secpod

CNAPP BUYER'S GUIDE:

Prevention-First Strategies for Securing the Cloud

www.secpod.com

Introduction

As cloud adoption continues to accelerate globally, security teams face an unprecedented flood of threats. In 2024 alone, cloud security incidents jumped by roughly 154% year-over-year,[1] yet only about four percent of organizations are able to quickly remediate those risks. These trends make it clear that a reactive, tool-by-tool approach no longer suffices.

Instead, leading security professionals advocate a prevention-first posture. We can achieve so by designing security into cloud infrastructure from the get-go, and stopping attacks before they can occur.

This buyer's guide explains what a Cloud-Native Application Protection Platform (CNAPP) must offer to make that approach real, based on the latest research and technological developments beyond 2024. It covers the CNAPP concept, its ideal capabilities, evaluation criteria, and practical strategies for deployment and usage, all of which are embossed with an emphasis on preventing breaches.

[1] World Economic Forum

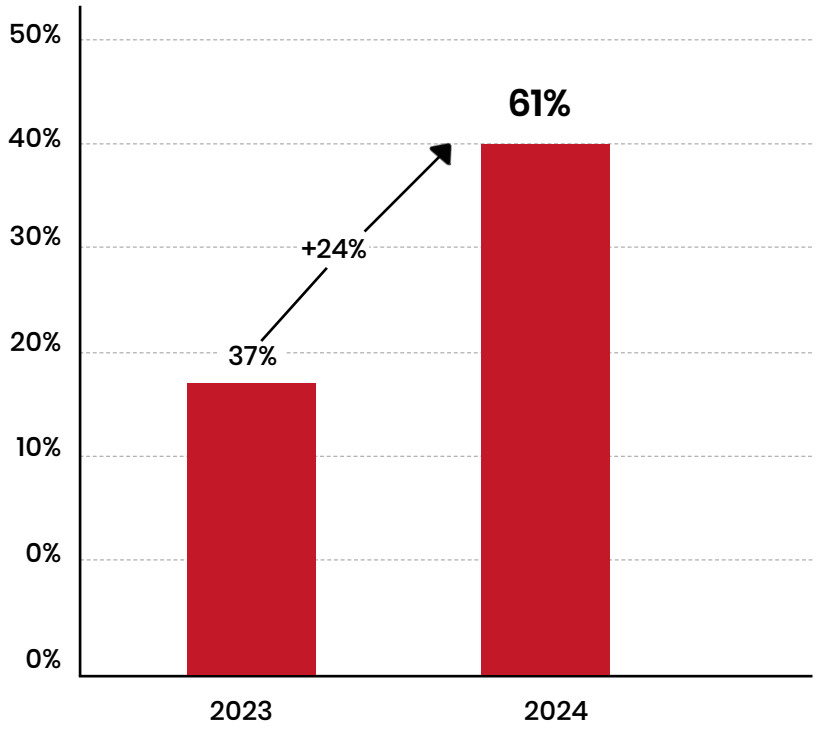
The Cloud Security Surge in 2024

Cloud environments have always been complex, and now they're all the more intricated. As such, attacks have scaled accordingly. In 2024, roughly 61% of organizations reported a significant cloud security incident, which is an increase of 24% when compared to 2023.[2] This surge is driven by factors like misconfigurations, rapid deployments, and exposed mismanaged services. Notably, research finds that misconfigured assets were the top cause of security rule failures in pure cloud environments.[3] In other words, simple mistakes in cloud settings, like open storage buckets or overly permissive policies, grant attackers windows of opportunity.

