A-LIGN

A-LIGN.com

Type 2 SOC 3

Prepared for:
Black Duck Software Inc.

Year:
2026

BLACKDUCK®

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

May 1, 2025 to April 30, 2026

Table of Contents

SECTION 1

ASSERTION OF BLACK DUCK SOFTWARE INC. MANAGEMENT

ASSERTION OF BLACK DUCK SOFTWARE INC. MANAGEMENT

May 12, 2026

We are responsible for designing, implementing, operating, and maintaining effective controls within Black Duck Software Inc.'s ('Black Duck' or 'the Company') Polaris Platform, Continuous Dynamic and Black Duck Software Composition Analysis Services System throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Black Duck's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Black Duck Software Inc.'s Description of Its Polaris Platform, Continuous Dynamic and Black Duck Software Composition Analysis Services System throughout the period May 1, 2025 to April 30, 2026" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Black Duck's service commitments and system requirements were achieved based on the trust services criteria. Black Duck's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Black Duck Software Inc.'s Description of Its Polaris Platform, Continuous Dynamic and Black Duck Software Composition Analysis Services System throughout the period May 1, 2025 to April 30, 2026."

Black Duck uses Amazon Web Services ('AWS') and Google Cloud Platform ('GCP') to provide cloud hosting services, and CenterSquare to provide colocation services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Black Duck, to achieve Black Duck's service commitments and system requirements based on the applicable trust services criteria. The description presents Black Duck's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Black Duck's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Black Duck's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Black Duck's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period May 1, 2025 to April 30, 2026 to provide reasonable assurance that Black Duck's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Black Duck's controls operated effectively throughout that period.

Ronald Lewis
Head of Cybersecurity Governance
Black Duck Software Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Black Duck Software Inc.:

Scope

We have examined Black Duck Software Inc.'s ('Black Duck' or 'the Company') accompanying assertion titled "Assertion of Black Duck Software Inc. Management" (assertion) that the controls within Black Duck's Polaris Platform, Continuous Dynamic and Black Duck Software Composition Analysis Services System were effective throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Black Duck's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Black Duck uses AWS and GCP to provide cloud hosting services, and CenterSquare to provide colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Black Duck, to achieve Black Duck's service commitments and system requirements based on the applicable trust services criteria. The description presents Black Duck's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Black Duck's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Black Duck, to achieve Black Duck's service commitments and system requirements based on the applicable trust services criteria. The description presents Black Duck's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Black Duck's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Black Duck is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Black Duck's service commitments and system requirements were achieved. Black Duck has also provided the accompanying assertion (Black Duck assertion) about the effectiveness of controls within the system. When preparing its assertion, Black Duck is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements

- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Black Duck's Polaris Platform, Continuous Dynamic and Black Duck Software Composition Analysis Services System were suitably designed and operating effectively throughout the period May 1, 2025 to April 30, 2026, to provide reasonable assurance that Black Duck's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Black Duck's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Black Duck's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Black Duck, user entities of Black Duck's Polaris Platform, Continuous Dynamic and Black Duck Software Composition Analysis Services System during some or all of the period May 1, 2025 to April 30, 2026, business partners of Black Duck subject to risks arising from interactions with the Polaris Platform, Continuous Dynamic and Black Duck Software Composition Analysis Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
May 12, 2026

SECTION 3

BLACK DUCK SOFTWARE INC.'S DESCRIPTION OF ITS POLARIS PLATFORM, CONTINUOUS DYNAMIC AND BLACK DUCK SOFTWARE COMPOSITION ANALYSIS SERVICES SYSTEM THROUGHOUT THE PERIOD MAY 1, 2025 TO APRIL 30, 2026

OVERVIEW OF OPERATIONS

Company Background

Black Duck Software, Inc. is the market leader in application security testing (AST). With the most comprehensive, powerful, and trusted portfolio of application security (AppSec) solutions in the industry, they help organizations worldwide build trust in their software.

Description of Services Provided

Black Duck provides software tools and services to improve the security and quality of its customers' software applications. Black Duck provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to find and fix vulnerabilities and defects in proprietary code, open-source components, and application behavior. With a combination of tools, services, and expertise, Black Duck helps organizations optimize security and quality in development, security, and operations and throughout the software development life cycle.

