SYNOPSYS®

Cloud Security Maturity Action Plan (MAP)

Get clear directions for establishing or maturing your software security initiative in the cloud.

Overview

Organizations of all sizes are continually striving to balance modernization, dependability, productivity, and security as they increasingly use public cloud services to host and deliver their application workloads. But whether you're migrating to the cloud or developing cloud-native applications, you need to adapt your software security practices to address the unique opportunities and risks that come with cloud deployment. The Synopsys Cloud Security Maturity Action Plan (MAP) helps you build a detailed plan and roadmap with a prioritized list of recommendations to improve your cloud security strategy as part of your software security initiative (SSI).

Build, evolve, and maintain your SSI in the cloud

The Cloud Security MAP helps you set cloud security objectives, outline a strategy to reach those objectives from where you are today, and evaluate the resources and processes you'll need to reach your cloud security goals. We work closely with your key stakeholders to understand your organization's current state, define an achievable future state, and develop a MAP to advance your SSI. The plan addresses the following security capabilities.

Once you have your Cloud Security MAP, we can help you socialize it to get the buy-in, resources, and support you need to implement it.

Identity and access management

Identity and access management is the backbone of cloud security deployment. To secure your cloud deployment, you must establish accounts with the appropriate level of privileges to provision or orchestrate resources. Key areas to assess include

- Audits for sources of authentication and authorization
- Policies and procedures for appropriate user groups
- Roles and responsibilities for minimal human access to production systems
- Data protection

Safeguarding important data is a critical piece of building and operating information systems in the cloud. Key areas to assess include

- Inventory and classification of data assets
- Policies and procedures for safeguarding data in transit and at rest
- Compliance requirements based on business needs and risk tolerance
- Opportunities for encryption and responsible retention of data

Infrastructure security

The foundational infrastructure for the cloud must be inherently secure, whether your cloud is public, private, or hybrid. Key areas to assess include

- Security requirements for the network, compute, and storage stack
- Network topology in regard to segmentation and multitenancy concerns
- Provisioning needs for automation and orchestration opportunities
- Access control requirements

Logging and monitoring

Logging and monitoring are key to gaining greater visibility into a cloud environment in real time, or near real time. Key areas to assess include

- Inventory lists of logging assets to identify aggregation, correlation, and analysis
- Policies and procedures for alerting and notifications
- Thresholds for critical business functions
- Tools for logging and monitoring activities

Incident response

You need a solid incident response plan to contain an event and return to a known good state. Key areas to assess include

- Categorization of critical business functions and assignment of risk profiles
- Policies and procedures for incident response, alerts, and notifications
- Metrics to determine the severity of incidents and assign appropriate responses
- Simulation and red teaming efforts to test incident response infrastructure

Vulnerabilities and configuration analysis

Using an automated security mechanism for both configuration management and vulnerability assessments can be a cost-effective approach for cloud environments. Key areas to assess include

- Cloud configurations to understand resource deployment and potential vulnerabilities
- Security testing for mobile and web applications, APIs, and containers

Sized to fit

Take advantage of our 20+ years of experience helping customers establish successful SSIs. Once you have your Cloud Security MAP, we can help you socialize it to get the buy-in, resources, and support you need to implement it.

Features

Cloud Security MAP feature	Details
Current state	• Current capability maturity • Six security capabilities
Future state	• 24-month roadmap • Recommendations for six security capabilities
Deliverable format	• Executive PowerPoint with current state and roadmap views

SYNOPSYS®

The Synopsys difference

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. With Synopsys, your developers can secure code as fast as they write it. Your development and DevSecOps teams can automate testing within development pipelines without compromising velocity. And your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com