Meanwhile, organizations struggle to keep pace. For example, it takes an average of two days just to patch even critical vulnerabilities in the cloud. During that window, threat actors can strike, especially with zero-day exploits up by 56% in 2023. In practice, security often lags behind. A 2024 survey warned that nearly half of developers push code with known flaws, and 97% of companies experienced an incident related to their own cloud-native applications in the last year.[4]

These observations point to a harsh truth: traditional security tools — which mostly detect issues and send alerts — leave a dangerous gap. By the time an alert fires, an attacker may already be compromising resources. To close that gap, many experts now argue that organizations must flip the script. Rather than responding to every alert, teams should build security by design and stop threats upfront. This means integrating prevention controls into every layer of the cloud stack, from code pipelines through runtime.

[2] Intelligent CIO
[3] IBM
[4] Cisco



Let's take a look at some important statistics:

154% OF INCIDENTS — **Cloud security incidents rose by 154% in 2024 from the past two years.**

4% OF TEAMS — **Only about 4% of teams can quickly remediate cloud risks.**

97% OF ORGS — **97% of orgs saw a cloud app security incident last year.**

100% OF FAILURES — **Misconfigurations caused most security failures in 100% cloud setups.**

These trends stress upon the need for a unified, prevention-focused platform that can continuously secure cloud applications. That platform is known as a CNAPP.

Understanding CNAPP: A Unified Cloud Security Platform

A Cloud-Native Application Protection Platform (CNAPP) is designed to address security across the full lifecycle of cloud-native applications. It brings together multiple, previously disparate tools under one roof. For example, cloud security posture management (CSPM), cloud workload protection (CWP), cloud infrastructure entitlement management (CIEM), and attack surface monitoring. In practice, CNAPP tools scan code repositories and infrastructure-as-code (IaC) files, monitor running workloads, analyze permissions, misconfigurations, and correlate all this context into prioritized findings.

Cisco succinctly describes CNAPPs as addressing the full life cycle protection requirements of cloud-native applications from development to production. In one place, it unifies everything from checking Kubernetes configurations and scanning container images, to finding vulnerable VMs and risky IAM roles. The core benefit is visibility and consistency. Rather than having separate point tools for CSPM, CWPP, and so on, a CNAPP provides a single pane view of risk. This lets teams see which vulnerabilities or misconfigurations are most pressing, and fix them early in development or before they affect production.

For example, CNAPPs combine several cybersecurity capabilities — CSPM, CIEM, and CWP, among others — into one platform.[5] Such a platform is designed to protect organizations through every operation, from concept development to runtime. In concrete terms, a CNAPP can automatically check infrastructure code and cloud settings before resources go live, block dangerous activities at runtime, and enforce consistent policies across multiple clouds. By integrating these capabilities, CNAPPs help developers and security teams work together, instead of each using their own siloed tools.

CNAPP solutions are maturing quickly. In 2023, about 40% of organizations reported using a CNAPP, and another 45% expected to adopt one by the mid-year mark of 2025. This rise reflects a broader shift: 87% of all companies are now in multicloud environments, so security must span AWS, Azure, and GCP to name a few cloud service vendors. Moreover, with 82% of breaches involving cloud data, a unified cloud-centric approach is becoming the need of the hour. The average cost of a data breach is also soaring, where companies have been reported to shell out around $4.45 million per incident, so inefficiencies and fragmentation in tooling are untenable.

[5] Microsoft

What a CNAPP Brings to the Table

CSPM

Automated scanning of cloud configurations and compliance benchmarks (e.g. NIST, PCI).

CIEM

Visibility into IAM users, roles, permissions and applying least-privilege checks.

WORKLOAD PROTECTION

Scanning container images, server workloads, and runtime behaviors for vulnerabilities or malware.

ATTACK SURFACE MONITORING

Discovering exposed assets, credentials, and external attacks.

VULNERABILITY & PATCH MANAGEMENT

Identifying and prioritizing software flaws and missing patches in cloud assets.