The Black Duck Software as a Service (SaaS) offerings include Black Duck, Polaris, and Continuous Dynamic. Black Duck is a software composition analysis tool that assesses an application's open-source constituents and analyzes them for security defects and license compliance. Polaris is a cloud platform designed to integrate a broad variety of application security tools and provide a single "pane of glass" across a variety of application-testing technologies. Static analysis is provided through Coverity. Software composition analysis is provided through Open-Source Security Tools and Risk Analysis (OSRA). Continuous Dynamic is a SaaS dynamic application security testing (DAST) solution that allows customer business to quickly deploy a scalable web security program.

The system description in this section of the report details the Black Duck SaaS offerings. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organizations).

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Black Duck SaaS offerings. Commitments are communicated in end-user license agreements, security commitments, data privacy and protection statement, and master service agreements, which can be found on the Company's security web page.

System requirements are specifications regarding how the Black Duck SaaS offerings should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the Black Duck SaaS offerings include the following:

Trust Services Category	Service Commitments	System Requirements
Security	The Company will maintain best-practice technical and organizational security measures to protect against such risks as accidental or unlawful destruction, loss, or alteration of data and unauthorized disclosure or access.	• Change Management • Incident Management • Risk Management • Configuration Management • Log Management • Vendor Management • Annual Security Assessment • Vulnerability Management • Access Management
Availability	The Company will back up customer data daily with a 7-day retention policy.	• Daily Backup and Restore Procedures • Business Continuity and Disaster Recovery Plans
	The Company will maintain a recovery time objective (RTO) of one (1) business day and a recovery point objective (RPO) of 24 hours.	
Confidentiality	The Company will disclose confidential information only to those who need to know in order to provide the services.	• Data Classification • Retention and Destruction Standards • Data Handling Standards • Data Encryption in Transit and at Rest
	Upon termination, the Company will return or destroy customer's confidential information.	
	The Company will keep customer data encrypted in transit and at rest.	

Components of the System

Infrastructure

Primary infrastructure used to provide Black Duck's Polaris Platform, Continuous Dynamic and Black Duck Software Composition Analysis Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
MySQL / PostgreSQL / MongoDB / Eventstore / Kafka / Hadoop	Databases	CentOS Linux / Debian Linux / Alpine Linux / Ubuntu Linux
Google Transmission Control Protocol (TCP) Load Balancing (LB) / Google L7 LB / Elastic LB / Nginx / F5 BigIP	Load Balancer	Solutions specific

Software

Primary software used to provide Black Duck's Polaris Platform, Continuous Dynamic and Black Duck Software Composition Analysis Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Datadog	Application monitoring / infrastructure monitoring	Datadog
Velero / GCP / AWS	Backup and replication	Velero / GCP / AWS
Stackdriver	Logging system	Stackdriver
Okta	Single sign-on	Okta
Prisma Cloud	Information technology (IT) asset management	Prisma Cloud
Prometheus / Zabbix	Infrastructure monitoring	Prometheus / Zabbix
Coverity	Static Analysis	Coverity
Prisma Cloud Compute (Twistlock)	File integrity monitoring / anti-malware / intrusion detection	Prisma Cloud Compute (Twistlock)
Jira / ZenDesk	Help desk / ticketing system	Jira & Service Now
Cloudflare	Web Application Firewall	Cloudflare
JAMF	Mobile Device Management	JAMF
Zscaler	Web Filter Proxy	Zscaler
SumoLogic / ReliaQuest	SIEM & SOC	SumoLogic / Zyston
Microsoft Purview	Data Leakage Prevention	Microsoft Purview
Knowbe4	Security Awareness Training	Knowbe4

For Continuous Dynamic:

Software	
Production Application	**Business Function**
Pgdump / S3 Sync	Backup and replication
Okta	Single sign-on / Identity and Access management
Ansible / DNS / Spreadsheet	IT asset management
Coverity	Static Analysis
CrowdStrike / Prisma Cloud Compute (Twistlock)	FIM / anti-malware / intrusion detection system (IDS)
Jira / ZenDesk	Help desk, ticketing system
PGBadger	Database query monitoring
Tableau	Business Analytics

Software	
Production Application	**Business Function**
Jenkins	Continuous deployment / manages repeating chronological tasks
Self-managed RabbitMQ	Managed RabbitMQ
Memcached	Cache
Nexus, Apt	Package management tool
Ansible Vault / AWS Key Management System (KMS) / Keeper	Secrets store
PGBouncer	PostgreSQL proxy
AWS Suite	Cloud Provider
BIND / InfoBlox	Domain Name System (DNS) / Web-Application Firewall (WAF)

