SYNOPSYS®

SYNOPSYS POLARIS SAAS SERVICE DESCRIPTION

SERVICE SUMMARY

For each of the below defined service level offerings, Synopsys will perform fAST Static Application Security Testing (“fAST Static”) and/or fAST Software Composition Analysis (“fAST SCA”) assessments for the Customer supplied application source code in support of an Application. The following sections provide an overview of the various levels of service offerings, as well as the defined program and support features. "Application" means a collection of Projects that are connected to or have been created to support a single business purpose. A "Project" supports an application. A project may be considered a single, unique application in its own right, or a contributing module or component to the application. In total, a single Application shall not exceed 1M lines of code.

POLARIS-SAAS SAST APPLICATION TESTING SUBSCRIPTION - AUTOMATED

The Polaris fAST Static subscription offering is based on a twelve (12) month consecutive period (“Subscription Term”) and based on the following process:

- A defined Application for the Subscription Term;
- Customer may create up to five (5) supporting Projects for the defined Application;
- Customer may utilize an unlimited number of single assessments during the Subscription Term which are allocated to the defined Application;
- Customer to submit the source code payload to the Polaris platform for fAST Static according to the Polaris user guide;
- Synopsys will conduct an automated source code analysis assessment leveraging the customer supplied source code; and
- Polaris Application Security test results are delivered to customer via Polaris’ portal.

POLARIS-SAAS SAST APPLICATION TESTING SUBSCRIPTION – FIRST SCAN TRIAGE

The Polaris fAST Static subscription offering is based on a twelve (12) month consecutive period (“Subscription Term”) and based on the following process:

- A defined Application for the Subscription Term;
- Customer may create up to five (5) supporting projects for the defined Application;
- Customer may utilize an unlimited number of single assessments during the Subscription Term which are allocated to the defined Application;
- Customer to submit the source code payload to the Polaris platform for fAST Static application security testing according to the Polaris user guide;
- Synopsys will conduct an automated source code analysis assessment leveraging the customer supplied source code;
- Synopsys will perform one-time results review audit of the assessment findings for each initial assessed project to identify and suppress false positives;
- All subsequent requests, all assessments will be delivered as automated scan; and
- Polaris Application Security test results are delivered to customer via Polaris’ portal.

POLARIS-SAAS PKG SAST/SCA TESTING SUBSCRIPTION – FIRST SCAN TRIAGE

The Polaris fAST Static and fAST SCA subscription offering is based on a twelve (12) month consecutive period ("Subscription Term") and based on the following process:

- A defined Application for the Subscription Term;
- Customer may create up to five (5) supporting projects for the defined Application;
- Customer may utilize an unlimited number of single assessments during the Subscription Term which are allocated to the defined Application;
- Customer to submit the source code payload to the Polaris platform for fAST Static and fAST SCA application security testing according to the Polaris user guide;
- Synopsys will conduct an automated source code analysis and automated software composition analysis assessment leveraging the customer supplied source code;
- Synopsys will perform one-time results review audit of the fAST Static assessment findings for each initial assessed project to identify false positives;
- All subsequent requests for both fAST Static and fAST SCA will be delivered as an automated scan; and
- Polaris Application Security test results are delivered to customer via Polaris' portal.

POLARIS-SAAS SCA APPLICATION TESTING SUBSCRIPTION – AUTOMATED

The Polaris fAST SCA subscription offering is based on a twelve (12) month consecutive period ("Subscription Term") and based on the following guidelines:

- A defined Application for the Subscription Term;
- Customer may create up to five (5) supporting projects for the defined Application;
- Customer may utilize an unlimited number of single assessments during the Subscription Term which are allocated to the defined Application;
- Customer to submit the source code payload to the Polaris platform for fAST SCA testing according to the Polaris user guide;
- Synopsys will conduct an automated software composition analysis assessment on the customer supplied source code;
- Customer may utilize an unlimited number of single assessments during the Subscription Term which may be allocated to the defined Project; and
- Polaris Application Security test results are delivered to customer via Polaris's portal.

