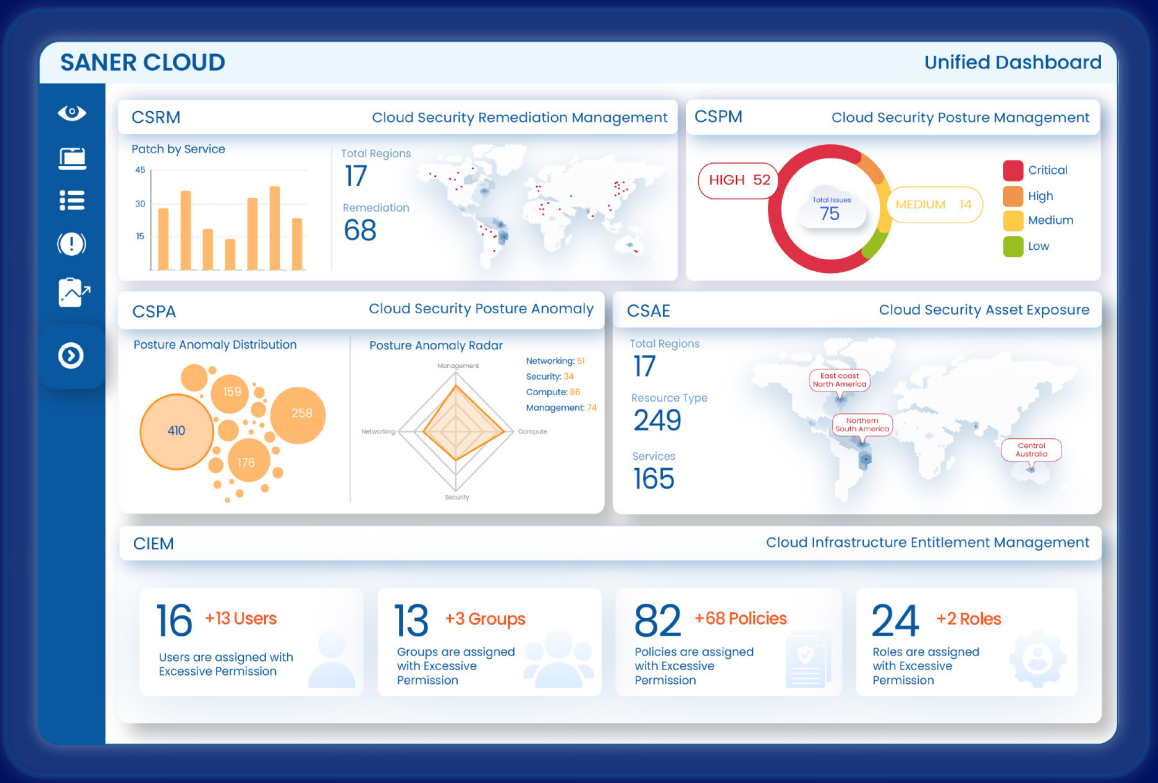
secpod

SANER CLOUD



Saner CNAPP Features Document

www.secpod.com

Table of Contents

Introducing Our AI-Fortified CNAPP:

A Unified Approach to Cloud Security

The modern enterprise is built on a complex and diverse Infrastructure - endpoints, cloud configurations, network devices, workloads, and much more. Yet, security solutions remain fragmented, forcing organizations to juggle multiple dashboards, decipher mixed vulnerabilities and misconfigurations, and struggle with a lack of clear segregation between sub-products. The result? Security teams overwhelmed with alerts, critical issues lost in the noise, and inefficient remediation processes that slow down response times.

At SecPod, we believe cloud security should be different. That's why we are excited to introduce our AI-powered Cloud-Native Application Protection Platform (CNAPP), a solution designed to transform cloud security operations with clarity, intelligence, and seamless automation.

What is Saner CNAPP?

Saner CNAPP is a comprehensive cloud security solution that integrates six AI-fortified products to provide robust protection for cloud environments. These products include:

1) Cloud Security Asset Exposure (CSAE): Identifies and analyzes cloud assets to determine exposure risks.

2) Cloud Security Posture Anomalies (CSPA): Detects deviations and anomalies in cloud security posture.

3) Cloud Security Posture Management (CSPM): Ensures compliance by continuously monitoring cloud configurations and security policies.

4) Cloud Security Entitlements Management (CIEM) : Manages identity and access entitlements to prevent unauthorized access.

