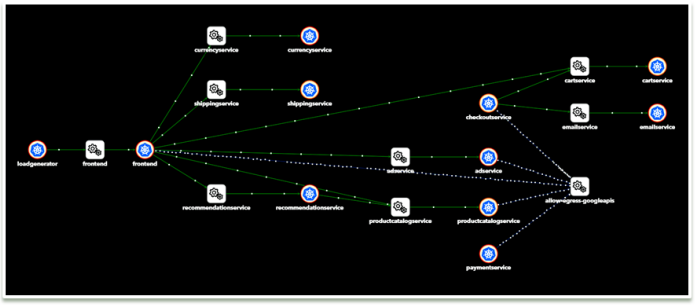
MICROSEC.AI

Stop Operating your Cloud in the Dark

Start Protecting your Data and Apps in Runtime

Today, valuable data and applications run in continuously changing IaaS environments are under constant attack. Data breaches are headline news. Last year, the top 5 data breaches alone represented nearly 2 Billion records exposed. Existing approaches using static reports, complicated deployments, disparate systems, platform-centric options, and manual remediation aren't working.

Your data must be continuously protectedand critical applications must be always-on or the business suffers. You need continuous visibility and protectionthat is runtime, data-centric, self-healing, and easy-to-deploy.



Start protecting your cloud in 5 minutes.
Microsec.ai connects to your cloud via APIs

About Microsec.ai

Embrace runtime protection with data loss prevention (DLP) and east-west network control. Microsec.ai is the only agentless, data-centric, runtimecloud native application protection platform (CNAPP) to protect your data and applications with extensive DLP controls, east-west network traffic control with self-healing microsegmentation, security posture management, and compliance analysis in one unified solution.

Protect your data in runtime

- Monitor everywhere you have data - cloud storage, databases, container volumes, east-west traffic
- Classify and track sensitivedata (PII, PCI, HIPAA, design docs, source code, etc.)
- Detect risky access, public exposures, and unauthorized east-west data flows
- Automatically remove data exposures and mitigate risk through protective access and network policies
- Use native data classification or integrate to extend your existing enterprise DLP policies to your cloud

Protect your running application

- Visually monitor and control your networked Kubernetes environment of workloads, microservices, APIs, and east-west traffic
- Track vulnerabilities and misconfigurations within the full context of the running environment
- Detect and eliminate abnormal traffic, unauthorized APIs, and rogue workloads
- Protect the system with self-healing microsegmentation and network policies to isolate and eliminate threats

Continuously monitor and improve your cloud security and compliance posture

- Automatically monitor compliance posture across multiple cloud platforms
- Continuously scan for misconfigurations, vulnerabilities, and open ports
- Detect and block high risk user and account access and activity
- Prioritize remediation with the full context ofthe running networked environment and if sensitive data is involved