SYNOPSYS®

Cloud Configuration Review

Find out whether your cloud configuration stands up to security checks

Overview

For organizations migrating to the Cloud or maintaining cloud applications, regular modifications to the network configuration, user access, application architecture, platform components, and security controls are necessary to keep up with business need. But even if reasonable change management processes are in place, deployment mistakes, configuration drift, and bad practices have the potential to introduce security flaws and exacerbate risks in time.

Synopsys Cloud Configuration Review audits the run-time configuration of cloud environments and security controls. We identify weaknesses in the cloud infrastructure that deviate from security standards, and expose architectural flaws. Cloud Configuration Review provides a report snapshot that describes how your applications meet or fail security checks against a known list of common cloud misconfigurations.

Synopsys Cloud Configuration Review

As part of a Cloud Configuration Review, we conduct interviews with application stakeholders (business analysts, developers, testers, program and product managers, etc.) to understand your application's business context and security criteria. Following this, we execute a manual and automated tool analysis of your cloud environment. The following are some of the security concerns we review during a Cloud Configuration Review:

- **Authentication, authorization, and identity management.** We assess your approach to access controls, including federation and realization as identity access management (IAM) policy. We evaluate the proper use of security groups to ensure that the principles of least privilege and separation of duties are followed. Other concerns include protection of privileged accounts using appropriate technologies (e.g., multifactor authentication).
- **Cloud networking.** We check your cloud networking configuration for proper isolation of sensitive cloud workloads from one another, correct use of network security groups and network ACLs, validation of authorization to make network changes, proper encryption of network traffic within and outside the cloud environment, and other controls required to guarantee secure networking in the cloud infrastructure.
- **Cloud compute.** We review the implementation of cloud virtual machines to ensure that they have been appropriately permissioned and secured to access company workloads.

- **Cloud storage.** We evaluate the implementation of controls used to protect cloud storage, including object storage, block storage, file storage, message queues, and other storage services used by the application. We determine whether data directed to application storage is properly protected in motion and at rest and not exposed to unauthorized parties, including anonymous users—a situation that is prevalent with many cloud service implementations.
- **Other services.** We assess other services you may have implemented to support your cloud workload, including database services (SQL or NoSQL based), server-less functions (e.g., AWS Lambda and Azure functions), logging and monitoring services, and backup and disaster recovery infrastructure. In each case, we review the service's configuration, identify security misconfiguration scenarios, and determine whether these exist on your infrastructure.

- Take full advantage of the security controls offered by your cloud provider.
- Address security gaps between what you think is covered by your cloud provider and what's actually covered.

The methodology used to develop and execute these reviews is an amalgam of techniques, manual and automated, that factor in best practices from cloud service providers and security standards from reputable sources (including hardening guides such as the Centre for Internet Security [CIS] Benchmarks). We periodically align our methodology to the compliance and regulatory standards that many organizations have to adhere to when implementing computing services (HIPAA/HITEC, ISO/IEC 27001, ISO/IEC 27017, PCI DSS 3.x, etc.).

At the end of a configuration review, we deliver a summary of your implemented security controls, our opinion on the effectiveness of these controls, and remediation guidance detailing how to improve poorly implemented controls. We can provide a sample of a configuration review deliverable on request.

Benefits

Cloud Configuration Review focuses primarily on the application's supporting cloud infrastructure. It provides insight into how effective the cloud application is at using a cloud provider's security controls to protect workloads. Traditional penetration testing cannot answer this question.

Customers who are familiar with the shared responsibility model of the Cloud can use a configuration review as a litmus test: How well are you using the security features offered by your cloud provider? Are there any mistakes you should correct quickly before your application starts receiving production traffic?

An alternative way of understanding a configuration review is to assess the infrastructure supporting the cloud application. Because most cloud providers expose infrastructure configuration programmatically, much of this configuration is now the responsibility of development teams and DevOps responsible stakeholders. Cloud Configuration Review assures stakeholders that the infrastructure has been properly configured to follow best practice guidelines and compliance/regulatory standards.

The Synopsys difference

Synopsys offers the most comprehensive solution for building integrity—security and quality—into your SDLC and supply chain. We've united leading testing technologies, automated analysis, and experts to create a robust portfolio of products and services. This portfolio enables companies to develop customized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. Synopsys, a recognized leader in application security testing, is uniquely positioned to adapt and apply best practices to new technologies and trends such as IoT, DevOps, CI/CD, and the Cloud. We don't stop when the test is over. We offer onboarding and deployment assistance, targeted remediation guidance, and a variety of training solutions that empower you to optimize your investment. Whether you're just starting your journey or well on your way, our platform will help ensure the integrity of the applications that power your business.

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

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

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

SYNOPSYS®
Silicon to Software™