Service Organization Controls (SOC) 3 Report

For the Period of January 01, 2025 to December 31, 2025

Report on the JFrog Artifactory, JFrog Curation, JFrog Security Essentials (Xray), JFrog Advanced Security (JAS), JFrog Distribution, JFrog Runtime, JFrog AppTrust, JFrog ML and JFrog Connect

Relevant to Security, Availability, Confidentiality, and Privacy

Table of Contents

Section I – Management's Report of its Assertions on the Effectiveness of Its Controls over the JFrog Artifactory, JFrog Security Essentials (Xray) JFrog Enterprise Plus, JFrog Connect, JFrog Distribution, JFrog Advanced Security (JAS), JFrog Curation, JFrog Runtime, JFrog ML and JFrog AppTrust Based on the Trust Services Criteria for Security, Availability, Confidentiality and Privacy

February 26, 2026

We, as management of, JFrog Ltd. are responsible for:

- Identifying the JFrog Artifactory, JFrog Curation, JFrog Security Essentials (Xray), JFrog Advanced Security (JAS), JFrog Distribution, JFrog Runtime, JFrog AppTrust, JFrog ML and JFrog Connect (System) and describing the boundaries of the System, which are presented in Attachment A.
- Identifying our service commitments and system requirements.
- Identifying the risks that would threaten the achievement of our service commitments and system requirements that are the objectives of our System, which are presented in Attachment B.
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirement.
- Selecting the trust services categories and associated criteria that are the basis of our assertion.

JFrog Ltd. uses Amazon Web Services ('AWS'), Google Cloud Platform ('GCP') and Microsoft Azure to provide infrastructure management services. The description of the boundaries of the system presented in Attachment A indicates that complementary controls at AWS, GCP and Microsoft Azure that are suitably designed and operating effectively are necessary, along with controls at JFrog Ltd. to achieve the service commitments and system requirements. The description of the boundaries of the system presents the types of complementary subservice organizations controls assumed in the design of JFrog Ltd.'s controls. It does not disclose the actual controls at AWS, GCP and Microsoft Azure.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period January 01, 2025 to December 31, 2025, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy (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.*

Very truly yours,
JFrog Ltd. Management

Aran AzarzarCIO

Aran Azarzar

Section II – Independent service auditor's report

To the Management of JFrog Ltd.

Scope

We have examined management's assertion, contained within the accompanying Management's Report of its Assertions on the Effectiveness of Its Controls over the JFrog Artifactory, JFrog Curation, JFrog Security Essentials (Xray), JFrog Advanced Security (JAS), JFrog Distribution, JFrog Runtime, JFrog AppTrust, JFrog ML and JFrog Connect Based on the Trust Services Criteria for Security, Availability, Confidentiality and Privacy (Assertion), that JFrog Ltd.'s controls over the JFrog Artifactory, JFrog Curation, JFrog Security Essentials (Xray), JFrog Advanced Security (JAS), JFrog Distribution, JFrog Runtime, JFrog AppTrust, JFrog ML and JFrog Connect (System) were effective throughout the period January 01, 2025 to December 31, 2025, to provide reasonable assurance that JFrog Ltd.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy (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*.

JFrog Ltd. uses AWS, GCP and Microsoft Azure (subservice organization) to provide infrastructure management services. The description of the boundaries of the system presented at Appendix A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at JFrog Ltd., to provide reasonable assurance that JFrog Ltd.'s service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS, GCP and Microsoft Azure. Our procedures did not extend to the services provided by AWS, GCP and Microsoft Azure and we have not evaluated whether the controls management assumes have been implemented at AWS, GCP and Microsoft Azure have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 01, 2025 to December 31, 2025.

Management's responsibilities

JFrog Ltd.'s management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that JFrog Ltd.'s service commitments and system requirements were achieved. JFrog Ltd. management is also responsible for providing the accompanying assertion about the effectiveness of controls within the System, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System.
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the service commitments and service requirements that are the objectives of the System.

