Feeling Secure in Synopsys Cloud

What Is Synopsys Cloud?

Synopsys has built a cloud model using Public Cloud Providers Microsoft Azure (Azure), Amazon Web Services (AWS), and Google Cloud Platform (GCP) to deliver a flexible and secure Bring Your Own Cloud (BYOC) offering. It plugs into Synopsys Cloud offering BYOC, and the infrastructure is built according to security best practices and standards. Cloud Service Providers operate under a shared security responsibility model where the Provider is responsible for securing the underlying cloud infrastructure. Synopsys is responsible for securing workloads and applying the highest levels of protection feasible at all layers.

What Qualifications Does Synopsys Have?

Based on ability to execute and completeness of vision, in 2021 Synopsys was recognized by Gartner as the leader in the Gartner Magic Quadrant for Application Security Testing (AST) for the fifth year in a row. Synopsys was also named leader in the Forrester Wave™ for Static Application Security Testing (SAST) based on an evalution of the Coverty® solution.

What Differentiates Synopsys On Security?

The company's innovative tools offer advanced protection against vulnerabilities. Synopsys is uniquely positioned to provide these products built with security in mind from the start because the entire suite of security tools and services are utilized. A risk-based approach to product security—defining the risks, measuring their levels of threat, and securing products—ensures that customers, in turn, can use the Synopsys products to secure their own.

How Does This Help Synopsys Customers?

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. As a recognized leader in static analysis, software composition analysis, and application security testing, the company is uniquely positioned to apply best practices across proprietary code, open source, and the runtime environment. With a combination of industry-leading tools, services, and expertise, Synopsys helps organizations maximize security and quality throughout the software development lifecycle.

How Does Synopsys Ensure Security?

These are the guiding principles that ensure safety for the public cloud:

- Data Classification: How sensitive is the data and how should it be protected
- Data Segregation: Production and non-production, sensitive and non-sensitive data should be placed in different cloud containers with logical controls for flows traversing those containers
- Auditing: Periodic reviews to ensure relevance, compliance with regulations and internal policies should be performed
- Monitoring: All activities should be monitored, and security personnel must be alerted on anomalous activity patterns
- Access Control: Access to cloud management must be carefully reviewed, granted, monitored, audited, and revoked with minimal privilege role-based access in mind

How Does Synopsys Control Security?

Synopsys leverages the following set of Cloud Security Controls and industry best practices provided by Cloud Security Alliance:

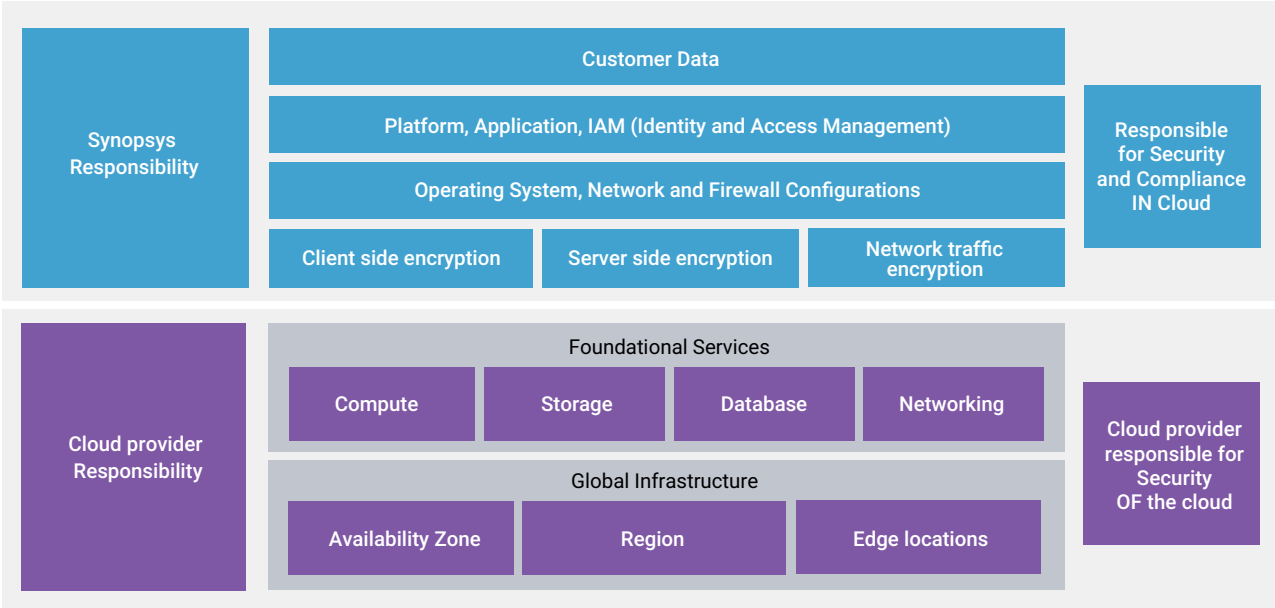
- Identity and Access Management
- Data Security
- Infrastructure Security
- Application and API Security
- Threat and Vulnerability Management
- Security Incident Response (IR)
- Compliance and Governance

Under the Shared Responsibility Model, the Cloud Service Provider is responsible for:

- Foundation services: networking, compute, and storage
- Global infrastructure
- End points

Synopsys is responsible for information security of:

- Customer data
- Customer application
- Operating system, network and firewall
- Identity and Access Management (IAM)
- High availability, scaling, and instance management
- Data protection (transit, rest, and backup)



What Is The Synopsys Security Architecture?

Synopsys provides a secure three-tier segregated architecture with segregation of Client Tier, Presentation Tier, Application, and Data Tier.

