Stop Operating Your Cloud In The Dark

Monitor and Protect Your Cloud-native Applications and Data in Runtime

Today, valuable data and critical cloud applications run in continuously changing IaaS environments that are under constant attack. The news is full of data breaches and cloud services exploited or knocked offline by attacks. Last year, an IDC research study estimated that 80% of organizations in the cloud had experienced a data breach within the preceding 18 months. It's clear that existing security approaches using static reports, complicated deployments, disparate tools, and manual remediation aren't working.

Cloud-native applications and the data they contain must be continuously protected or the business suffers. Static compliance reports and lists of vulnerabilities and misconfigurations are not enough. Securing cloud-native applications and data requires continuous visibility and runtime protection that is data-centric, agentless, and automated

Start protecting your cloud in minutes

Linkedin

01. Protect your data in runtime

- Monitor everywhere you have data: cloud storage, databases, container volumes, east-west traffic
- Classify and track confidential and regulated data: PII, PCI, HIPAA, design docs, source code, etc.
- Detect risky access, public exposures, abnormal encryption, and unauthorized east-west data flows
- Automatically remove data exposures and block high-risk users, accounts, APIs, and workloads
- Use native data classification or integrate to extend your enterprise DLP to your cloud

02. Protect your running application

- Monitor and control your networked Kubernetes environment of workloads, microservices, APIs, and east-west traffic
- Detect and block abnormal traffic, unauthorized APIs, and rogue workloads
- Track vulnerabilities and misconfigurations in the context of your running application
- Protect applications with micro segmentation and network policies to isolate compromised assets and block threats

03. Continuously monitor and improve your security and compliance posture

- Automatically monitor compliance posture across multi-cloud: CIS Benchmark, NIST, PCI, SOC2, etc
- Continuously scan assets for misconfigurations, vulnerabilities, and open ports
- Detect and block attacks and high risk user/account access and activity
- Prioritize remediation with the full context of the running networked environment and if sensitive data is involved

Stay in the loop!

Get notified about the latest product releases & updates

Your Email

Submit

About Microsec.ai

Get easy-to-deploy, runtime visibility, protection, and compliance monitoring for cloud serverless, VM, and Kubernetes environments. Microsec.ai is the only agentless, data-centric, runtime cloud-native application protection platform (CNAPP) that protects your data and applications with data loss prevention (DLP), east-west network traffic control with self-healing micro segmentation, security posture management, and compliance analysis in one unified solution.

MICROSEC.AI

MICROSEC.AI

Agentless real-time security dynamically protecting your cloud, container, and data assets

Privacy Policy | Terms & Condition

CONTACT US

USA Office: 4701 Patrick Henry Dr. Building 2, ste.170 Santa Clara, CA 95054

India Office: 103/28, Mansarovar, Jaipur, Rajasthan, INDIA, PIN: 302020

support@microsec.ai