COMPLIANCE MANAGEMENT

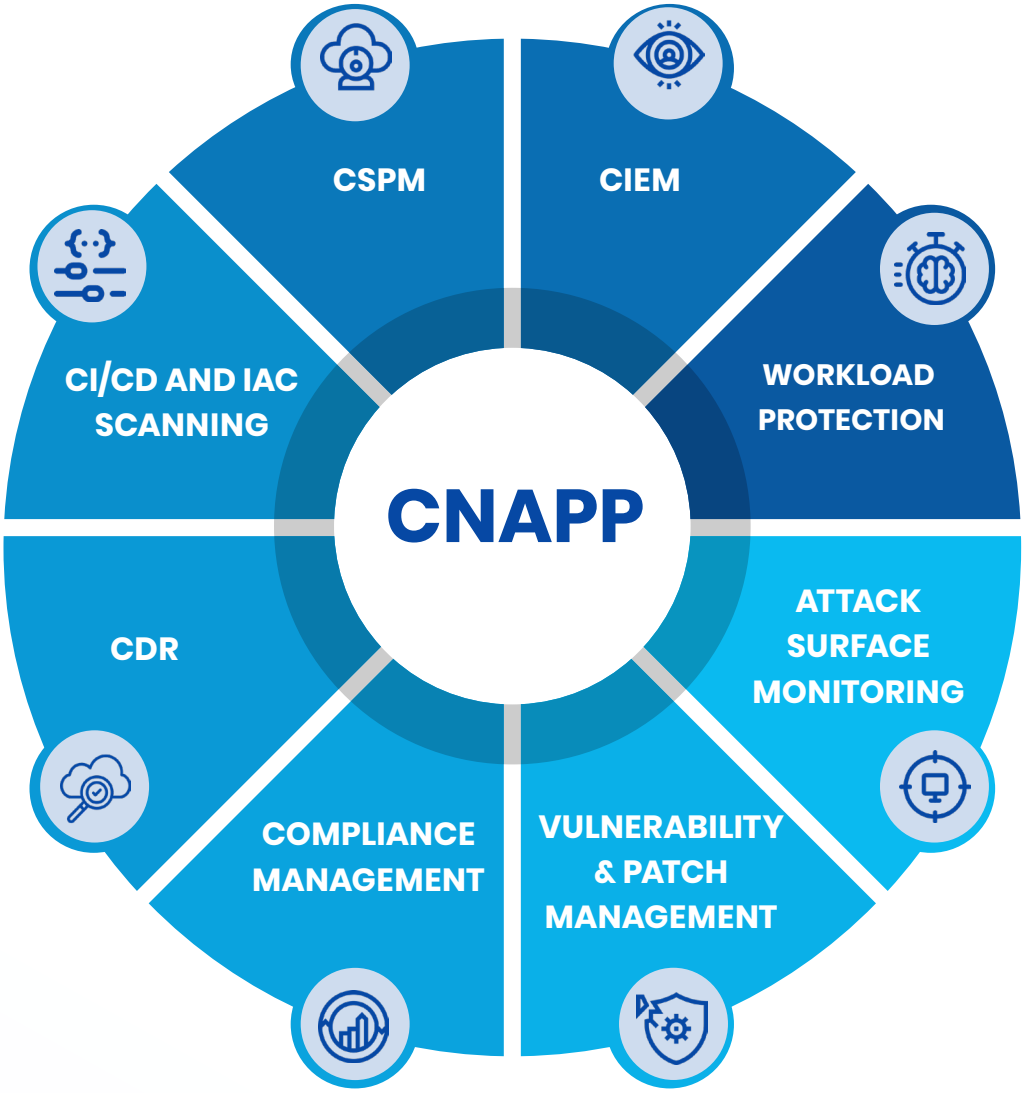
Continuous reporting against standards like CIS, HIPAA, PCI-DSS (often using custom or built-in benchmarks).

CDR

Cloud Detection and Response to detect and respond to threats in real-time.

CI/CD AND IAC SCANNING

To scan code pipelines and IaC templates for security risks.



