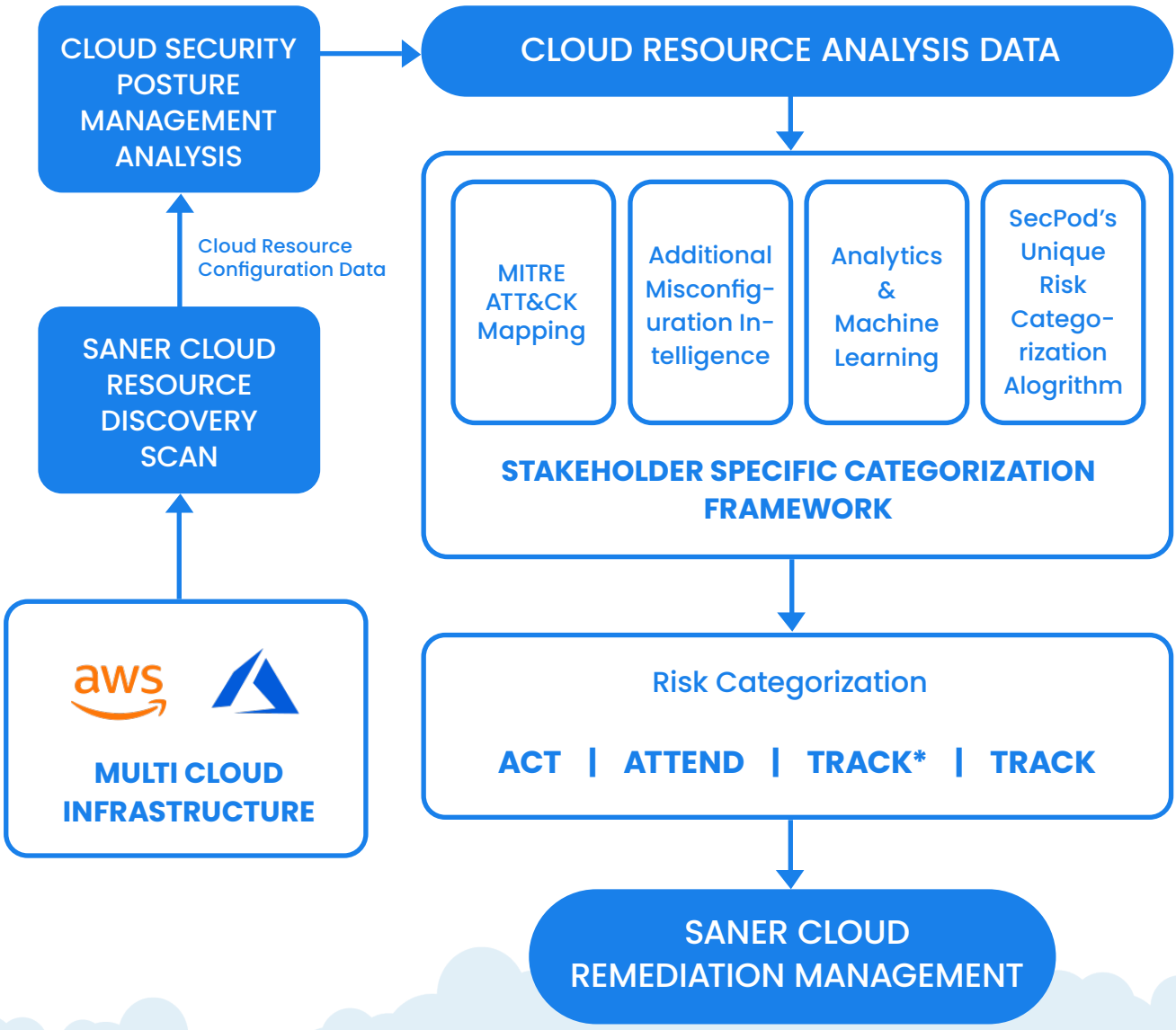
Cloud Security Risk Prioritization - CSRP

www.secpod.com

Introduction

Cloud environments generate tens of thousands of misconfigurations, risks, and exposures across accounts and services. CSRP reduces this noise into a prioritized list of cloud risks that require immediate action. The prioritization model evaluates based on exploitability, automation feasibility, technical impact, and mission relevance — helping security teams act where it matters most.