Our responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("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. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of JFrog Ltd.'s relevant Security, Availability, Confidentiality and Privacy policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating JFrog Ltd.'s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program**.**

Our examination was not conducted for the purpose of evaluating the performance or integrity of JFrog Ltd.'s AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of JFrog Ltd.'s AI services.

We are required to be independent of JFrog Ltd. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve JFrog Ltd.'s service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, JFrog Ltd.'s controls over the System were effective throughout the period January 01, 2025 to December 31, 2025, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted use

This report is intended solely for the information and use of JFrog Ltd. and user entities of JFrog Ltd.'s JFrog Artifactory, JFrog Curation, JFrog Security Essentials (Xray), JFrog Advanced Security (JAS), JFrog Distribution, JFrog Runtime, JFrog AppTrust, JFrog ML and JFrog Connect system and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators and is not intended to be, and should not be, used by anyone other than these specified parties.

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global Limited

Kost Forer Gabbay and Kasierer

February 26, 2026
Tel-Aviv, Israel

Attachment A – Description of the JFrog's platform, including JFrog Artifactory, JFrog Curation, JFrog Security Essentials (Xray), JFrog Advanced Security (JAS), JFrog Distribution, JFrog Runtime, JFrog AppTrust, JFrog ML and JFrog Connect

JFrog Overview and Background

JFrog is on a mission to enable continuous updates through Liquid Software, empowering developers to code applications that securely flow to end-users. JFrog is the creator of Artifactory, the heart of the end-to-end universal platform for automating, managing, securing, distributing, and monitoring all types of binaries. The JFrog platform is available as an open-source offering, an on-premises offering, and as a cloud offering.

JFrog Ltd. is an Israeli company publicly traded on NASDAQ, with co-headquarters in Sunnyvale, California and Netanya, Israel (JFrog and its subsidiaries, hereinafter, JFrog). The company focuses on enabling what it terms "Liquid Software," referring to the continuous and secure movement of software from development to production. The end-to-end, hybrid JFrog Platform provides tools and visibility designed to support the needs of modern software development organizations adopting DevOps practices. JFrog's products are used by organizations seeking to support digital transformation initiatives and to enhance software-driven customer interaction.

Products and Services

JFrog Platform is a unified, hybrid, and multi-cloud DevOps solution designed to manage the entire software supply chain, from development to distribution. It acts as a single pane of glass for storing, securing, and deploying software packages, binaries, and container images, providing end-to-end traceability and automation for DevSecOps, MLOps, and IoT workflows. This is an integrated, end-to-end Software Supply Chain platform designed to manage, secure, and automate the lifecycle of software binaries and artifacts. As a "Single System of Record," the platform provides a centralized hub for DevOps, DevSecOps, and MLOps teams to orchestrate software releases from development to production across hybrid and multi-cloud environments.

The Platform delivers its capabilities through the following deeply integrated products:

JFrog Artifactory is an enterprise-grade repository manager designed to store, manage, and control binaries throughout the entire software release life cycle. It addresses the critical needs of software development and DevOps teams by enabling seamless management, hosting, and secure control over the flow of binary artifacts from development to production. Artifactory fully supports software packages from virtually any language or technology, and provides secure, clustered, high-availability Docker registries.
Artifactory's deep integration with all major CI/CD and DevOps tools delivers an automated and reliable solution for tracking artifacts from development through to production.
Mission Control, previously available as a standalone product, is now an integral microservice within JFrog Artifactory.

JFrog Curation defends a user's software supply chain, enabling early blocking of malicious or risky open-source packages before they even enter. JFrog Curation seamlessly identifies harmful, vulnerable, or risky packages, ensuring increased security, compliance, and developer productivity. JFrog Curation is a gatekeeping layer that blocks malicious or non-compliant open-source components before they enter the internal ecosystem.

JFrog Security Essentials (Xray) is a universal software composition analysis (SCA) solution that natively integrates with Artifactory to give developers and DevSecOps teams an easy way to scan binaries. Proactively identifies vulnerabilities in source code and license compliance violations before the manifest in production releases, offering unique application security value. JFrog Xray continuously scans the JFrog Platform to secure all packages stored at a binary level and helps to achieve control and trust earlier in software release cycles by automating security workflows as part of the JFrog CI/CD pipeline.