In short, a CNAPP provides automated security, complete and unified visibility, powerful compliance monitoring, and centralized management for cloud environments. By catching issues early — when code is committed, for instance — and maintaining continuous oversight, it sets the stage for prevention. But not all CNAPPs are equal and, by themselves, even CNAPPs may default to a "reactive" mode. The important step here is to use a CNAPP in a prevention-first way, which we'll explain next.

Why Alert-Only Tools Fail: Moving from Reaction to Prevention

Many traditional security approaches are designed around alerts and fixes, not stopping attacks in real-time. This "reaction-first" mindset doesn't scale in the cloud. The World Economic Forum cautions that CNAPPs in isolation focus on alerting and remediation rather than stopping breaches. In practice, CNAPPs will flag a dozen high-severity issues, but if the team takes days to apply fixes, attackers can still strike.

Consider how a typical CNAPP operates: It will scan cloud infrastructure and code, generate reports of vulnerabilities or misconfigurations, then suggest remediation steps. While that is valuable, it still leaves a window of exposure. As one expert puts it, CNAPPs "focus on alerting and managing risks, not preventing attacks from happening". In other words, they tell you what's wrong but not help you fix issues before any damage occurs.

The gap is clear when you look at timelines. Even after a critical vulnerability is identified, many teams take days or weeks to address it. The Cloud Security Alliance reports the average organization takes 48 hours just to patch a critical cloud vulnerability. Meanwhile, Google's Threat Analysis Group saw 75 zero-day exploits in 2024. In such an environment, a reactive platform will always be a step behind.

By contrast, a prevention-first approach aims to deny attackers the chance to exploit any vulnerability in the first place. This means embedding controls at design time and runtime so that even new or unknown attacks are blocked.

SOME EXAMPLES INCLUDE

SHIFT-LEFT SECURITY

Integrate security checks, like IaC scanning and static analysis, into the development pipeline. Build security rules into code, so dangerous changes fail automatically.

VULNERABILITY AND MISCONFIGURATION

Identifying vulnerabilities and mitigating them continuously across cloud infrastructure and workload.

RUNTIME DEFENSES

Employ runtime protection, such as host intrusion prevention and cloud web application firewalls (WAF), that intercept exploit attempts in real-time.

ZERO TRUST

Enforce least privilege everywhere by using a CNAPP's CIEM to remove excessive permissions before they're abused.

AI/ML ANALYSIS

Use anomaly detection and AI-driven policies to predict and prevent posture anomalies and the unknowns before they escalate.

CONTINUOUS REMEDIATION

Automate fixes and policy enforcement; the platform should auto-remediate known issues where safe, without waiting for manual intervention.

In practice, a prevention-first posture requires pairing CNAPP insights with proactive controls. For example, adopting a zero-trust network model where you segment services, and enforcing identity checks, complements the CNAPP's visibility with hard blocks on lateral movement.

The takeaway here is that a CNAPP can generate fewer alerts to reduce noise, but preventing breaches still requires active controls. Outfitting the cloud with real-time blocking — via AI-powered WAFs, microsegmentation, and policy engines among other practices — shifts an organization's posture from reactive to preventive.

Components You Should Find in a Prevention-First CNAPP

A modern CNAPP for prevention should include several core modules:

CLOUD SECURITY POSTURE MANAGEMENT (CSPM)

Continuously scans cloud configurations — storage, network, and IAM policies, for instance — against industry benchmarks and internal policies. It automatically detects misconfigurations and compliance gaps. In a prevention mode, the CSPM should not only report problems but also automatically enforce safe configurations where possible. Locking down a public S3 bucket or disabling an unused service is a great example. A prevention-oriented CSPM will also trend scan results over time to catch recurring patterns.

CLOUD INFRASTRUCTURE ENTITLEMENT MANAGEMENT (CIEM)

Maps cloud identities and permissions like users, roles, and service principals. It detects excessive privileges and unused roles that attackers might exploit. The platform should enable automated least-privilege remediation, such as prompt revoking overly broad roles, and enforce just-in-time access where possible. For example, evaluate “excessive permissions” categories for AWS and Azure policies, flagging high-risk actions like ‘Delete S3 Bucket’ or wildcards. This prevents privilege abuse before it starts.