To operationalize this, CSRP adapts CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) into a decision tree tailored for cloud. The model classifies each cloud risk into one of four actionable categories: Track, Track*, Attend, and Act.



An Overview of Saner Cloud Risk Prioritization

Saner Cloud Risk Prioritization (CSRP) evaluates and mitigates cloud risk across AWS and Azure using clear inputs and decision points.

It ingests large-scale misconfiguration and resource data from the Cloud Security Asset Exposure (CSAE) and Cloud Security Posture Management (CSPM) modules, combines it with contextual intelligence from threat feeds, in-built malware mapping and the MITRE ATT&CK Cloud Matrix , and produces a prioritized list of actionable risks.

Key highlights include:

SSVC-Based Framework

Adapts CISA's SSVC model for cloud-native workloads, making risk decisions more contextual and actionable.

Comprehensive Analytics

Correlates misconfigurations with live threat data, exploitability scores, and automation feasibility.

AI & ML-Driven Scoring

Uses machine learning to continuously refine prioritization outcomes based on new evidence or evolving cloud conditions.

Integrated Remediation Pathways

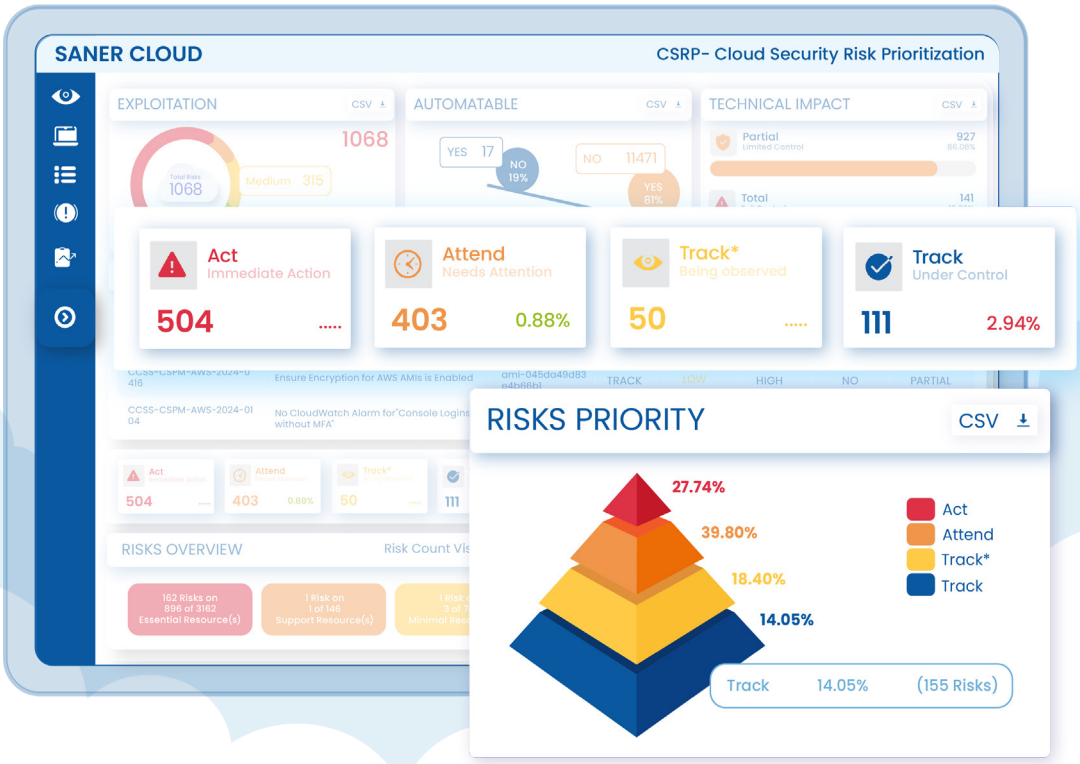
Links directly with Saner Cloud Remediation Management for automated patching, policy enforcement, and rollback support.

Multi-Cloud Coverage

Supports heterogeneous cloud infrastructures, analyzing cross-account, cross-service, and cross-region risks through a unified lens.