5) Cloud Security Remediation (CSRM) Management : Automates patch distribution for CSPM, CIEM, and CSPA, ensuring vulnerabilities are quickly mitigated.

6) Cloud Security Workload Management (CWPP) : Covers cloud workload security, including Virtual Machines (VM), Configuration Management (CM), Patch Management (PM), Application Enforcement (AE), Workload Management (WM), and Cloud Posture Anomaly Management (CPAM).

Saner CNAPP provides comprehensive dashboards that deliver meaningful insights into each of these security domains. An overarching Cloud Infra Dashboard aggregates critical information from all products, offering a unified view of security posture across cloud assets. Unlike other market solutions, Saner CNAPP eliminates siloed security operations by enabling seamless integration, where findings from one product inform the actions of another.

Key Innovations That Set Us Apart

1. Comprehensive & Actionable Insights Unlike traditional tools that lump together workload vulnerabilities and cloud services misconfigurations, our platform intelligently categorizes and prioritizes each issue, ensuring teams can act swiftly on what truly matters.

2. AI-Powered Summarization & Q&A Security teams no longer have to wade through endless data. Our built-in AI provides instant insights, smart summaries, and answers to security questions, reducing investigation time and improving efficiency.

3. Seamless Integration Across Infrastructure Our CNAPP unifies cloud infrastructure security, bridging gaps across endpoints, cloud services, and workloads. No more working in silos, our platform ensures smooth interoperability across security layers.

4. In-Built, One-Click Remediation Say goodbye to lengthy remediation processes and workflows. With just a few clicks, security teams can implement fixes across multiple sub-products without complex manual intervention.

5. Customizable Reports & Prioritization Every organization has unique risk tolerances. Our CNAPP allows teams to customize severity levels and generate tailored reports, ensuring the right priorities are addressed at the right time.

6. Posture Anomalies Find unique deviations in your cloud infrastructure, normalize the configurations to reduce your attack surface whilst minimizing vulnerabilities due to heterogenous cloud services set up.

7. Deep workload discovery, remote access, and management Identify vulnerabilities and anomalies in operating systems and applications, patch them efficiently and control workloads through Workload Management(WM).

Key Advantages of Saner CNAPP

1. Unified Operations: Eliminates manual mapping of security findings to patches, ensuring faster and more accurate responses.

2. Reduced Scan Times: A common discovery mechanism powers all products, enabling rapid scanning and analysis.

3. Customizable Reports: Users can generate combined or custom reports by leveraging data across different security products, enhancing cloud security visibility and decision-making.

4. Individual Product Uniqueness: Unlike conventional solutions that lump all security functions into a single interface, each Saner CNAPP product retains its distinct identity and functionality for precise security management.

5. Automated and On-Demand Scanning: Security scans are scheduled every 24 hours and can also be initiated on demand.

Onboarding Process

1. Role Stack Creation (Automated): If you are already logged into the AWS, we automatically create the role in your infrastructure with required access to run scans.

2 .Role Stack Creation (Manual) : Manually create the role offline and upload the Role details to the Saner CNAPP portal.

3. AWS Credential Integration : Use AWS credentials such as an access key and secret key to grant access securely. These credentials are encrypted and securely stored to maintain confidentiality.

4. Azure Credential Integration:Use Azure credentials such as a tenant ID, access key and secret key to grant access securely. These credentials are encrypted and securely stored to maintain confidentiality

Once the onboarding process is complete, an initial discovery scan is initiated according to the service provision settings.

Understanding Service Provision

Saner CNAPP offers flexible subscription options, allowing customers to choose security modules based on their needs. The chosen products — CSAE, CSPA, CSPM, CIEM, and CSRM — operate dynamically along with CWPP for workload management, collecting relevant security insights and presenting them through intuitive dashboards.

Cloud Security Asset Exposure (CSAE)

Actors: Cloud Security Engineers, IT Administrators

Introduction

In the ever-expanding cloud landscape, visibility is the foundation of a strong cybersecurity strategy. Organizations must have a clear understanding of what they are securing—every service, resource, and configuration within their cloud environment. Leading cloud providers like AWS and Azure offer a vast array of services, each housing multiple resources critical to business operations. Without proper asset discovery, classification, and monitoring, security risks can go undetected, leading to potential breaches or compliance failures.