JFrog Advanced Security (JAS) is based on deep security research by JFrog's Security Research team that delivers extended insights into security issues, their impact on the software, and advice on how to remediate them. Helps sharpen developers with prioritized, contextual remediation advice that identifies what matters most to ensure protection. JFrog Xray previously released a powerful capability, the JFrog Security CVE Research and Enrichment feature, which helps to enhanced analysis of CVE findings in a way that allows to focus on the most important issues with the capability of finding the best resources invested in fixing them.

JFrog Distribution enables platform users to speed up deployments and concurrent downloads at scale throughout a user's SDLC process. From CI to CD through device management, spanning remote sites, hybrid infrastructure, clouds, edges, embedded devices, and IoT fleets, JFrog Distribution provides a vital development tool for managing trusted software releases across the globe. JFrog Distribution is a secure tool for orchestrating the delivery of immutable release bundles to various consumption points at scale.

JFrog Runtime enables Security and DevOps teams to monitor Kubernetes clusters in real time, identify, prioritize, and remediate security incidents based on actual risk, verify image integrity, and meet compliance requirements.

JFrog AppTrust provides end-to-end governance for the software supply chain by aggregating signed and verifiable release evidence from development and security tools and applying configurable policy controls at each stage of delivery. By establishing control gates and producing auditable release records, AppTrust helps ensure that only approved, validated versions are deployed as trusted releases.

JFrog ML provides a unified platform for AI/ML development by integrating essential tools, environments, and ready-to-use solutions tailored for efficient and reliable machine learning workflows. The platform enables Data Scientists, ML Engineers, and AI Developers to move models into production seamlessly, applying DevOps best practices throughout the AI/ML lifecycle. Key capabilities include: model training, deployment, and monitoring; fine-tuning or building models from scratch; developing LLM-based applications and prompt engineering; and comprehensive feature lifecycle management.

JFrog Connect, an integral part of the JFrog Platform, provides a unified, enterprise-grade solution for securing and managing the entire IoT development lifecycle, from developer to device. It simplifies software deployment to IoT and edge device fleets, offering native integration with JFrog Artifactory for trusted artifact management and JFrog Security for comprehensive vulnerability scanning. Connect's core capability is the automation of secure Over-The-Air (OTA) updates to thousands of devices running Linux, complete with configurable rollback mechanisms. The platform also includes robust features for continuous monitoring, fleet management (tagging, project organization), and remote access tools (Terminal, Port Tunnel) for efficient diagnosis and control.

Subservice Organizations Carve-Out Controls: Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure

JFrog has contracted with Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure for Infrastructure as a Service (IaaS) and JFrog does not host any system in the scope of this report on-premises. The CC6.4 trust services criteria related to physical security are mostly managed by AWS, GCP, and Azure and are therefore partially included in the scope of this report. Control activities performed by AWS, GCP, and Azure have been excluded from the scope of this report. JFrog performs a review of service auditor reports for its service providers as part of its annual vendor monitoring and risk assessment processes.

Control Environment, Risk Assessment Process, Information and Communications, and Monitoring Activities

Internal control is a process, effected by JFrog's boards of directors, management, and other personnel. The internal control process is designed to enable JFrog to achieve organizational objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations. The following section is a description of the components that comprise internal control for JFrog.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management, the board of directors, and others, concerning the importance of controls and the emphasis given to them in JFrog's policies, procedures, methods, and organizational structure.

Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and made available to the Company's employees through JFrog's internal portal. JFrog's executive management recognizes its responsibility to direct and control operations, and to establish, communicate, and monitor control policies and procedures. Responsibility and accountability for developing and maintaining these are assigned to relevant personnel.