Through these capabilities, Saner Cloud Risk Prioritization enables organizations to:

1. **Focus on critical risks first, not just high-volume alerts.**
2. **Enhance cloud security hygiene through continuous assessment.**
3. **Accelerate remediation workflows through automation-ready intelligence.**



Exploitability in Cloud

Exploitability is computed by correlating cloud misconfigurations with:

1. **Threat intelligence feeds (CISA KEVs, Project Zero, vendor advisories).**
2. **MITRE ATT&CK Cloud Matrix mappings.**
3. **SecPod's Risk–to–Malware Enumeration (MVE) dataset.**

Each cloud risk is assigned an Exploitability Score (High, Medium, Low) indicating the likelihood of exploitation within the cloud control plane or workload environment.

Automatable Cloud Risks

Automatable assesses: Can an attacker reliably automate exploitation of this cloud misconfiguration?

Reconnaissance

Attackers gather information about the target, such as identifying vulnerabilities, employee details, and the organization's technical infrastructure.

Weaponization

The attacker develops a malicious payload, such as malware or a virus, to exploit the target's vulnerabilities.

Delivery

The weaponized payload is sent to the target, often through phishing emails, infected attachments, or exploiting network vulnerabilities.

Exploitation

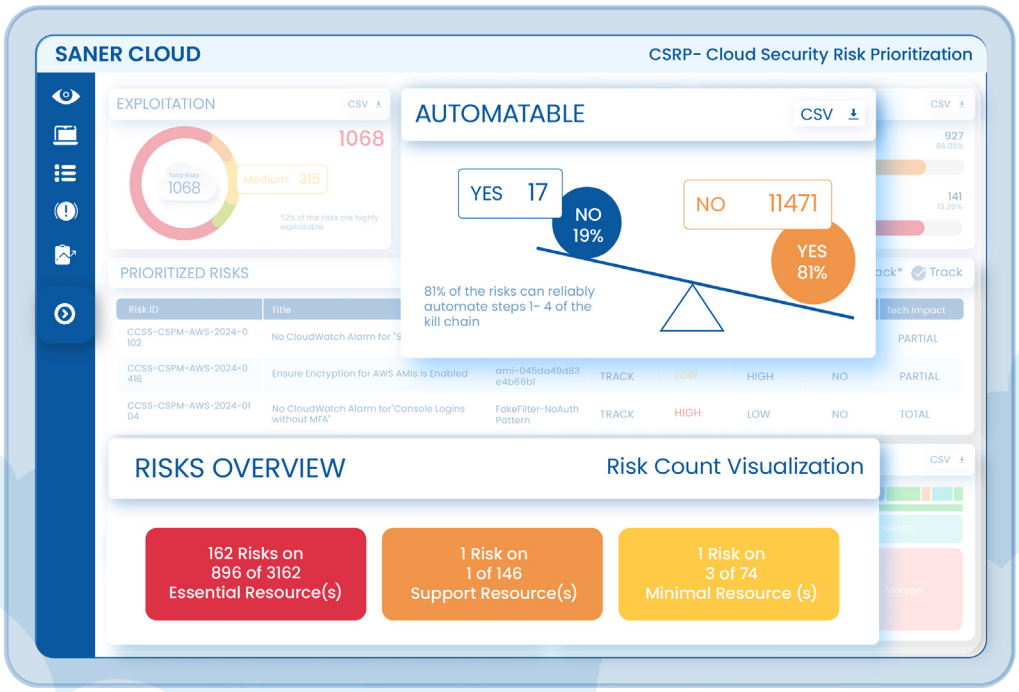
The malicious code runs on the target system, exploiting the identified vulnerability to gain unauthorized access.

If steps 1–4 of the cyber kill chain can be automated with no user input, the risk is flagged as Automatable = Yes.

Multiple factors help determine that Steps 1-4 of Kill Chain can be reliably automated such as

- determining if a device is internet facing and enumerable on the network,
- if CCE weaponization is possible through chaining
- delivery that checks if channels that cannot be blocked by widely deployed network security configurations and
- if there is an exploitation mitigation mechanism that is already in place that frustrates attackers from automating the attack, this considers MITRE ATT&CK Techniques, Tactics and Mitigations mapping with CCEs, and evaluating these automated checks with scan.

A set of questionnaires also aids to answer some of the data points that cannot be automated through scan. These helps assuring the Automatable value.