Cloud Security Asset Exposure (CSAE) bridges this gap by providing a comprehensive view of your cloud infrastructure. By enabling organizations to identify, categorize, and track cloud assets across regions and services, CSAE ensures that security teams can proactively manage risks, optimize resources, and maintain compliance. From visualizing service heatmaps to detecting publicly exposed resources, CSAE empowers businesses with the insights needed to safeguard their cloud environments effectively.

Visualize Heat Map of Services Used & Drill Down into Resources

CSAE provides an interactive heat map that gives an instant overview of the cloud services in use. The intensity of colors in the map highlight the most frequently used services, enabling security teams to focus on high-impact areas. Users can drill down into each service to explore the specific resources it contains, ensuring granular visibility of cloud assets.

Distribution of Resources by Usage & Deep Dive into Resource Types

CSAE categorizes cloud resources based on their type and visualizes their distribution. This helps customers identify which resource types (e.g., virtual machines, storage buckets, IAM policies) are most utilized. Users can explore each resource type further to uncover configurations, usage patterns, and security risks.

Geo Distribution & Resource Analysis by Region

Cloud infrastructure is often spread across multiple geographic regions. CSAE offers a global view of asset distribution across AWS, Azure, and other cloud providers. Users can filter resources by region, ensuring compliance with data residency laws and optimizing performance based on location.

Categorization of Resources & Drill Down by Service Type

CSAE GROUPS RESOURCES INTO LOGICAL CATEGORIES SUCH AS:

1. AI/ML Services (e.g., AWS SageMaker, Azure Machine Learning) high-impact areas. Users can drill down into each service to explore the specific resources it contains, ensuring granular visibility of cloud assets.
2. Compute Infrastructure & Virtual Machines (e.g., EC2 instances, Azure VMs)
3. Network Configuration (e.g., VPCs, security groups, firewalls)
4. Users can explore resources within each category to detect misconfigurations and optimize security policies.

Identify & Secure Publicly Accessible Resources with Evidence

CSAE identifies all publicly accessible cloud resources, such as exposed databases, storage buckets, or compute instances. It provides clear evidence explaining why a resource is public (e.g., misconfigured IAM policies, open security groups) .

Service Usage Trends & Insights

CSAE tracks how cloud services are being used over time, allowing users to visualize trends in service adoption, utilization, and performance. This helps teams optimize their cloud strategies and reduce unused or underutilized services.

Resource Usage Trends & Historical Insights

Beyond services, CSAE also analyzes individual resources to identify usage trends. This feature is especially useful for capacity planning and cost optimization, ensuring that underutilized resources are scaled down.

Cost Visualization Based on Services & Resources

A dedicated cost analysis dashboard provides insights into cloud expenditure by breaking down costs at both the service and resource levels. This enables organizations to pinpoint high-cost areas and make informed budgeting decisions.

Cost Trends for the Last 6 Months

CSAE tracks cloud expenses over six months, offering detailed cost trends and anomaly detection. If sudden cost spikes occur, security teams can investigate the cause, such as an increase in compute resources, excessive data transfers, or misconfigured auto-scaling.

Detect Deprecated & Outdated Services in Use

Cloud providers frequently deprecate older services. CSAE automatically flags deprecated services that may pose security or functionality risks, allowing teams to migrate to newer alternatives before support is discontinued.

Create a Custom Watchlist for Critical Resources

Users can define their own watchlists to monitor critical cloud assets. This feature ensures that high-priority resources are easily accessible, with alerts and filters providing instant visibility into security risks affecting these resources.

Resource Deep-Dive & JSON Data Export

CSAE provides a detailed view of each resource, including configurations, permissions, usage, and security posture. Users can export this data in JSON format for easy integration with external security tools, SIEMs, or compliance reports.

Download CSV Reports for Dashboard Grids

For further analysis and reporting, CSAE allows users to export grid data from dashboards in CSV format. This is useful for offline review, financial forecasting, and internal audits.

Generative AI-Powered Insights for Data Interpretation

If complex graphs and tables seem overwhelming, CSAE features a built-in Generative AI Analyzer. This tool interprets visualizations and tabular data, providing human-readable summaries. Users can copy AI-generated insights into reports, presentations, or team discussions, making data-driven decisions more accessible.

Cloud Security Posture Anomalies (CSPA)

Actors: Cloud Security Engineers, Cloud Administrators

Introduction

In the world of cloud security, it is easy to visualize individual resources and their configurations. However, a deeper analysis often reveals certain resources that deviate from the expected behavior when compared to their peer group. These outliers, if left unaddressed, can introduce vulnerabilities due to misconfigurations or unnecessary permissions. Identifying and mitigating these anomalies is crucial to reducing the attack surface and strengthening cloud security.