Authority and Responsibility: Lines of authority and responsibility are clearly established throughout the organization and are communicated through JFrog's:

- management operating style
- organizational structure
- employee job descriptions, and
- organizational policies and procedures

Board of Directors: The JFrog Board of Directors (BOD) is comprised of nine directors, three of whom are Co-founders. The Board of Directors actively provides strategic direction to JFrog. The Board's responsibilities include but are not limited to, the following: (1) monitoring JFrog's actual performance through its financial results; (2) monitoring JFrog's compliance with legal and regulatory requirements; (3) analyzing JFrog's budget against actual results; (4) guiding JFrog's operational funding; (5) approving arrangements with executive officers relating to their employment relationships with JFrog, including, without limitation, employment agreements, severance agreements, change in control agreements, and restrictive covenants, and (6) approving equity-based compensation plans in which directors, officers or employees may participate. The Board meets on a quarterly basis. The Board meeting has a fixed agenda that includes, as applicable (1) financial (2) HR (3) security (4) business updates (5) Marketing and Sales (6) other matters (management discussion) (7) updates from the Board committees**.** The Board's Committees (Audit, Compensation, and Nominating Governance) meet quarterly to discuss a preset agenda and to evaluate threats and risks during risk assessment meetings according to each respective committee's charter**.**

Management Philosophy and Operating Style: The BOD has delegated to the executive team, chaired by the Chief Executive Officer (CEO), the responsibility of managing JFrog and its day-to-day business operations. The executive team has proven expertise in software management and distribution. It assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management team also designs policies and procedures that communicate to JFrog employees, JFrog's objectives, how an employee's individual actions interrelate and contribute to those objectives, and how and for what an employee will be held accountable. The executive team meets at least on a monthly basis, in order to evaluate risks and threats and discuss, inter alia, security and non-compliance issues and address them.

Integrity and Ethical Values: Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the cornerstones of JFrog's ethical and behavioral standards and are implicitly communicated, monitored, and enforced in JFrog's business activities. These cornerstones are included in the "Codex", which is provided to all new JFrog employees. The "Codex" communicates organizational values and behavioral standards through JFrog policy statements and statements from its corporate executives. The BOD and the Management team not only recognize their responsibility to foster a strong ethical environment within JFrog but more importantly, to guarantee that JFrog's business affairs are conducted with integrity and in accordance with the highest standards of personal and corporate conduct. These high standards of personal and corporate conduct are reflected in JFrog's Code of Business Conduct and Ethics, Anti-Corruption Policy, and other relevant corporate governance policies. New employees are required to sign a standard employment agreement and an NDA addressing business practices, conflicts of interest, confidentiality, and intellectual property**.**

Human Resource Policy and Practices:
JFrog has established a "Human Resources Security Policy" that outlines security guidelines for employees and managers related to HR processes. This policy and other procedures relate to hiring, orienting, training, evaluating, promoting, and compensating personnel. The organization's ability to recruit and retain highly trained, competent, and responsible personnel is dependent on its human resource policies and practices. Job descriptions are documented and posted on JFrog's website. Candidates go through screening and appropriate background checks when applicable by local law, and include checking references and recommendations**.**
JFrog has defined various user roles, according to the various positions and activities in the company, at each of its locations worldwide. Each JFrog employee and/or contractor will be assigned an applicable role (in accordance with the employee/contractor's position within the company) and receive access control privileges relevant to that role.

Control Activities

Control activities include, but are not limited to, JFrog's Information Security Policy, Information Security Incident Management Policy, Information Classification Policy, and JFrog's Security Awareness Training Program. These policies and procedures enable management directives to be executed to address risks that may hinder JFrog in achieving its objectives. JFrog's operating and functional units must implement control activities that help achieve business objectives associated with the following:

- (1) the reliability of financial reporting,
- (2) the effectiveness and efficiency of operations, and
- (3) compliance with applicable laws and regulations

The control activities are designed to address specific risks associated with JFrog's operations and are reviewed as part of the risk assessment process. JFrog has developed formal policies and procedures covering various operational matters, which document the requirements for the performance of many control activities. Controls are in place to put the policies into action in a timely manner. Competent personnel with sufficient authority perform the control activities with diligence and focus. Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary. Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and made available to JFrog's employees through JFrog's internal portal.

