SYNOPSYS®

Cloud Security Blueprints

Guide your teams' security strategy when building or deploying cloud applications

Overview

Security teams working with organizations implementing cloud applications encounter several opportunities to generalize security controls. Whether the delivery model is infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), or software-as-a-service (SaaS), Synopsys can provide guidance for implementing cloud applications with our Cloud Security Blueprints. A Cloud Security Blueprint is a consumable reference architecture with baseline security controls that can help guide development teams and systems integrators building or deploying cloud applications.

Synopsys Cloud Security Blueprints

Cloud Security Blueprints solve some of the more difficult security issues that organizations face when building cloud workloads. We deliver blueprints for the following areas:

Federation and identity management	Manage access with on-premises identity stores (e.g., Active Directory and Samba).
Continuous integration / continuous delivery (CI/CD)	Build secure CI/CD pipelines with Jenkins to a cloud provider's scheduling and orchestration environment (e.g., Docker Swarm, Kubernetes, Mesos, and Nomad).
Container security	With the CI/CD pipelines above, create a secure pipeline for container scanning before deployment using Docker Bench, Aqua, Twistlock, Clair, and others.
Logging and monitoring	Monitor cloud and application workloads using logging and analysis tools.
Backup and disaster recovery	Implement backup and disaster recovery solutions for protecting cloud workloads in the event of catastrophic failure.
Secrets and credentials management	Use cloud provider vaults (e.g., Azure Key Vault and AWS Key Management Service) or third-party tools (e.g., HashiCorp Vault and Keywhiz) to protect and provision secrets to cloud workloads.
Service hardening	Harden cloud-provided services for increased assurance.

Synopsys Cloud Security Blueprints are delivered using infrastructure-as-code tools. We provide a security control matrix that maps the solutions outlined in the blueprint to the 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.). Synopsys consultants can also work closely with your development, testing, and operational management teams to customize or develop new blueprints that meet your requirements.

- Find clear answers to security questions about your cloud workloads.
- Get faster deployment, stronger security, continued compliance, and more business value—a win-win for all cloud deployment stakeholders.

Benefits

Reference guides. Our blueprints, delivered as infrastructure-as-code solutions, are in an immediately consumable format and can serve as implementation reference guides. Teams can pick up these blueprints, deploy them into their cloud environments, and start customizing them to support their service workloads.

Automated deployments to increase speed to market. Most organizations invest in the Cloud to accelerate their speed to market, and Synopsys Cloud Security Blueprints increase DevOps efficiency with solutions that automate environment deployment. Our blueprints allow organizations to rapidly provision and dispose of separate development, QA, and production environments in an elastic manner—while keeping all environments very similar in configuration.

Secure, compliant environments. A critical need for security, compliance, and development teams is adherence to regulatory requirements. Even after delegating infrastructure to a cloud provider, an organization is still responsible for certain aspects of security, owing to shared responsibility. Synopsys Cloud Security Blueprints offer solutions to many of these requirements and provide a clear line from policy demands to implementation, with reasoning as to why these solutions are the best choice for the reference architecture.

Synopsys Cloud Security Blueprints not only help customers accelerate cloud infrastructure deployments with environments that meet regulatory and compliance requirements, but also solve scenarios of critical concern to most security and compliance teams, all while supporting the needs of development teams who must focus on delivering business value.

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™