SYNOPSYS®

Cloud Architectural Risk Analysis

Discover where your cloud security controls are insufficient and how to improve them.

Overview

Public cloud providers supply services that organizations use to develop cloud applications. Unfortunately, an inherent flaw of these services is that their globally accessible nature can lead to unauthenticated access. In the shared security model, the cloud provider offers security features that organizations can use to protect their cloud applications and help mitigate this risk.

Whether you are developing a cloud-native application or migrating an existing application to the cloud, it is critical to have the appropriate infrastructure and application design. A well-thought-out design template will ensure that you are implementing cloud provider services effectively and securely. It provides a general overview of the system and simplifies your decisions regarding where to implement security controls.

Synopsys Cloud ARA

Synopsys Cloud Architectural Risk Analysis (ARA) is an interview-driven application and cloud infrastructure assessment process that evaluates a cloud application's design and security controls. Cloud ARA can help you design security controls for a cloud migration or assess the effectiveness of controls in an existing application.

Cloud ARA identifies all platform components in a cloud application and their architectural relevance. It analyzes the security threats affecting these components and cross-references the security controls in place to determine how effective these controls are at reducing threats. The output is a design document that highlights areas where controls are sufficient, insufficient, or absent, and proposes remedies to improve the application's security posture. The table on the next page details the security areas examined.

Authentication, authorization, and identity management	• Access controls for the cloud provider's management and monitoring interfaces • Access controls for the application hosted on the cloud platform • Life cycle management of access controls, including the creation and revocation of entitlements
Cloud networking	• Architecture of the cloud networking infrastructure and security protections for data in motion • Solutions to protect the application from unauthorized traffic • Approach to isolating sensitive compute workloads from the network
Cloud computing	• Measures to harden and protect compute nodes and continuously assess their security posture • Approach to preventing rogue compute instances from participating in workloads
Cloud storage	• Controls to protect data at rest on cloud service components, including blocks, blobs, files, queues, and other services • Access controls to protect data from untrusted parties, including anonymous users
Other services	• Integration of other platform-as-a-service (PaaS) or infrastructure-as-a-service (IaaS) services including SQL and NoSQL stores, orchestration managers, container solutions, automation for deployment (infrastructure-as-code), and continuous integration system solutions • Security controls in these solutions to prevent leaking of trusted data to unauthorized parties • Security controls in place to protect the cloud application's secrets (usernames, passwords, and database and other service credentials, such as API keys) from unauthorized access
Operational management processes	• Measures to properly log and audit security activity by management interfaces and the cloud application • Software update and patching processes for services deployed in an IaaS configuration • Protection against malware for services that retrieve data from untrusted users or sources
Business risks	• Any concerns affecting the business elicited during interviews, including disaster recovery and resilience to cloud infrastructure failure

The Cloud ARA methodology factors in best practices from cloud service providers and security standards from reputable sources, including hardening guides such as the Center for Internet Security benchmarks. Synopsys also periodically realigns the methodology to the compliance and regulatory standards that many organizations must adhere to when implementing computing services (HIPAA/HITEC, ISO/IEC 27001, ISO/IEC 27017, PCI DSS 3.x, etc.).

The artifacts produced by a Cloud ARA can serve as blueprints for teams migrating applications with a similar risk profile. Performing a Cloud ARA during initial development of new applications can also provide recommendations that influence their design.

Benefits

Synopsys Cloud ARA offers significant benefits because its multipurpose nature focuses on the design of cloud applications and on cloud infrastructure support of application and security controls. Additionally, a Cloud ARA can be used to prioritize activities—for example, by highlighting services that deal with sensitive information or are likely to have weak security controls, which customers can focus on during implementation reviews. Possible follow-up assessments include configuration review, penetration testing, and vulnerability analysis or code review of the cloud application.

As a standalone service, Synopsys Cloud ARA fulfills many regulatory standards' requirement for a security architectural assessment. For example, the Cloud ARA diagram meets the ISO/IEC 27017 requirement for network diagrams to clearly identify high-risk environments and the dataflows into and out of them. A Cloud ARA also lists the security controls used to protect this data and makes recommendations when they are insufficient.

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