People

The Company develops, manages, and secures the Black Duck SaaS offerings via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Information Security Management System (ISMS) Management Committee Body	• Provides the ISMS Program with operational and tactical direction, strategic alignment, and guidance as the Company encounters both successes and issues
Business Operations	• Oversees Company business operations and legal or regulatory compliance abidance • Business Operations Director participates in the ISMS Management Committee as a member
Cloud Operations	• Oversees and manages Company application programming interfaces (APIs), SaaS services, database storage, OSs and Virtual Machines (VMs), and internal and external firewalls protecting production systems and services • Coordinates with Company IT to manage vulnerabilities and conduct operational change management • Cloud Operations Manager participates in the ISMS Management Committee as a member
IT	• Oversees and manages user access management, network services, and projects and provides core IT services to internal customers • Coordinates with Cloud Operations to manage vulnerabilities and conduct operational change management • IT Director participates in the ISMS Management Committee as a member

People	
Group/Role Name	**Function**
Cybersecurity Organization	• Secures the Company's software products and professional service offerings • Cybersecurity Org Leader participates in the ISMS Management Committee as a chair

The following organization chart reflects the Company's internal structure related to the groups discussed above:

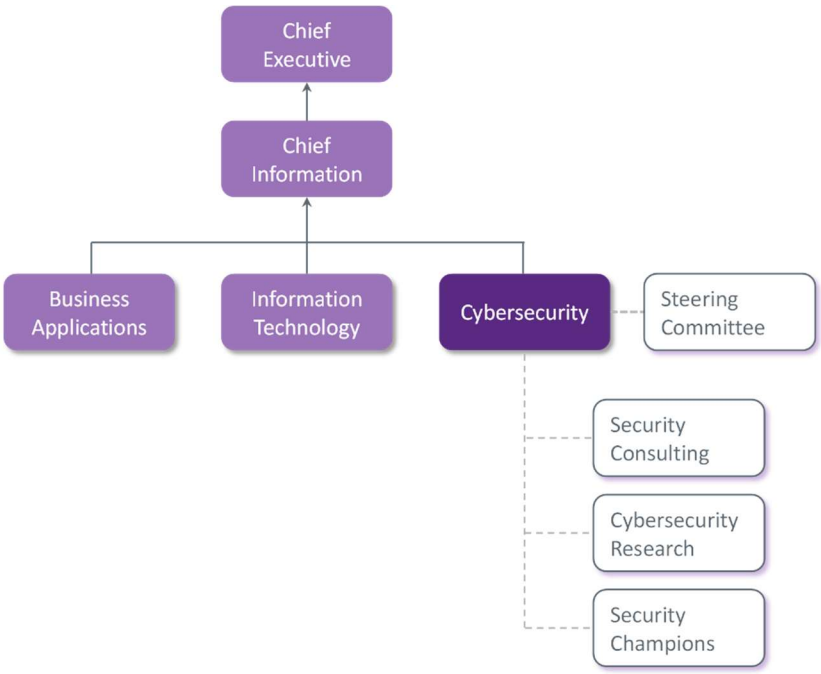

Figure 1: Black Duck Organization Chart

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the API, the customer or end user defines and controls the data they load into and store in the Black Duck SaaS offerings' production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for the transmission of confidential or sensitive information over public networks. Encryption is enabled for databases housing sensitive customer data.

The following table details the types of data contained in the production application for the Black Duck SaaS offerings:

Data		
Production Application	**Description**	**Data Store**
Polaris	• User credentials • Source code • Static analysis security assessment results	GCP / PostgreSQL / Eventstore
Black Duck	• User credentials • Source code snippets • Software composition security assessment results • Software license compliance results	GCP / PostgreSQL

Continuous Dynamic	• User credentials
	• For dynamic analysis customers:
	  ○ Web site configuration, optionally with login credentials
	  ○ Dynamic analysis security assessment results
	• For API analysis customers:
	  ○ API documentation
	  ○ API security assessment results
		PostgreSQL / NFS

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to Black Duck policies and procedures that define how services should be delivered. These are located on the Company's Intranet and can be accessed by any Black Duck team member.