Cloud Security Posture Anomalies (CSPA) helps in detecting such outliers by providing insightful analytics and actionable remediation paths. With advanced visualization techniques and data science-driven insights, organizations can swiftly detect and rectify security gaps.

Visualize Heat of Anomalies Based on Severity

Understanding the severity of anomalies is essential for prioritizing remediation efforts. CSPA provides a heatmap visualization that categorizes anomalies into high, medium, and low severity levels. This helps security teams focus on the most critical issues first, ensuring that high-risk misconfigurations are addressed promptly.

Bubble Distribution of Anomalies Based on Category

CSPA employs a bubble chart visualization to showcase the distribution of anomalies across different security categories. This helps in quickly identifying which areas of security are most affected and require immediate attention. The size and density of bubbles give an intuitive understanding of the volume of anomalies in each category.

Visualize Attack Categories Based on Anomaly Count

CSPA maps anomalies to specific attack categories, allowing organizations to understand which types of attacks they are more vulnerable to. By analyzing the number of anomalies per attack category, security teams can proactively strengthen their defences against potential threats.

In-depth Analysis Using Data Science Algorithms

Each anomaly detected undergoes thorough analysis using advanced data science techniques. The system intelligently filters meaningful insights and presents them in an actionable format. Users can drill down into the details of each anomaly, examining its impact and root cause, thereby enabling well-informed security decisions.

Identify Publicly Accessible Resources and Secure Them

Publicly accessible resources pose a significant risk if they are not meant to be exposed. CSPA provides clear evidence of why a resource is publicly accessible, enabling organizations to swiftly secure such resources. By addressing publicly accessible misconfigurations first, organizations can mitigate risks associated with unauthorized access.

Visualize Anomaly Trends Over Days

Security teams can track anomaly trends over time using CSPA's timeline-based visualization. This feature helps in monitoring how anomalies fluctuate across different time periods, providing insights into emerging security issues and the effectiveness of remediation efforts.

Geo Distribution of Anomalies

CSPA offers geo-based visualization of anomalies, displaying how security issues are distributed across various geographical locations. This helps organizations understand regional security patterns and take necessary steps to mitigate location-specific risks.

Create a Whitelist for Expected Anomalies

Not all anomalies require remediation. If a finding is expected or deemed acceptable, users can whitelist it within the detailed findings page. Whitelisted anomalies are excluded from patching recommendations, allowing organizations to focus only on actionable security gaps.

One-Click Remediation for Anomalies

CSPA simplifies the remediation process with a one-click remediation feature. Users can choose to remediate anomalies based on individual resources or apply fixes to all identified security gaps collectively. This reduces the manual effort required to secure cloud resources.

Whitelist Entire CSPA ID(s)

For cases where an entire category of anomalies is not applicable to an organization's security posture, users can whitelist specific CSPA ID(s). Once whitelisted, these anomalies vanish from remediation suggestions, streamlining the security management process.

Detailed Anomaly Insights

Each anomaly in CSPA is accompanied by a comprehensive summary that includes:

1. Historical trend data over days
2. Geo-distribution of affected resources
3. Findings table listing affected and unaffected resources
4. Categorization of resources into anomalous and non-anomalous groups

This in-depth analysis helps security teams make informed decisions regarding anomaly resolution

Grid View for All Anomalies

Users can access a complete grid listing of all detected anomalies. This view clearly distinguishes between problems requiring attention and normalized configurations, enabling better anomaly management.

Download CSV Reports for Further Analysis

For further processing and record-keeping, CSPA allows users to download CSV reports from each grid on the dashboard. This feature is particularly useful for audit purposes, compliance reporting, and deeper offline analysis.

Generative AI-Based Analysis for Graphs and Data

If you find data or graphs mind-boggling, each grid is equipped with a Generative AI analyzer that provides meaningful insights into your visual graphs or tabular data. Users can copy this AI-generated analysis and include it in reports or conversations, simplifying complex data interpretation.