Technical Impact in Cloud

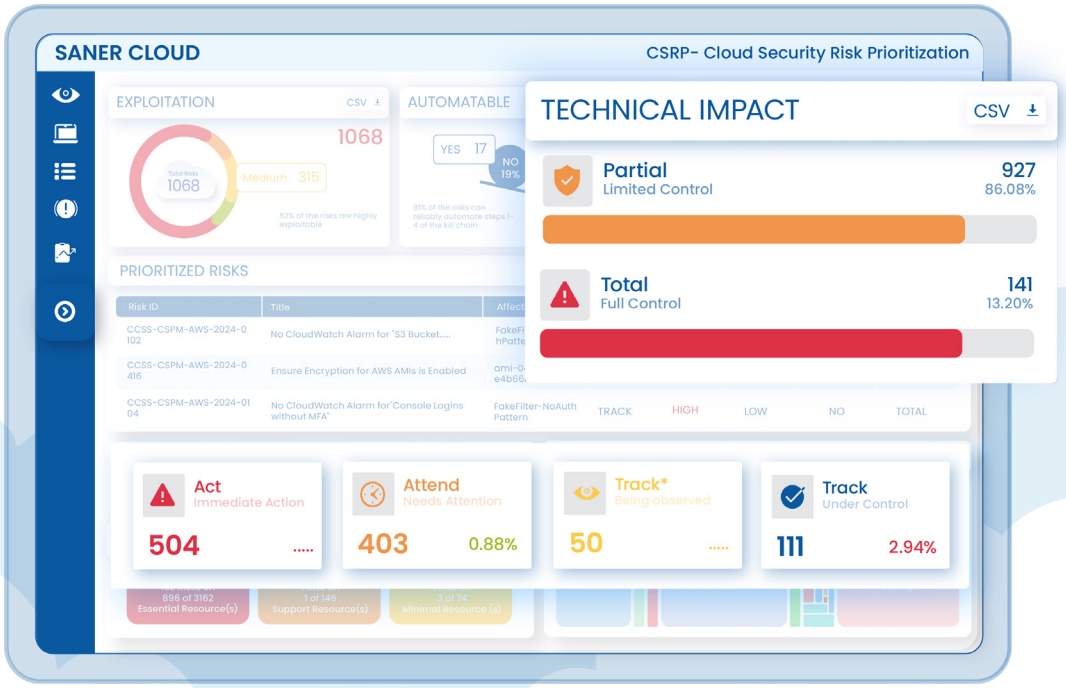
Technical impact is similar to the Common Cloud Scoring System (CCSS) base score's concept of "severity." When evaluating technical impact, the definition of scope is particularly important.

The decision point, "Total," is relative to the affected component where the misconfiguration resides. If a misconfiguration discloses authentication or authorization credentials to the system, this information disclosure should also be scored as "Total" if those credentials give an adversary total control of the component.

In condense we can understand that technical impact measures the degree of compromise if the misconfiguration is exploited:

1. **Total:** Complete compromise of cloud resources or credentials (e.g., IAM keys, role assumption).
2. **Partial:** Limited disruption, data disclosure, or scoped privilege escalation.

Detection uses CCE mappings, information disclosure patterns (e.g., leaked secrets in S3/EBS), and natural language parsing of misconfigurations to evaluate severity.

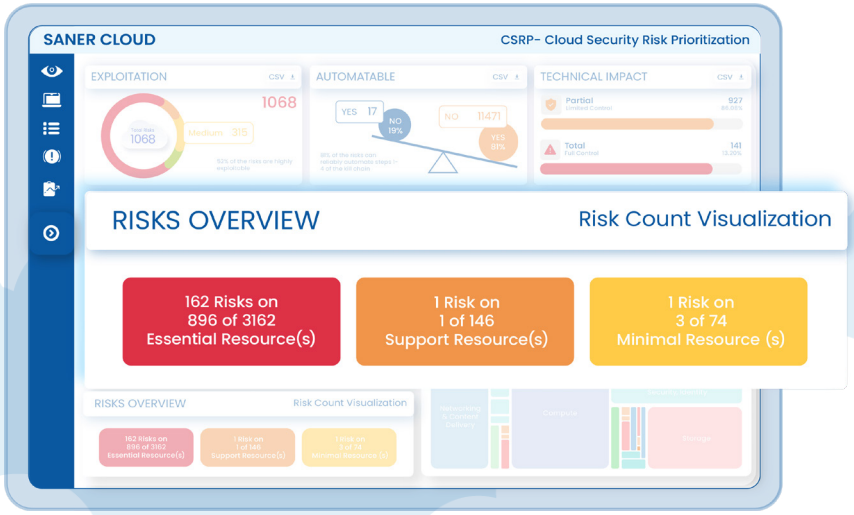


Mission Prevalence in Cloud

Mission Prevalence determines whether the affected resource is tied to Mission Essential Functions (MEFs):