WORKLOAD PROTECTION (CWPP)

Scans container images, server workloads, and deployed apps for known vulnerabilities and secrets. A prevention-first CNAPP might integrate with CI/CD pipelines to block deployment of images with critical flaws or leaked credentials. It also monitors runtime processes for anomalous activity. Crucially, it should tie findings back to the CSPM/CICD environment. For instance, if a container vulnerability appears, quickly cross-check if it has network exposure, and quarantine that workload automatically if needed.

EXTERNAL ATTACK SURFACE EXPOSURE (EASM)

Discovers all assets exposed to the internet like public storage buckets, orphaned snapshots, or unused load balancers. The CNAPP should actively flag these resources and automatically reclassify them under actions to revoke public access or quarantine the asset. For example, giving administrators full visibility and control over asset exposure, flagging public resources in real-time, categorizing resources under Compute, DB, Networking, etc. and track usage trends, so that teams can instantly spot a newly exposed asset.

VULNERABILITY AND PATCH MANAGEMENT

Continuously scans for OS and library vulnerabilities in VMs, containers, and managed services. Instead of just notifying, a prevention-first CNAPP will link vulnerabilities to risk (using exploitation likelihood or asset criticality) and can drive automated patch workflows. For example, automatically updating missing-patch after every scan and prioritizes high-severity patches for remediation.

POLICY AND COMPLIANCE ENGINE

Embeds security benchmarks and compliance standards into automated checks. Preventive posture means blocking or alerting on policy violations immediately. For example, using composite of NIST, CIS, PCI, HIPAA, SOC2 rules, so that any deviation is automatically flagged as a “Fail” and then fixing it. This ensures security is enforced by default according to global best practices.

ANALYTICS AND AI

Incorporates analytics to correlate threats across tools. AI assistants can answer queries on demand. For example, generative AI-powered insights, summarizing complex dashboard data in plain language helps a SOC analyst triage issues faster. AI also complements anomaly detection, spotting irregular traffic spikes that could signal an active breach, and then auto-applying a policy fix.

By integrating these components, a CNAPP can cover threats “from code to cloud.” And when tuned to prevention, it can actually stop many attacks from materializing. In the next section, we’ll look at effective strategies for using a CNAPP in a prevention-first way.

Prevention-First Best Practices with CNAPP

Choosing the right CNAPP is only part of the journey. Equally important is how you implement it. The following best practices help embed prevention into your cloud security program:

"SHIFT LEFT" INTO DEVELOPMENT

Embed CNAPP controls early. Integrate IaC scanning and container-image checks into CI/CD pipelines so that insecure configurations or vulnerable code are blocked before deployment. For example, a policy-as-code system can reject any code change that violates least-privilege guidelines or compliance rules. This prevents issues from reaching production where they become emergencies.

AUTOMATE REMEDIATION

Leverage the CNAPP to automatically fix straightforward issues. If the platform detects an unauthorized open port or a publicly exposed bucket, it should either close it instantly or escalate immediately with remediation playbooks. For instance, running continuous scans and automatically whitelisting or remediating anomalies using prebuilt response schemes. This reduces dwell time for threats.

IMPLEMENT ZERO TRUST PRINCIPLES

Use your CNAPP's identity governance features to enforce strict access controls. Adopt just-in-time access, multifactor authentication (MFA), and regular entitlement reviews. CNAPPs with CIEM capabilities help identify any "over-privileged" accounts that violate the principle of least privilege. In practice, this might mean automatically disabling inactive accounts or removing wildcard permissions, mitigating the risk of stolen credentials.