Risk Assessment

JFrog has implemented Cyber, Information Security & GRC Risk Assessment and Treatment Methodology policy and procedure in place, to outlines JFrog's approach for assessing and treating risks related to cyber-security, information security, and cyber & information security compliance. It is designed to ensure that the JFrog systematically identifies, evaluates, and mitigates risks to protect its information assets and comply with relevant cyber and information security regulations.

Risk Identification

The process of identifying, assessing, and managing risks is a critical component of JFrog's internal control system. The purpose of JFrog's risk assessment process is to identify, assess, and manage risks that affect the organization's ability to achieve its objectives. Risk analysis includes identification of key business processes in which potential exposures of some consequence exist. Potential exposures defined by JFrog consider both internal and external influences that may harm JFrog's ability to provide reliable products and services. The JFrog Risk Identification process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying threats to information assets from intentional (including malicious) and unintentional acts, and environmental events; and (4) identifying the vulnerabilities of the identified assets. Identifying potential exposures also includes analyzing potential threats and vulnerabilities arising from vendor-supplied goods and services, business partners, customers, and others with access to JFrog's information systems.

Information and Communication

Information and communication are integral components of JFrog's internal control system. Communication is the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage and control the organization's operations. At JFrog, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees. Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties. A knowledge base tool is available to customers to better guide them how to use the JFrog product. Managers communicate to their employees their responsibilities and employees are provided with the information required to execute those responsibilities. The JFrog change management tool is used to communicate changes that may affect system security, availability, or confidentiality-related issues to management. Changes are classified by severity and priority. The JFrog knowledge management system is used to communicate and share general, organization-wide updates to security policies and procedures to the appropriate personnel. Changes that may affect system security, availability, or confidentiality are communicated to management and affected users. Such communication is carried out via the help center. Changes impacting customers are communicated to them through release notes posted to the JFrog support portal, while internal employees receive notifications via JFrog's internal portal or other applicable methods of internal communication.

Network Security

JFrog has Network Security Policy in Place to ensure the protection of JFrog's information in corporate networks and its supporting information processing facilities. JFrog has implemented a variety of controls and network-based security measures to protect its enterprise network. A combination of hardware and software-based tools has been deployed to protect the network and help control access to and maintain the integrity of data residing on its systems. This includes the use of network security infrastructure and continuous monitoring tools. JFrog network access is authenticated using an industry-standard security protocol, which requires at least two factors of authentication. Endpoint devices (i.e., workstations and laptops) is encrypted by automated software to ensure the safety of sensitive information. Access to, exchange of, and extraction from memory storage is allowed only to registered and authorized JFrog devices.

Secure Software Development Life Cycle (SSDLC) Overview

JFrog has implemented a formal Secure Development Life Cycle (SDLC) policy that covers all stages of software development, including design, development, testing, and deployment. This policy integrates security at every stage of the lifecycle through the Secure Software Development Life Cycle (SSDLC) process, ensuring compliance with industry standards and organizational security requirements. The policy reviewed and approved by management annually.

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by authorized personnel within JFrog's Change Management application. Infrastructure Changes follow the same process as Code changes. Software development and change management include development and production changes to all JFrog solutions. As part of JFrog's practices, JFrog follows the Open Web Application Security Project (OWASP) standards and updates, adopting their secure coding checklist and sharing them with the relevant teams. Relevant JFrog personnel are trained in secure development best practices in accordance with industry standards using a development secure training application, educational sessions, security vulnerabilities demonstrations from penetration tests, bug bounty programs, Capture the Flag (CTF) events and more.

The software development lifecycle incorporates a continuous review of the product roadmaps to identify initiatives requiring enhanced security scrutiny. Such initiatives undergo a risk evaluation to determine the necessity of specific interventions, such as secure design reviews or internal penetration testing. These security requirements are defined, executed, and validated to ensure the integrity of the release.

A code review process is enforced throughout the continuous integration process. All code builds are transferred to a staging environment by an automated tool after successfully passing the testing pipeline. Once approved, new versions are promoted for public use to the production environment while, in parallel, each released build must pass unit and integration tests using the orchestrator tool. Each repository has at least one designated code owner responsible for reviewing and approving changes. A periodic review of the code owners list is conducted to ensure it reflects current team structures and responsibilities.

