COSMIC ARMOR

secure system

CosmicArmor Cloud Security Platform

Cloud Security That's Easy To scale

Overview

Cosmic Armor is built for organizations that want to spend less time sifting through endless alerts and more time taking action on the risks that truly matter. As a leading Cloud Security Platform, Cosmic Armor empowers security teams to work smarter—not harder—by delivering clear, prioritized insights that drive faster, more effective remediation. Trusted by security teams across industries, Cosmic Armor is an enterprise-scalable platform built to protect complex multi-cloud estates with low operational overhead. With seamless integrations into over operational tools—such as Slack, Jira, etc. Cosmic Armor fits effortlessly into your existing workflows, accelerating outcomes without disrupting operations.

Why Cosmic Armor?

- ✅ Unified Cloud Security Platform
- ✅ Deploys in Minutes
- ✅ 100% Continuous Coverage
- ✅ AI-Driven Risk Prioritization

A Unified Platform For Complete Cloud Security

Cosmic Armor delivers end-to-end visibility and protection across your entire cloud environment—including workloads, identities, configurations, and compliance—on AWS, Azure, Google Cloud, Kubernetes.
Our platform consolidates fragmented tools into a single, seamless solution—eliminating the complexity of managing multiple point products and enabling faster, more effective security operations at scale.

Cloud Security That's Built to Scale

Cosmic Armor uses an agentless-first approach, connecting to your cloud environment in minutes—no disruption, no complex deployment.
Our proprietary SideScanning™ technology delivers deep, continuous visibility across your infrastructure without installing agents.
Need real-time protection? We offer a lightweight sensor for critical workloads—scalable, efficient, and designed for speed.

Accelerate Cloud Security with AI

Speed matters in the cloud—and Cosmic Armor puts AI at the center of faster, smarter security.By leveraging advanced Generative AI, we simplify threat investigations, automate remediation, and reduce reliance on deep technical expertise.
The result? Security, DevOps, and engineering teams save valuable time while dramatically improving outcomes across the board.

Cosmic Armor's Defining Features

Total Visibility. Total Control.

Cosmic Armor continuously protects all cloud assets—without requiring agents—by detecting risks across every layer of your cloud environment. This includes: misconfigurations, vulnerabilities, malware, overprivileged identities, exposed sensitive data, API threats, suspicious activity, AI risks, and more.

Unlike point solutions, Cosmic Armor provides deep, contextual insight into your environment, surfacing interconnected risks that others miss—so you can stop threats before they reach your crown jewels.

Compliance, Handled Continuously.

With support for 180+ regulatory frameworks and CIS Benchmarks, Cosmic Armor delivers continuous, automated compliance monitoring. You can fully customize frameworks and schedule detailed reports to ensure your cloud posture meets evolving regulatory and business requirements.

Security Across the Entire SDLC.

From SCM posture management to static and dynamic code analysis, Cosmic Armor secures every phase of your software development lifecycle. We support advanced tools like SCA, SAST, secrets detection, IaC scanning, and container image scanning—tracing risks back to their source and enabling seamless remediation via Cloud-to-Dev capabilities.

"Cosmic Armor: A Unified Cloud-Native Application Protection Platform (CNAPP)"

Cloud Security Posture Management (CSPM) | Cloud Workload Protection (CWPP) | Vulnerability Management | API Security | Cloud Infrastructure Entitlement Management (CIEM) | Kubernetes Security | Data Security Posture Management (DSPM) | Multi-Cloud Compliance | Cloud Detection & Response | AI Security Posture Management (AI-SPM) | Application Security

Modern Day Complexities adapting our Public Cloud Infrastructure

Securing Cloud Infrastructure | Discovery & Visibility | Mis-Configuration | Compliance | Automated Risk Exposure | Remediation | Security Misconfiguration

CSPM - Cloud Security Posture Management

Cloud Security Posture Management (CSPM) is a security approach designed to continuously monitor and improve the security posture of cloud environments. It focuses on identifying and correcting misconfigurations, compliance violations, and potential security risks in cloud infrastructure. As organizations increasingly adopt cloud services, the complexity and scale of cloud environments make manual oversight difficult and error-prone. CSPM helps automate the detection of vulnerabilities such as open storage buckets, excessive permissions, and unencrypted data, which are common causes of cloud-based breaches. By maintaining visibility across cloud assets and ensuring adherence to security and compliance best practices, CSPM plays a critical role in reducing risk and maintaining a strong security framework in dynamic cloud environments.

Asset Discovery

Cosmic Armor performs continuous asset discovery to ensure complete visibility across cloud environments. It automatically identifies and catalogs all cloud resources—including compute instances, storage, databases, containers, and identities—across multiple cloud platforms. This enables organizations to maintain an accurate, real-time inventory of their digital assets, detect unauthorized or unmanaged resources, and proactively manage risks. By building a comprehensive map of the cloud infrastructure, Cosmic Armor lays the foundation for effective security posture management, compliance tracking, and incident response.

CWPP - Cloud Workload Protection Platform

CWPP is a unique platform discovers all the workloads across the Multi-Cloud environment and detects Vulnerabilities, Malware and Misconfigurations. Up to date Threat database to stop threats. Runtime Security to prevent exploitation at memory level. CWPP behaviour is to detect any anomalies that could include threats as and when they occur. Single pane of glass visibility into every system from a central location.

CIEM - Cloud Infrastructure Entitlement Management

CIEM automates, correlates and contextualizes security signals across multiple cloud-native tools, providing security and SDLC teams shared visibility for anticipating, identifying and correcting discovered vulnerabilities. DevSecOps teams practicing secure-by-design principles - testing, triaging, and mitigating risk - earlier in the SDLC cycle. CNAPP gives security teams easy access to monitor and set appropriate permissions, ensuring that cloud identities are assigned the minimum level of privileged access as necessary, thus reducing the risk of unauthorized access on the network. Alongside enforcement of least privilege. Our CNAPP embeds Zero Trust policies when implementing a CNAPP. While building on a zero trust architecture, security teams can use risk context from our CNAPP to make more intelligent decisions about what access to assign various cloud workloads. CIEM leverages combined superior AI & predictive analysis to co-relate the policy changes, also providing remediation recommendations to lower IAM risks. Provides granular, continuous entitlement assessments for the cloud infrastructure.

Attack Detection

Cosmic Armor actively detects and responds to potential cloud-based attacks in real time. It continuously monitors cloud environments for suspicious behavior, unauthorized access attempts, privilege escalations, lateral movements, and anomalous activity across accounts and services. By analyzing user behavior, network traffic, and configuration changes, Cosmic Armor identifies threats such as account compromises, data exfiltration, malware deployment, and insider attacks. Once a threat is detected, the platform can trigger automated alerts, provide detailed context for investigation, and optionally initiate predefined response actions to contain the threat. This proactive approach enables organizations to reduce detection and response times, minimize damage, and maintain the integrity of their cloud infrastructure.

Where cloud chaos ends—and intelligent defense begins!

Our Current Location

Currently we are placed in:

India HQ

Plot No. 338, Phase 4, Udyog Vihar,
Sector 19 Gurugram – 122016

Expanding Horizons

We are expanding soon in these locations

CANADA

UAE

SINGAPORE