Physical Security

AWS, GCP, and CenterSquare are collectively responsible for monitoring and managing the supporting infrastructure that supports the Polaris Platform, White Hat Dynamic and Black Duck Software Services. As such, all physical and environmental controls are the responsibility of AWS, GCP, and CenterSquare.

Logical Access

Black Duck uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, Black Duck implements monitoring of one or more of the responsibilities. Monitoring is performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

Resources are managed in the asset inventory system and each asset is assigned to an owner. Owners are responsible for approving access to the resource and for performing annual reviews of access by role.

Employees and approved vendor personnel sign on to the Black Duck network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the Black Duck network are required to use a token-based multifactor authentication (MFA) system. Employees are issued tokens upon employment and return the token during their exit interview. Vendor personnel are not permitted to access the system from outside the Black Duck network.

Customer employees' access Black Duck services through the Internet using the Secure Socket Layer (SSL) functionality of their web-browser. These customer employees supply a valid user ID and password to gain access to customer cloud resources. Passwords conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with Black Duck configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Customer employees may sign on to their systems using virtual server administration accounts. These administration accounts use a digital certificate-based MFA system.

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees' start date, the HR management system creates a report of employee user IDs to be created and access to be granted. The report is used by the security help desk to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the Chief Information Security Officer. As part of this process, the Chief Information Security Officer reviews access by privileged roles and requests modifications based on this review.

The HR system generates a list of terminated employees on a daily basis. This daily report is used by the security help desk to delete employee access. On an annual basis, HR runs a list of active employees. The security help desk uses this list to suspend user IDs and delete access roles from IDs belonging to terminated employees.

On a quarterly basis, managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the security help desk for processing. The security help desk manager identifies any records not returned within two weeks and follows up with the manager. As part of this process, the Chief Information Security Officer reviews employees with access to privileged roles and requests modifications through the event management system.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Backup is stored in cloud environment managed by CSP. The backup infrastructure resides on private networks logically secured from other networks.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to IT incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Black Duck monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Black Duck evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Cloud storage
- Network bandwidth

Black Duck has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Black Duck system owners review proposed operating system patches to determine whether the patches are applied. Customers and Black Duck systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Black Duck staff validate that patches have been installed and if applicable that reboots have been completed.

Change Control

Black Duck maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Black Duck has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Black Duck system owners review proposed operating system patches to determine whether the patches are applied. Customers and Black Duck systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Black Duck staff validate that patches have been installed and if applicable that reboots have been completed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal Internet Protocol (IP) addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Black Duck. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed internally by the Cybersecurity team on a daily basis in accordance with Black Duck policy. The Cybersecurity team uses industry standard scanning technologies and a formal methodology specified by Black Duck. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Black Duck system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through from the Internet through the use of leading Virtual Private Network (VPN) technology. Employees are authenticated through the use of a token-based MFA system.

Boundaries of the System

The scope of this report includes the Polaris Platform, Continuous Dynamic and Black Duck Software Composition Analysis Services System performed in the Burlington, Massachusetts facility.

This report does not include the cloud hosting services provided by AWS and GCP, and the colocation services provided by CenterSquare at multiple facilities.

Changes to the System in the Last 6 Months

No significant changes have occurred to the services provided to user entities in the 6 months preceding the review date.

Incidents in the Last 6 Months

No significant incidents have occurred to the services provided to user entities in the 6 months preceding the review date.

Criteria Not Applicable to the System

All Common Criteria/Security, Availability, and Confidentiality criterion were applicable to the Polaris Platform, Continuous Dynamic and Black Duck Software Composition Analysis Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS and GCP, and the colocation services provided by CenterSquare at multiple facilities.

Subservice Description of Services

Black Duck uses AWS and GCP as subservice organizations for cloud hosting services and CenterSquare for colocation services. Black Duck' controls related to the Black Duck SaaS offerings cover only a portion of the overall internal control for each user entity of the Black Duck SaaS offerings.

AWS, GCP, and CenterSquare are responsible for physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS, GCP, and CenterSquare's physical security controls mitigate the risk of unauthorized access to the hosting facilities. AWS, GCP, and CenterSquare's environmental protection controls mitigate the risk of fires, power loss, climate, and temperature variabilities. GCP also provides security monitoring services as part of its Platform-as-a-Service offering. GCP security monitoring services mitigate the risk of unauthorized logical access.