Successful unit tests and integration tests are performed to each merge request, using the orchestrator coverage tool. Authorized personnel deploys changes to the production environment by using continues deployment machinimas. Through the use of an orchestrator coverage tool, every merge request undergoes unit testing and integration testing**.** Vulnerability code scanning findings trigger an alert to relevant personnel. Notifications of test failures are sent to key JFrog personnel. Each is documented in the change management tool**.** Appropriate JFrog personnel are notified when new versions are deployed to production. Changes impacting customers are reviewed in the change management meetings and, where applicable, are communicated through release note emails. Database changes are developed by the developers and tested as part of the QA process (see above).

JFrog's Production Environments

JFrog SaaS products are offered via AWS, GCP and Azure (Microsoft's cloud computing platform), with data centers located around the globe. JFrog Connect and JFrog Advanced Security (JAS) are offered on AWS in different regions.

The processes described below are executed within JFrog's production environments, which are hosted in multiple data centers and operated by a variety of cloud service providers to include AWS, GCP and Azure (Microsoft's cloud computing platform). JFrog's production environment is located in multiple regions. To maintain high availability standards, each region has a replica in a different availability zone. Access to the production environment is restricted to authorized personnel. Access is accomplished via a unique account. Developers have restricted permissions to the production environment based on predefined policies**.** Access to system administration and deployment tools and servers is restricted to authorized personnel. Access to version control, build, and change management tools is restricted to authorized personnel only. Permissions are granted through personal identity verification using SSO with 2FA.

The JFrog production environment architecture leverages each cloud provider's best practices. Security and access standards infrastructure management are performed using a given cloud provider's tools. JFrog uses a dedicated web interface, as well as infrastructure as a code Access to the individual cloud provider's management interface is restricted to authorized individuals. Customers are permitted to choose a preferred cloud provider, as well as a region in which their application(s) will run. Customers may also opt for an isolated solution, which entitles them to dedicated resources. Interactions between customers and JFrog's production environment are restricted to an encrypted channel on an authenticated SSL connection.

JFrog's Access Control strategy avoids legacy corporate-network architecture, focuses all security efforts on a full zero-trust model, enforces MFA, device and user verification, and temporary credentials wherever possible. Each physical network is the same as a public network; JFrog does not own its physical network infrastructure. Access to the production environment servers is restricted to authorized personnel (detailed under the section 'Production Environment Logical Access').

System Documentation

A description of the JFrog system and its boundaries is documented and communicated through the JFrog website and/or online help-center**.** The description is also available to all JFrog employees. The information provided is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information, including but not limited to policies, procedures, guidelines and system documentation, is reviewed annually and the information's relevance is assessed to support JFrog's internal control components.

Production Environment Logical Access

The JFrog Cloud ("SaaS") is a fully separated network on a dedicated infrastructure. The production environment is completely isolated from any other environment. Access to the production environment is restricted to authorized personnel. Access is accomplished via a unique account. Access to the production environment is given based on operational requirements. Only relevant Operations personnel are granted access. Users are identified through the use of a unique user ID/password combination using JFrog's identity management system. Strong password configuration settings are enforced for system access to ensure robust authentication. These settings include the requirement for multi-factor authentication (MFA), password complexity standards, and account lockout mechanisms to protect against unauthorized access. Access is provided using a change management (CM) tool, which allows for the creation of individual user accounts that have a one-time access token to the Kubernetes, host, and production stuck.

Logical Access

JFrog has established a JFrog-wide Physical and Environmental Security policy designed to protect information at a level commensurate with its values. The policy dictates security controls for media where information is stored, the systems that process it, as well as the infrastructure components that facilitate its transmission. Logical access to stored data is restricted to application and database administrators. Data is stored in encrypted format using software that supports the advanced encryption standard (AES). Access permissions are reviewed on an annual basis. A Just-In-Time (JIT) access mechanism is implemented to grant and revoke access automatically to the AWS, GCP and Azure production environments. The process is fully automated according to pre-approved requests by the system owner and the direct manager of the requester.