Cloud Security Posture Management (CSPM)

Actors: Compliance Officers, Risk Managers

Introduction

Cloud Security Posture Management (CSPM) is a widely recognized and essential tool designed to detect misconfigurations across various regions of cloud infrastructure by benchmarking them against established standards. SecPod's Security Intelligence team has developed the SecPod Default Benchmark, an exceptional combination of best practices derived from prominent compliance frameworks like NIST, CIS, PCI, HIPAA, and SOC2. By adhering to the SecPod Default Benchmark, organizations can ensure that their cloud configurations are set to a high standard, with automatic benchmarking against globally recognized compliance frameworks. This approach not only guarantees security but also simplifies the process of meeting stringent regulatory requirements.

Region-Specific Benchmarking

Different regions have their own compliance standards, and CSPM allows for creating tailored benchmarks for each of them. This ensures that configurations meet the specific compliance requirements of each geographic area and reduces the risk of non-compliance.

Downloadable CSV Reports

Users can download CSV reports from each grid on the dashboard, allowing for easy extraction and use of data for personal purposes, further analysis, or inclusion in detailed reports.

Customizable Severity and Values

While creating benchmarks and remediating configurations, users can adjust the severity levels and values as needed. This flexibility ensures that patching efforts are aligned with the most critical issues, and that remediation takes into account varying requirements across different environments.

Quick Evaluation for Regular Audits

CSPM offers fast and efficient evaluations of benchmarks, allowing organizations to quickly identify and resolve configuration issues during routine audits. This feature helps save time and ensures continuous compliance with security standards.

Benchmark Application Across Multiple Accounts

If you've created a comprehensive list of benchmarks for a particular environment, you can effortlessly apply them to other accounts in the final step of the creation process. This enables consistent security posture management across all cloud accounts with minimal effort.

Primary Benchmarks for Automated Configuration Fixes

SecPod CSPM prioritizes the most important benchmarks for fixing configuration issues, either automatically or with minimal manual intervention. This approach helps to maintain a consistent, secure cloud environment with minimal effort from security teams.

Top 5 Affected Regions and Attack Surface Analysis

CSPM provides insights into the regions with the most vulnerabilities. By highlighting the top five affected regions, users can dig deeper to explore the specific resources that are most vulnerable and need immediate attention.

Severity-Based Findings Across Regions

The tool categorizes findings based on severity levels—high, medium, and low—across different regions. This allows for a more targeted remediation approach, focusing on the most critical issues first, while ensuring that all security gaps are addressed.

Instant Access to Publicly Accessible Resources

Identifying publicly accessible resources is crucial for cloud security. CSPM allows for instant identification of such resources and provides detailed insights into compliance issues, helping users secure their cloud environments more effectively.

Geo-Distribution of Non-Compliance

Visualizing non-compliance geographically allows organizations to quickly identify regions where compliance gaps are more prevalent. This feature aids in targeted remediation efforts based on location-specific risks.

Bar Graph for Findings by Service

A visual bar graph provides a clear breakdown of findings based on services, allowing users to filter and focus on issues specific to particular services. This helps streamline the process of identifying and remediating vulnerabilities.

Compliance Statistics for Primary Benchmarks

CSPM offers a comprehensive overview of primary benchmarks, showing their severity distribution and compliance status. You can track whether resources have passed, failed, or remain unchecked due to disabled checks or unavailable data, providing a clear understanding of your compliance posture.

Clear Categorization of Results

Each detailed analysis of resources is categorized into Pass, Fail, Unchecked, and Not Evaluated, providing a clear distinction between different compliance statuses. This helps prioritize remediation efforts without ambiguity.

Date-Wise Affected Resources Trend Analysis

The Date-Wise Affected Resources Line Trend graph tracks the status of affected resources over time, helping organizations monitor their progress and avoid sudden spikes in non-compliance in the future.

Generative AI Insights for Data and Graphs

If the data or graphs on your dashboard seem overwhelming, the built-in Generative AI analyzer provides meaningful insights, summarizing key takeaways from complex visual data. This feature helps translate raw data into actionable insights that can be incorporated into reports or shared in conversations.

Cloud Infrastructure Entitlement Management (CIEM)

Actors: Cloud Administrators, Security Analysts

Introduction

Cloud Infrastructure Entitlement Management (CIEM) is a critical security process that ensures organizations have proper control over access to their cloud resources. It helps mitigate risks stemming from excessive permissions, misconfigurations, and unmonitored identities. As organizations move more workloads to the cloud, managing entitlements becomes essential for preventing unauthorized access and minimizing security vulnerabilities.

CIEM solutions continuously monitor, analyze, and remediate permissions-related risks by enforcing the principle of least privilege, ensuring that users, applications, and services have only the access they need. With automated detection, policy recommendations, and real-time insights, CIEM plays a crucial role in securing cloud environments.