Infrastructure Security	Identity and Access Management	Data Security	Application Security	Logging & Monitoring	Incident Response
• Posture Management • Workload Protection • Vulnerability Mgmt • Dedicated VPC • Host Level Security	• MFA enforcement with Identity Provider integration • Authentication using role-based access • User and service account roles	• Data encryption at rest • Data encryption in transit • Azure Key Vault/Secrets Manager	• Static Application Security Testing (SAST) • Dynamic Application Security Testing (DAST) • Open-Source Scanning (OSS) • Web Application Firewall (WaF)	• Azure Resource Logs • Azure AD sign-in and Audit logging • Network Security group logs	• Secure Logging and SOC monitoring 24x7 • 3 Tiers of staffing for investigations • Threat hunting and intelligence forensics

Security by Design

How Does Synopsys Ensure Infrastructure Security?

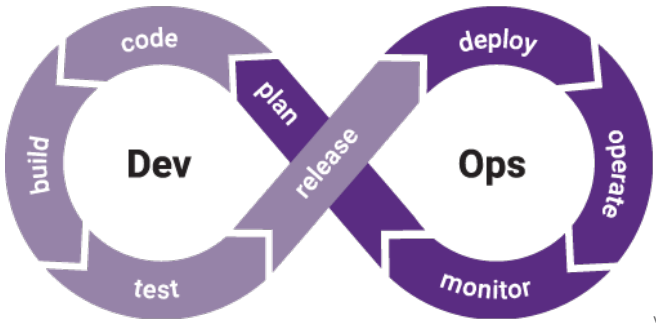
Cloud infrastructure such as on-premise datacenters needs to be managed securely with a multitenant consideration in mind and unique controls specific to the Cloud Service Provider environment. Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. To ensure that customer data is not compromised by infrastructure attacks, Synopsys enforces the following rules:

- A mitigation strategy quickly isolates suspicious instances (inside and outside)
- All Synopsys managed hosts are configured according to best practices
- Production and non-production environments are separated in such a way as to prevent unauthorized access between environments
- Access between environments occurs over encrypted communication channels only
- System updates and virtual image transfer occur over encrypted channels only
- Access to all cloud management functions and administrative consoles for virtualized systems is restricted to personnel based upon the principle of least privilege
- Patching and update procedures deliver security and product bug fixes and enhancements in a timely manner via encrypted communication channels

How Does Synopsys Ensure Application And API Security?

To ensure highly secure cloud applications for customers, Synosys follows the Secure Software Development Lifecycle (S-SDLC), which has various phases for Application and Interface Security and Security Requirements:

- Secure Architecture
- Threat Modelling
- Secure Coding and Security Training
- Application Scanning



v

How Does Synopsys Provide Threat And Vulnerability Management?

All infrastructure and production instances have threat prevention (anti-malware) components installed. Periodic vulnerability scanning is performed within the cloud environments and externally using an industry-recognized vulnerability scanner with up-to-date signatures. The results of such scans are reviewed and addressed based on their risk. A vulnerability management program monitors for, and addresses, Cloud Service Provider infrastructure vulnerabilities found by scanning, vendor, or external reporting.

How Does Synopsys Ensure Compliance And Governance?

Secure configuration standards are set for each system component used, whether a managed application or an internally managed system or application. These secure configuration standards align with governing standards such as CIS and PCI. Synopsys uses CIS Benchmarks for core OS hardening (Windows/Linux) and Cloud Service Provider and third-party published best practices for Cloud Service Provider services. Monitoring/audit procedures are in place to ensure compliance to the secure configuration standards. A vulnerability scanner performs authenticated scans and compares the results against the baseline to ensure compliance on a periodic basis. Independent reviews and assessments are performed on a periodic basis to ensure that the established policies, standards, procedures, and compliance obligations are addressed by:

- Complete infrastructure penetration tests on an annual basis for each service/component
- Cloud application penetration tests on an annual basis for each service
- Manual penetration tests of the customer-facing application/service performed by the in-house SIG (Software Integrity Group)
- Internal audits to ensure compliance with processes and procedures defined in this document, backed by automated configuration checks and manual reviews
- ISO27001 and SOC2 certification

How Are Authentication And Authorization Achieved?

Authentication and Authorization are achieved with existing customer-used identity systems SolvNet and Okta.

Is Multifactor Authentication (MFA) Supported?

All successful logins are challenged with Second Factor Authentication using Okta.

How Is Data In Transit Encryption Done In A Web Application?

Data in Transit Encryption is enforced by TLS 1.2 (HTTPS).

How Is Data At REST Encryption Done?

Data at REST Encryption is enforced with Native Key Management Service (KMS) with a Unique Key Encryption key (KEY) derived using AES-256:

- AWS—AWS KMS
- GCP—GCP Cloud Key Management
- Azure—Azure Key Vault | Microsoft Azure

Is IP Safelisting Supported To Allow Customer-Specific Traffic For BYOC?

IP safelisting is supported. Customers can provide IP address information during on-boarding and can maintain this.

How Are Vulnerability Management And Patching Performed?

Vulnerability Management scans are enforced using scheduled infrastructure and network scans. Application interfaces and infrastructure code are scanned using SAST, DAST, and SCA.

How Does Synopsys Handle Threat Defense And Incident Response?

Threat Monitoring is done using Log Ingestion to the Security Incident Event Monitoring (SIEM) Platform and correlated with Threat feeds. Configuration Management is achieved with a centralized deployed tool. Any actionable events are alerted to the Security Operations Center (SOC) for IR Incident Response. Synopsys provides Integrated Secure Monitoring and SOC Monitoring 24*7 using the follow-the-sun model.

Where Is More Information Available?

Contact a Synopsys account representative, contact Synopsys at cloud@synopsys.com, or visit https://www.synopsys.com/cloud to learn about and experience the benefits that Synopsys Cloud has to offer.