USE INTELLIGENT ALERTING

Tune the CNAPP to correlate across data sources and suppress noise. Modern CNAPPs often use risk scoring or AI to prioritize alerts, reducing alert fatigue. For example, a CNAPP might only escalate a misconfiguration if it coincides with an active threat or affects a high-value asset. This allows security teams to focus on the most pressing threats first.

CONTINUOUS COMPLIANCE MONITORING

Regularly run all relevant compliance checks against standards like HIPAA, ISO, and GDPR in the CNAPP, and automatically block or tag noncompliant resources. Many CNAPPs let you apply organization-specific policies.

INTEGRATE WITH EXISTING TOOLS

A CNAPP should complement — not replace — other preventive controls. Pair it with network firewalls, API gateways, and Web Application Firewalls (WAFs) as suggested by experts. For example, if the CNAPP flags an app vulnerability, have the WAF automatically apply a blocking rule until the app can be patched. Likewise, feed CNAPP findings into SIEM/SOAR systems so that containment actions, like isolating a compromised server, can be triggered promptly.

FOSTER A SECURITY CULTURE

Prevention relies on people too. Train developers and operators on secure coding and cloud hygiene. Use the CNAPP's insights to give continuous feedback. For instance, dashboard trends could show teams where their errors lie. Many CNAPP platforms offer trend graphs to identify recurring vulnerabilities or seasonal spikes. By making security a shared responsibility, you multiply the impact of prevention tools.

All things considered, the ideal CNAPP should be the enabler of a prevention-first program. It shines most when woven into DevOps practices and automated processes.

Criteria for Choosing the Right CNAPP

Not all CNAPPs are built alike. When evaluating products, use the following factors with a prevention-first mindset.

Comprehensive Coverage

The CNAPP should support all your cloud platforms, like AWS, Azure, GCP, and Kubernetes to name a few. Ideally, it unifies findings across clouds in one pane. A multicloud CNAPP avoids blind spots.

Prevention-Focused Features

Look for embedded automation and features like auto-remediation and policy enforcement; basically, functionalities that extend beyond reporting. For instance, platforms that can fix or whitelist anomalies continuously are preferable. Also check for built-in benchmarks and policies like CIS or NIST that can be enforced automatically.

Integration with DevOps

Confirm that the CNAPP integrates with your CI/CD pipeline and IaC tools, such as Terraform, CloudFormation, and Git repositories. Prevention happens early, so a CNAPP must scan code and configuration files on check-in.

Advanced Analytics

AI capabilities are a plus. A CNAPP with machine learning can reduce false positives and catch novel attacks. For instance, Saner Cloud includes an AI assistant that summarizes dashboard data into plain language, and provides live insights after each scan. Those features can speed decision-making.

Scalability and Performance

The platform must handle your cloud scale. It should perform frequent scans — possibly daily — without crippling costs. A prevention-focused CNAPP will often run continuously in the background. Evaluate how the product scales by raising questions like, “Does it use SaaS or regional scanning engines?”

Reporting and Alerting

While prevention is the goal, you still need visibility. The CNAPP should deliver easy-to-understand dashboards, trend analysis, and alerting workflows. Look for features like live trend charts, tracking number of failed checks over time, and drill-down reporting that aids both security and ops teams.

Vendor Reliability

Finally, pick a vendor with timely updates and intelligence feeds. Cloud threats evolve rapidly, so the CNAPP's security knowledge base must stay current. Reputable vendors often update their benchmarks and scanning content monthly or quarterly.

After you assess such factors, you'll guarantee that the CNAPP you choose can actually enforce prevention and not just shake out old vulnerabilities.