What Does CIEM Do?

1. Enforce Least Privilege

CIEM ensures that each user, application, and service has the minimum required access to perform their designated tasks. It continuously audits cloud permissions and revokes excessive or unused access rights to reduce the risk of unauthorized actions.

2. Detect Misconfigurations

One of the leading causes of security breaches is misconfigured permissions. CIEM helps identify and correct improper access configurations, reducing the risk of privilege escalation and data exposure.

3. Audit Access

CIEM provides visibility into access controls by monitoring who has access to cloud resources, tracking changes, and generating detailed audit logs. This helps organizations meet compliance requirements and respond to security incidents effectively.

4. Remediate Risks

By identifying overly permissive roles, unused accounts, and insecure policies, CIEM helps organizations proactively reduce their cloud attack surface. It provides automated remediation actions, such as revoking unnecessary permissions or enforcing security best practices.

5. Provide Visibility

CIEM offers a centralized dashboard that visualizes access rights, policies, and security insights. It enables security teams to analyze permissions across multiple cloud providers and take informed actions to enhance security posture.view of security posture across cloud assets. Unlike other market solutions, Saner CNAPP eliminates siloed security operations by enabling seamless integration, where findings from one product inform the actions of another.

How Does CIEM Work?

1. Automatically Detects Overly Permissive Policies: Identifies users and roles with excessive privileges and flags potential security risks.
2. Uses Pre-Built Policies to Detect Risky Permissions: Leverages predefined security policies to assess access controls.
3. Provides Automated Recommendations: Suggests the necessary actions to enforce the least privilege principle.
4. Centralizes Data Points into Actionable Insights: Aggregates access-related data and presents meaningful security insights.
5. Streamlines Access Management: Simplifies user and role access reviews, reducing operational overhead.

Why Is CIEM Important?

CIEM plays a crucial role in securing cloud environments by preventing unauthorized access, enforcing compliance, and reducing security risks. Cloud identities with excessive permissions pose a major security threat, as they can be exploited by attackers to gain unauthorized access to sensitive data. By implementing CIEM, organizations can proactively secure their cloud infrastructure and minimize the risk of data breaches.

Identify Users with Access to Cloud Infrastructure

CIEM provides a detailed analysis of users who currently have access to cloud resources. It categorizes users into groups such as overly permissive, inactive, or both. This helps organizations determine which identities pose a security risk and take corrective action.

Deep Analysis of User Permissions

CIEM digs deeper into user permissions, offering insights into which policies make them overly permissive or why they are marked as inactive. A graphical representation helps security teams visualize access-related risks and make informed decisions.

Group Access Management

Users in cloud environments often belong to groups. CIEM identifies the total group count and highlights groups that are empty but still have policies attached. This ensures that unnecessary groups do not retain access privileges.

Deep Analysis of Groups

Similar to users, CIEM provides an in-depth view of group permissions. A graph-based approach helps security teams identify overly permissive groups or empty groups that may still have policies assigned.

Comprehensive Policy Inventory

CIEM generates a count of all policies in AWS, including inline, managed, and custom-managed policies. These policies are further classified into 15 overly permissive categories, helping organizations prioritize remediation efforts.

Overly Permissive AWS Policies Analysis

CIEM allows users to explore the 15 overly permissive categories of AWS policies with a graphical representation. It provides essential details on why specific services and actions make these policies insecure and displays the applicable versions currently used in the cloud infrastructure.

Role-Based Access Control (RBAC) Analysis

Roles define entitlements for users and groups. CIEM helps organizations visualize the total number of roles in AWS, including overly permissive roles, as well as RBAC and Entra roles in Azure.

Overly Permissive Azure Roles Analysis

CIEM provides a deep analysis of the five overly permissive categories of Azure roles, offering graphical insights into why these roles pose security risks. It includes key details on roles currently used in the cloud environment.

Application Management in Azure

CIEM identifies all applications in Azure and flags unused applications. It further analyzes security attributes and provides a visual representation of why these applications are considered unused or pose a security risk.

CIEM Trend Graph for Security Insights

A trend graph helps security teams track changes in cloud access over time. A trend number appears on top of the count, indicating an increase or decrease since a specific date. This feature reduces the effort needed to interpret graphs and provides quick insights into security trends.