Black Duck management receive and review the AWS, GCP, and CenterSquare SOC 2 reports annually. In addition, through its operational activities, Black Duck management monitor the services performed by AWS, GCP, and CenterSquare to determine whether operations and controls expected to be implemented are functioning effectively. Management also has communication with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS, GCP, and CenterSquare management.

Complementary Subservice Organization Controls

Black Duck' services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all the trust services criteria related to Black Duck' services to be solely achieved by Black Duck control procedures. Accordingly, the subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Black Duck.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible power supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

The following subservice organization controls should be implemented by GCP to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	User access lists to data center server areas are reviewed on a quarterly basis and inappropriate access is removed in a timely manner.
		All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.
		Visitors must be signed in by an employee before a single-day paper visitor badge that authorizes them can be issued.
		Annual data center security reviews are performed, and results are reviewed by executive management.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
		Physical security measures in place include: • Existence of security guards, access badges, and video cameras to secure the data centers is reviewed during the annual data center security reviews • Data center entrances have a perimeter security system consisting of badge readers or biometric access system • Data centers utilize a badge reader or biometric access controls to restrict access to raised floor spaces and lock/keys to restrict access to facilities rooms within the building • All emergency exit points from the raised floor are alarmed • Badge reader and biometric access control systems are secured in a restricted space and no physical access to them from public spaces exists • Visitors to the datacenter facilities must gain appropriate approval, sign in at the front, and remain with an escort during the duration of their visit • Video cameras exist to monitor building entrances, exits, and the areas immediately surrounding the building • At least one security guard is on-site 24x7 • All staff members are required to either sign in or badge in to gain access to the facility and a no tailgating policy is in place • All Google cages, suites, and private rooms are secured using either lock/key, badge access control, or biometric access controls • A key sign out sheet and/or log of badge reader activity exists and covers access to Google spaces
Availability	A1.2	Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
		All data centers are equipped with fire detection alarms and protection equipment. Data center server floors and network rooms are connected to an UPS system and emergency generator power is available in the event of a loss of power. Google protects the information system from damage resulting from water leakage by providing shutoff valves that are accessible, working properly and known to key personnel.

The following subservice organization controls should be implemented by CenterSquare to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - CenterSquare		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	User access lists to data center server areas are reviewed on a quarterly basis and inappropriate access is removed in a timely manner.
		All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.
		Visitors must be signed in by an employee before a single-day paper visitor badge that authorizes them can be issued.
		Annual data center security reviews are performed, and results are reviewed by executive management.
		Physical security measures in place include: • Existence of security guards, access badges, and video cameras to secure the data centers is reviewed during the annual data center security reviews • Data center entrances have a perimeter security system consisting of badge readers or biometric access system • Data centers utilize a badge reader or biometric access controls to restrict access to raised floor spaces and lock/keys to restrict access to facilities rooms within the building • All emergency exit points from the raised floor are alarmed • Badge reader and biometric access control systems are secured in a restricted space and no physical access to them from public spaces exists • Visitors to the datacenter facilities must gain appropriate approval, sign in at the front, and remain with an escort during the duration of their visit • Video cameras exist to monitor building entrances, exits, and the areas immediately surrounding the building • At least one security guard is on-site 24x7 • All staff members are required to either sign in or badge in to gain access to the facility and a no tailgating policy is in place • All Google cages, suites, and private rooms are secured using either lock/key, badge access control, or biometric access controls • A key sign out sheet and/or log of badge reader activity exists and covers access to Google spaces
Availability	A1.2	Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).

Subservice Organization - CenterSquare		
Category	**Criteria**	**Control**
		All data centers are equipped with fire detection alarms and protection equipment. Data center server floors and network rooms are connected to an UPS system and emergency generator power is available in the event of a loss of power. Google protects the information system from damage resulting from water leakage by providing shutoff valves that are accessible, working properly and known to key personnel.

COMPLEMENTARY USER ENTITY CONTROLS

Black Duck' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Black Duck' services to be solely achieved by Black Duck control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Black Duck'.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Criteria	Complementary User Entity Controls (CUECs)
CC2.1	User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames. Controls to provide reasonable assurance that the Company is notified of changes in: • User entity vendor security requirements • The authorized users list
CC2.3	It is the responsibility of the user entity to have policies and procedures to: • Inform their employees and users that their information or data is being used and stored by the Company • Determine how to file inquiries, complaints, and disputes to be passed on to the Company
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel
CC6.4 CC6.5 CC7.2 A1.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity
CC6.6	• Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company