SERVICE ASSUMPTIONS

- For Polaris fAST Static and/or fAST SCA, an Application may include up to five (5) Projects and, regardless of number of Projects, in total, a single Application shall not exceed 1M lines of code.
- Upon initiation of the first assessment, the Project source code may not be changed for the term of the Subscription Period. Any updates to Project source code must be a derivative of the original Project source code which was assessed during the first assessment.
- Any source code submitted by the customer must meet the minimum requirements as published by Coverity Static Application Security Testing ("SAST") and/or Blackduck Software Composition Analysis ("SCA") language support guidelines.
- Upon initial tenant creation, all organization administration will be performed by the customer.
- The Synopsys support staff provides coverage path for any issues with the Polaris offering. Synopsys will provide coverage via phone, email and, Synopsys Community and will maintain service level objectives with published resolution times.

- For any Application under subscription, only one (1) single test may be active per project, per test type at any one time.
- All Polaris SaaS services, or types described are subject to the following security controls: https://www.synopsys.com/company/legal/software-integrity/security-commitments.html
- All Polaris SIG support services described are subject to the following terms and conditions, which are incorporated herein by reference (registration for a community account is not required for Polaris customers): https://www.synopsys.com/content/dam/synopsys/sig-assets/guides/synopsys-sig-support-guide.pdf
- All Polaris SIG services and deliverables will be delivered in English.

SERVICE LEVEL OBJECTIVES

Service Level Objectives	Description of Service Level
Triage Activity Response Times	For fAST Static tests, scan issue triage for any project will be delivered in up to three (3) business days.
Polaris Platform Availability	Polaris will make all Services and Content available to customer at 99.95% platform availability per month.

POLARIS SERVICE OUTCOME

Upon completion of the vulnerability assessment, the customer may access a detailed report with the discovered vulnerability findings. The results of the assessment will be available via an automated process once all analysis processes have been fully completed. The return time of the results is dependent on the size of the Application. Increased return times may be required as the submitted size of the payload increases. The following information is available for each discovered vulnerability:

fAST Static - Static Application Security Testing

- Issue Type
- Issue Description
- Issue Severity
- Engine Type
- Assessment Date and Time
- Contributing Code Event

fAST SCA - Software Composition Analysis

- Issue Type
- Issue Description
- Issue Severity
- Engine Type
- Assessment Date and Time

POLARIS PLATFORM SECURITY CONTROLS

Polaris brings the power of the Synopsys Software Integrity (“SIG”) products and managed services together into an integrated, easy-to-use solution that enables security and development teams to build secure, high-quality software faster. Polaris is delivered as a multi-tenant, cloud-based solution with a user-friendly web interface for managing projects and analyzing results.

As an organization dedicated to protecting and securing our customers’ applications, (SIG) is equally committed to our customers’ data security and privacy.

DATA CENTER SECURITY

The Polaris platform leverages the Google Cloud Platform (“GCP”) to take advantage of the highest standards for security, compliance, and availability for multiple regions of the globe. For additional information on the GCP platform security, infrastructure, privacy, or compliance, please refer to:

https://cloud.google.com/security

Our data centers are protected with several layers of security to prevent any unauthorized access of your data. We use secure perimeter defense systems, comprehensive camera coverage, biometric authentication, and a 24/7 guard staff.

Polaris is physically housed in a Tier 4 A+ datacenter featuring multiple redundant power and network feeds and “five-nines” uptime. The datacenter is compliant with SAS 70 Type II/SSAE 16 Type II, ITIL V2 Services Manager, and ITIL V3 Foundation Certifications. The datacenter has 24x7x365 security utilizing CCTV. All datacenter employees are background checked. All physical data center access is supervised , and all doors require PIN, magnetic card, and biometric retina scans before granting access. The data centers has redundant power systems with backup generators and double-conversion UPS.