Critical Event Analysis

CIEM continuously monitors and analyzes critical cloud events such as failed login attempts and access-related incidents. This analysis is conducted every 24 hours, with future updates aiming for real-time or more frequent monitoring.

Recommended Remediation Actions

A dedicated remediation section provides a tabular listing of affected identities and offers one-click patching to fix security vulnerabilities efficiently

Exportable Security Reports

Users can download CSV files from each dashboard grid for further analysis, reporting, or internal documentation.

Gen AI-Powered Insights

Understanding complex data can be overwhelming. CIEM incorporates a Gen AI-powered analyzer that interprets visual graphs and tabular data, providing meaningful insights. Users can copy this analysis and integrate it into security reports or discussions.

Cloud Security Remediation (Patch) Management (CSRM)

Actors: Security Operations Center (SOC) Teams, DevOps, Response Teams, IT administrators

Introduction

Cloud Security Remediation (Patch) Management (CSRM) plays a pivotal role in cloud security by addressing vulnerabilities, anomalies, entitlements issues, and compliance gaps efficiently. Once vulnerabilities are identified and analyzed, the next crucial step is patching. This process ensures that security risks are mitigated promptly to maintain a robust security posture.

CSRM OFFERS TWO APPROACHES TO PATCHING

1. Patch Task Creation (Job-based Patching) – This involves creating patch tasks upon detecting issues, allowing users to schedule remediation immediately or at a later date and time.
2. Automated Patching – This method fixes issues recurrently whenever specific findings appear, streamlining security operations without requiring manual intervention.Network Configuration (e.g., VPCs, security groups, firewalls)

REMEDIATION IS CATEGORIZED INTO THREE PRIMARY SECURITY DOMAINS:

1. Cloud Security Posture Management (CSPM)
2. Cloud Infrastructure Entitlement Management (CIEM)
3. Cloud Security Protection & Automation (CSPA)

EACH PATCH FALLS UNDER EITHER PREDEFINED OR CUSTOM CATEGORIES:

1. Predefined Patches – Fully automated flows that do not require user input.
2. Custom Patches – Require user input such as specifying allowed IPs/ports in security groups, encryption keys, etc. Although CSRM aims to automate most patches, some user configurations remain necessary for precise security tuning.

With minimal user intervention, CSRM ensures that patching is efficient, effective, and tailored to cloud security needs.

Visualize Product-wise Patch Count Distribution

CSRM provides an intuitive visualization of the number of patches applied across different products, helping organizations assess their security posture at a glance.

Top CSPM Patch Count by Cloud Service (Bar Graph)

A bar graph representation of the CSPM patches categorized by cloud service (e.g., AWS, Azure, GCP) offers insights into which cloud services require the most attention.

Patch Count Based on Geolocation for CSPM, CIEM, and CSPA

Displays patch distribution across different geographic regions, enabling security teams to identify high-risk zones and prioritize remediation based on location-specific threats

Tabular Listing of Remediation Tasks and Status

Provides a structured table displaying all initiated remediation tasks, their status (pending, completed, failed), and additional metadata for tracking security efforts.

Patch Aging Analysis (Line Plot)

A time-based line plot shows the correlation between the number of pending patches and their age in days, helping teams address older, high-risk vulnerabilities first.

Patching Impact Visualization

Plots the number of security rules fixed against the number of patches applied, offering a clear understanding of the effectiveness of remediation efforts.

Patch Job Orchestration Workflow

Users can initiate remediation patches in a few steps: Select the affected resources. Review patches or modify selections (skip patches if unsure). Enter scheduling details, assign a unique job name, and configure other options. Review the summary and finalize job creation.

Approval-Based Execution

At the final step of patching tasks creation, users with approval permissions can either approve the execution immediately or create a task for approval. Only approved tasks proceed to execution.

Task Status and Approval Dashboard

A dedicated dashboard allows users to monitor patch execution status, approve pending tasks, and ensure timely security enforcement.

Automated Patching on Schedule

Users can set up automated patching tasks that trigger recurrently based on predefined schedules. Once a security scan identifies issues, patches are automatically generated and applied without manual intervention.

Cloud Security Workload Management(CWPP)

Actors: Security Teams, IT administrators

Similar to Saner CVEM, CWPP (Cloud Workload Protection Platform) provides comprehensive security for cloud workloads by integrating key capabilities such as Vulnerability Management (VM), Configuration Management (CM), Patch Management (PM), Posture Anomalies (CPAM), and Workload Management (WM). This unified approach ensures that cloud environments remain secure by continuously identifying and mitigating vulnerabilities, enforcing compliance through robust configuration controls, deploying timely patches, restricting unauthorized access, and proactively managing potential security exposures. By consolidating these critical security functions, CWPP strengthens cloud workload protection, reducing attack surfaces and enhancing overall cybersecurity resilience.