1. **Essential: Business-**critical workloads, perimeter-facing systems, sensitive data stores.
2. **Support:** Services that enable or indirectly support MEFs.
3. **Minimal:** Ancillary or test resources with low business impact.

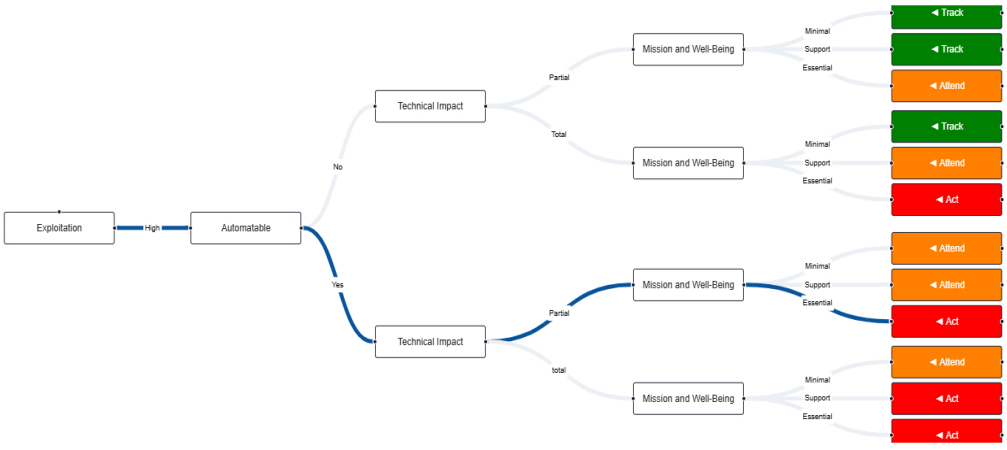
Cloud context enriches this by factoring in tags, metadata, and resource relationships (e.g., production vs. dev VPC, critical SaaS integrations, storage tiers).



Decision Tree Outcomes

The values of Exploitability, Automatable, Technical Impact and Mission Prevalence helps reach to a decision and prioritizes whether the risk should be acted upon immediately.

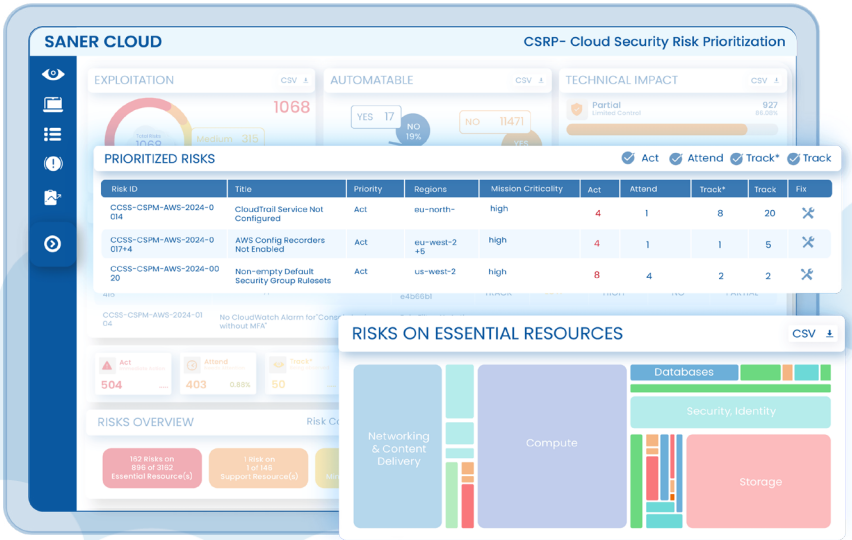
1. **Track:** No immediate action; monitor under standard patch/config timelines.
2. **Track*:** Requires close watch due to potential escalations or dependencies.
3. **Attend:** Escalate to supervisory stakeholders; may require broader notification or staged remediation.
4. **Act:** Urgent mitigation required; immediate patch, config change, or service restriction.