SOFTWARE SECURITY

Polaris was designed and developed from the ground up using industry best practices throughout the Secure Development Lifecycle. This includes, but is not limited to, the following:

- Comprehensive architecture and threat model review
- Defined secure software development process
- Automated and Manual security testing
- Data flow diagram
- System, Network, and Application Security procedures
- Compliance with ISO 27001 and SOC 2, Type 2

DISASTER RECOVERY AND BUSINESS CONTINUITY

Disaster Recovery (“DR”) and Business Continuity (“BC”) are at the core of all Synopsys Information Technology operations. All DR and BC documents are managed internally by the Synopsys operations team. Should an entire regional datacenter fail due to physical or logical disaster, procedures documented in the Disaster Recovery Plan for the specified region is implemented. At a high level, this plan outlines the location of all data backups along with key personnel required to access and perform a full restoration. This process is owned by the Synopsys Director of Operations. During the time between

the loss of the Synopsys online service and the restoration of service the Customer Account Manager will enact the communication process to the customer base with updates to the recovery process.

- Recovery Point Objective (RPO): 24 Hours
- Recovery Time Objective (RTO): 8 Hours

Any event which poses a disruption to business as normal must be reported through the Synopsys response team.

DATA STORAGE AND PRIVACY

Synopsys takes every necessary precaution to protect our customers' data. Synopsys has browser-to-system SSL encryption. All data, including intellectual property and analysis results, are encrypted with data-at-rest encryption technologies. Only duly authorized Synopsys personnel have direct access to customer data. A customer is provided the ability to delete all historical tenant-level data which includes all data / historical results, from the Polaris platform.

ACCESS CONTROL / MANAGEMENT

Multi-factor authentication (MFA) capability is provided to customers for accessing SIG applications.

- Access to Synopsys Information, Synopsys Information Assets, Information Systems, and Synopsys Networks are unauthorized unless expressly approved by Synopsys.
- Synopsys designates the responsibility for authorizing system access to Synopsys Information, Synopsys Information Assets, Synopsys Information Systems, as well as Synopsys Network and operating services to assigned Asset Owners and Data Owners.
- Asset Owners and Data Owners must authorize access to Synopsys Information and Synopsys Information Assets according to valid business requirements.
- Access authorizations must limit system access, accounting for Least Access Privilege Principles and the sensitivity levels of Synopsys Information
- Wherever feasible, Asset Owners and Data Owners shall define access authorizations to align with functional workgroups or roles, such as Role Based Access Control (RBAC).
- Access authorizations shall also account for any legal or contractual restrictions for limiting access to Synopsys Information or services.

SYSTEM ARCHITECTURE

The Polaris system architecture includes multiple layers of security including, but not limited to up-to-date encryption technologies and access control. All access to the system uses secure connectivity, allowing authorized personnel only, with the highest level of encryption for all users to access the environment. This includes:

- Required two-factor authentication
- Access permitted only from predefined locations - Access is denied from unauthorized locations
- Encrypted Ethernet between servers using a minimum of 128-bit encryption
- All private decryption keys stored off site and at a separate site than the data

COMMITTED AVAILABILITY

Polaris provides the following uptime commitment for customers. Polaris will (a) make all Services and Content available to customer at 99.95% availability per month, (b) use commercially reasonable efforts to make Polaris Services available 24 hours a day, 7 days a week apart from: (i) scheduled downtime, and (ii) any force majeure events including, but not limited to Internet service provider failure or delay, Non-Polaris Applications or services, or denial of service attack.

INCIDENT RESPONSE

The Synopsys Information Security defines, maintains, and communicates all security incidents as a part of the Security Incident Response Plan. The information security team will continuously evaluate and address information security events and Information Security Incidents in a timely, effective, and orderly manner.

SECURE SOFTWARE DEVELOPMENT LIFECYCLE

For all Synopsys software assets, the strongest security processes and controls are required and built on two pillars:

- Core Security Requirements
- Product Security Requirements

Given Synopsys leadership in the world of software security, it is imperative that Synopsys internal development efforts not only meet but also exceed the standards used by other security-minded development groups. What follows below is a high-level overview of the various areas that are covered in depth within the detailed standards for:

- Information Gathering and Threat Modeling
- Infrastructure Security
- Data Classification
- Configuration and Deployment Management Security
- Identity Management Security
- Authentication Security
- Authorization Security
- Access Controls
- Session Management Security
- Input Validation and Output Encoding
- Logging and Error Handling
- Encryption of Sensitive Data (Transit and Rest)
- Business Logic Security
- Client-side Security
- API Security