Cloud Infrastructure Dashboard

Actors: C-Suite personnel such as CISO, CEO

Introduction

A comprehensive Cloud Infrastructure Dashboard provides organizations with an overarching view of their cloud assets, security posture, and compliance status across multiple cloud providers. This unified dashboard aggregates meaningful insights from various products, offering a standardized language to analyze and monitor cloud infrastructure irrespective of whether it is hosted on AWS, Azure, or other providers. It also enables organizations to drill down into provider-specific views, offering deeper insights into Azure and AWS environments. By presenting consolidated and segregated data, the dashboard facilitates efficient cloud resource management, cost optimization, and security posture enhancement. Below are the key components and insights that the Cloud Infra Dashboard delivers:

TOTAL RESOURCES OVERVIEW

1. Displays the total count of resources across all cloud providers.
2. Compares the current month's total resource count with the previous month
3. Helps in tracking resource growth or reduction trends.

PUBLICLY ACCESSIBLE RESOURCES

1. Lists resources that are publicly accessible.
2. Provides an average count of publicly accessible resources over the past month. Helps in tracking resource growth or reduction trends.
3. Enables comparison to determine if the current number is above or below the monthly average.

CLOUD INFRASTRUCTURE COST ANALYSIS

1. Presents the total cost incurred due to cloud resource usage
2. Breaks down cost distribution across multiple cloud providers.
3. Helps in budgeting and identifying cost optimization opportunities.

HIGH SEVERITY RISKS MONITORING

1. Identifies total high-severity risks detected from all cloud security findings.Breaks down cost distribution across multiple cloud providers.
2. Displays trends over the past month, indicating an increase or decrease in high-severity risks.
3. Helps in assessing and prioritizing security threats.

RESOURCE CATEGORIZATION

1. Consolidates resources into categorized groups based on cloud infrastructure types.
2. Helps organizations understand resource distribution and utilization.

GEO-LOCATION BASED RESOURCE DISTRIBUTION

1. Provides insights into the geographical distribution of cloud resources.
2. Assists in understanding region-based resource allocation and potential cost implications.

COMPLIANCE BENCHMARKING

1. Lists resources that are publicly accessible.
2. Provides an average count of publicly accessible resources over the past month. Helps in tracking resource growth or reduction trends.
3. Enables comparison to determine if the current number is above or below the monthly average.

CLOUD ENTITLEMENT ISSUES

1. Highlights issues in user access control, roles, groups, policies, and application permissions.
2. Provides concise issue descriptions for different cloud providers.
3. Helps organizations manage cloud entitlements effectively.

ANOMALY DETECTION & TREND ANALYSIS

1. Highlights issues in user access control, roles, groups, policies, and application permissions.
2. Provides concise issue descriptions for different cloud providers.
3. Helps organizations manage cloud entitlements effectively.

PATCH MANAGEMENT INSIGHTS

1. Visualizes patch distribution across CIEM (Cloud Infrastructure Entitlement Management), CSPM (Cloud Security Posture Management), and CSPA (Cloud Security Protection and Automation).
2. Categorizes patches based on cloud providers to streamline security patching.

RECOMMENDED PATCHES OVERVIEW

1. Provides a tabular summary of recommended patches for all cloud-related security issues.
2. Assists security teams in prioritizing and applying necessary patches to maintain cloud security integrity.

Conclusion

The Cloud Infra Dashboard serves as a centralized platform for organizations to monitor and manage their cloud infrastructure effectively. By providing real-time insights into resource utilization, cost, security risks, compliance status, and anomaly detection, the dashboard enables informed decision-making. Organizations can leverage this dashboard to enhance cloud security, optimize resource allocation, and ensure compliance with industry standards.

With this launch, we are redefining cloud security - moving from fragmented, reactive approaches to a unified, proactive, and intelligent security posture. Our commitment is to empower security teams with the tools they need to navigate today's complex cloud environments confidently.

We can't wait for you to experience the future of cloud security.

Welcome to the new era of prevention, where clarity meets action.

secpod

CONTACT US

info@secpod.com/www.secpod.com