A detailed listing of Risk Prioritization is showed in a tabular format. Search, sort and Filters are in place for sieving risks, intellectualize, understand impact on resources & apply mitigations.

Mitigation & Remediation

Each prioritized Cloud Risk is mapped directly to MITRE ATT&CK Mapping helping analysts understand the criticality of the Cloud Risk and how it is part of the attacker lifecycle. Each risk can be fixed using SanerCloud Remediation Management (CSRM) feature. A single click on Fix symbol next to Risk ID from dashboard can redirect to RM remediation interface. Remediation tasks or automation can be created easily and tracked using the Remediation Management Interface.



Unique Capabilities

Cloud-Native SSVC Decisioning	contextualizes exploitability and mission impact per service based on business impact of the resources.
Threat Intelligence-Driven Scoring	continuously updates from KEV, MVE, and ATT&CK feeds.
Cross-Module Integration	unifies CSAE (asset data), CSPM (misconfigurations), and CSRM (remediation).
Actionable Analytics Dashboard	interactive filters, visualizations, and trend charts.
Remediation-Ready Design	With Automated Remediation minimal user interaction is needed to remediated priority risks identified.

About SecPod

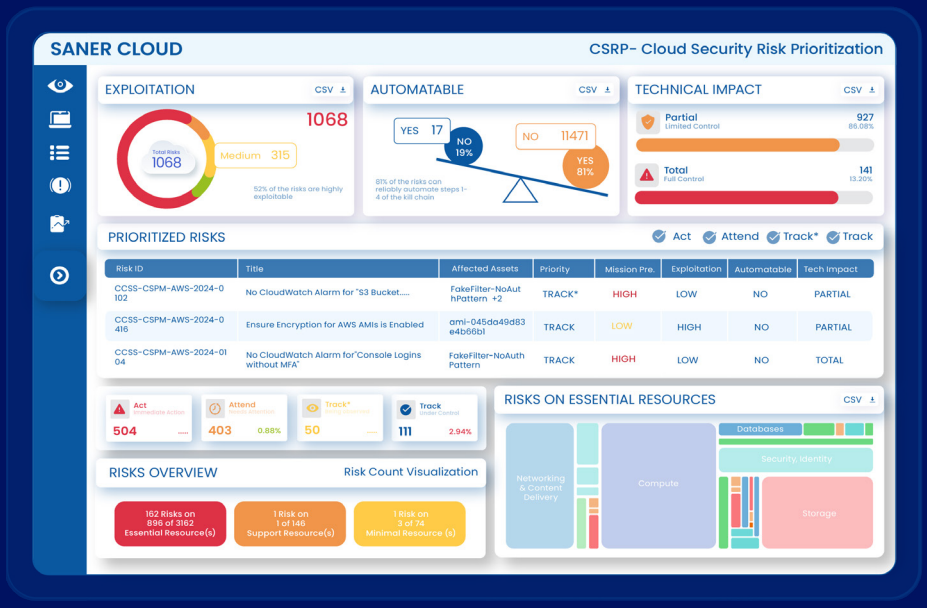
SecPod is a leading cybersecurity technology company committed to preventing cyberattacks through proactive security. Its mission is to secure computing infrastructure by enabling preventive security posture.

At the core of SecPod's offerings is the Saner Platform - a suite of solutions that help organizations establish a strong security posture to preemptively block cyber threats. The platform includes:

1. **Saner Cloud –** An AI-fortified Cloud-Native Application Protection Platform (CNAPP) that delivers continuous visibility, security compliance, and risk mitigation for cloud environments.

2. **Saner CVEM –** A Continuous Vulnerability and Exposure Management (CVEM) solution that delivers continuous visibility, identifies, assesses, and remediates vulnerabilities across enterprise devices and network infrastructure.

With its suite of cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.



Focus on the risks that truly matter.

Saner Cloud CSRP intelligently prioritizes misconfigurations based on exploitability, automatability, mission prevalence, and business impact, empowering you to remediate faster.