

Checklist to implement a

Zero Trust Cloud-Native Environment

01. Discover & secure data, communications, & assets

Users/services/roles, devices, network communications, applications, microservices, workloads, & especially sensitive data

02. Limit access permissions to only the resources that each user needs

Enforce Role-based Access Control (RBAC), Multi Factor Authentication (MFA), Zero Trust Network Access (ZTNA), security attribute & UEBA -based access control

03. Harden workloads, networks, & credentials

Keep software up-to-date, secure data systems, close unnecessary open ports, require strong passwords/identity access management (IAM)

04. Implement network monitoring & traffic control with microsegmentation

Continuously monitor network traffic for abnormal activity, segment sensitive data zones in your environment, use microsegmentation to isolate compromised workloads

05. Encrypt sensitive data & workload connectivity

Deploy encryption for data-at-rest in storage, databases, & volumes; & encrypt workload communications to protect data-in-motion

06. Enact vulnerability management (CWPP)

Vulnerabilities are inevitable; deploy cloud workload protection, develop & follow a documented vulnerability management process

07. Implement cloud security posture management (CSPM)

Continuously monitor your cloud for misconfigurations & remediate; most successful breaches take advantage of security posture misconfigurations at some point in their kill chain

08. Automate run-time security remediations, processes, & policies

Save time & improve your protection by automating response & remediations via policy as much as possible

09. Protect data with Data Loss Prevention (DLP)

Monitor and control confidential & regulated data everywhere at-rest & in-motion in cloud to prevent expensive data breaches

Linkedin

in

f

twitter

email

download

HIPAA Compliance Requirement

Stop Operating Your Cloud In The Dark

Stay in the loop!

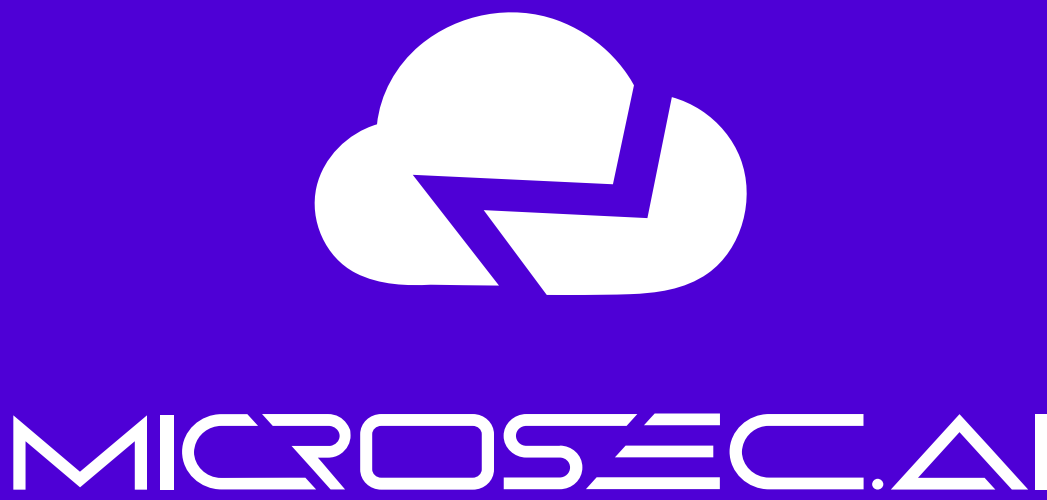
Get notified about the latest product releases & updates

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

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

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

© 2021 Microsec, Inc. All rights reserved.

Privacy Policy | Terms & Condition

support@microsec.ai