LET'S RECAP

1. Comprehensive Coverage
2. Prevention-Focused Features
3. Integration with DevOps
4. Advanced Analytics
5. Scalability and Performance
6. Reporting and Alerting
7. Vendor Reliability

Saner Cloud by SecPod: A Prevention-First CNAPP

When it comes to prevention-first CNAPPs, Saner Cloud by SecPod exemplifies the approach. Saner Cloud offers an integrated platform covering CSPM, CIEM, CSAE, posture anomaly management (CSPA), risk prioritization, vulnerability management, patch management, and more, all in one solution. Its design reflects a clear prevention mindset:

Continuous, Automated Scanning

Saner Cloud's scanners run day and night, continuously assessing your cloud environment. Any anomalies found are automatically fixed or placed on a whitelist using pre-built response schemes. This means known issues can be closed within minutes of discovery, greatly narrowing the attack window.

Vulnerability and Misconfiguration

Beyond posture checks, Saner Cloud continuously identifies vulnerabilities and misconfigurations across both infrastructure and workloads — automating their mitigation to keep risk exposure to an absolute minimum.

Generative AI Insights

To aid rapid decision-making, Saner Cloud includes a built-in AI assistant. It interprets visualizations and tabular data, providing human-readable summaries. Security analysts can query the dashboard and get instant answers. This cutting-edge feature helps teams understand risks faster and focus on prevention actions.

Full Visibility and Exposure Management

The platform's Cloud Security Asset Exposure (CSAE) module gives full visibility and control over all cloud assets. It can automatically flag publicly accessible resources with distinct color codes, show outdated or deprecated services, and categorize assets by type or region. This transparency ensures nothing falls through the cracks, so even hidden exposures are caught.

Cloud Security Posture Anomaly (CSPA)

Saner Cloud's CSPA dashboard surfaces anomalies by confidence level — high, medium, or low — so you know where to act first. The Posture Anomaly Distribution view summarizes total anomalies and their confidence tiers in real-time, while the Anomaly Radar and real-time "Posture Anomaly Details" view drill into specific misconfigurations or policy violations by resource category and region.

Risk Prioritization

Findings are triaged using SecPod's proprietary machine learning, categorizing risks into Act, Attend, Track*, and Track, so you patch the most pressing issues first and allocate resources intelligently.

Workload Management & Protection (CWPP)

Saner Cloud's CWPP layer safeguards every cloud workload — whether VMs, containers, databases, or serverless functions — by extending visibility into identity & entitlement management, posture anomaly detection, patching status, and asset exposure across those workloads.

Built-in SecPod Default Benchmark

Saner Cloud comes preloaded with the SecPod Default Benchmark, combining best practices from NIST, CIS, PCI, HIPAA, SOC2, and more. Every resource is continuously checked against these standards, giving you compliance-by-design and greatly simplifying audits.

Broad Cloud Platform Support

Saner Cloud supports all leading public clouds (AWS and Azure out of the box) — and updates live after each scan — so multicloud teams get unified dashboards and controls across providers.

Actionable Remediation Guidance

Findings in Saner Cloud include detailed recommendations. For example, the patch management module prioritizes missing patches by severity and even tracks patch aging trends. Administrators can immediately see which patches have been outstanding longest and act before vulnerabilities are exploited.

Real-Time Dashboards

Every dashboard in Saner Cloud updates live after each scan. Users see trends over time and can drill into any finding. The Trend reports graphically depict vulnerable resources over days or weeks, helping teams anticipate and prevent recurring issues.

In combination, these features give Saner Cloud a true prevention-first posture. Rather than simply inventorying past missteps, it actively helps your IT and security teams harden your cloud environment in real-time. The automated fixes and AI insights remove many manual steps, so security staff can focus on strategy rather than triage. And because SecPod continuously updates its security intelligence and benchmarks, customers are empowered to constantly safeguard themselves against persistent and emerging threats.

As a preventionfirst CNAPP, Saner Cloud embodies the principles outlined in this handbook. It integrates cloudwide protection, automates remediation, and provides an always-on defense layer. For CISOs and architects seeking to secure the cloud by design, Saner Cloud offers the technical features and unified approach required to make prevention an everyday practice.

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:

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

www.secpod.com | info@secpod.com