Recertification of Access Permissions

JFrog has implemented a recertification process to help ensure that only authorized personnel have access to the production interface, servers, environments, and databases. Users, administrators, and permissions on the production environment's servers and databases are reviewed on a quarterly basis. The JFrog platform's new users are granted access upon notification from the HR department, using an on-boarding tool, first to staging, and then granted access, following internal accreditation, to production. Access to the JFrog platform is only possible via SSO, which is managed centrally by authorized personnel. The DevOps Group is responsible for granting access to the JFrog production environments, databases, and other production-related systems and services, based on the employee's role; the user's access is documented within a dedicated tool. Other relevant JFrog employees are granted permissions to relevant applications on a need-to-know (least privilege) basis, where access to the specific systems and applications are authenticated using multi-factor-authentication (MFA).

Access Revocation

Upon notification of job termination by an HR employee, the offboarding process is initiated to automatically disable user accounts from JFrog's production platform, applications, and databases on a timely manner. A process is in place to automatically deactivate users on their termination day. Terminated employees go through an off-boarding process which includes the completion of a termination clearance process on their last day at JFrog. The termination notification and completion are documented and accessible within the JFrog Internal IT management ticketing system. This process includes access revocation of access permissions to JFrog's systems and premises, as well as the timely return of JFrog property, data, equipment, and other JFrog assets. If the terminated employee and if they had access to the production environment, their permissions are removed in a timely manner, as well as access to all company information assets.

JFrog has implemented a security awareness training program that focuses on secure handling of JFrog's confidential information, secure handling of personal information, and secure handling of customer data. Phishing training is performed on a quarterly basis by the JFrog Security Group and sanctioned management with defined KPI's for success. If an employee fails the campaign, remediation training is mandated. Role and Responsibilities oriented security and privacy awareness training is delivered in accordance with JFrog's training program, at least annually. The internal ticketing system maintains the employees' training records, enables an employee to receive training on JFrog Guidelines, JFrog policies and procedures, and provides the capability to acknowledge completion of a specific training module. Training can be delivered by LMS, Frontal, Guidelines, Policies, and acknowledgment.

Production Monitoring

JFrog's production network encompasses numerous components, including web services, application and data server types, databases and monitoring tools provided as part of AWS, GCP and Azure services. To provide high service availability to customers and to support the operations of the cloud environments, JFrog maintains a list of authorized personnel that are responsible for ongoing work within the production environment and responsible for investigating escalated issues. An automatically generated log entry is produced after every access to a JFrog-hosted environment or database. The production environment, including servers and the application, is monitored 24/7/365 by the DevOps Group, the Production engineering, and NOC teams. Key JFrog management staff members are notified of events related to security, availability, and confidentiality.

Changes to production are strictly audited and monitored and rely on major design principles, Infrastructure as code (IaC), and immutable infrastructure.

Infrastructure-as-code - All changes to JFrog's production environment follow the same SDLC principles as all other code. All changes are written as code and performed automatically. This means all changes are audited and approved, leveraging the same process, gates, and auditability of the code CI/CD pipeline. This approach enhances configuration management controls, auditability, and security of the production environment; access into the production environment is strictly controlled and manual changes create an immediate red flag for suspicious activity. Immutable infrastructure - The complementing control to IaC is immutable infrastructure. All components of the infrastructure are immutable and are automatically replaced when an upgrade is needed. Furthermore, any manual change in production will be immediately flagged and inspected.

Attachment B – Principle Service Commitments and System Requirements

Availability Procedures

JFrog's production environment is managed and monitored 24/7/365 to ensure high service availability. The infrastructure is distributed across multiple geographic regions, with data replicated across different availability zones to maintain resilience against localized failures.

As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water. The detection measures allow JFrog to identify anomalies that could result from environmental threat events.

JFrog maintains robust backup and recovery processes to protect the integrity and availability of information. Automated backups are performed at regular intervals (daily and weekly) and are retained for defined periods according to business requirements. These backups are stored in a secure, secondary infrastructure with restricted access. To ensure data durability, JFrog utilizes cross-region replication for critical data sets. Restoration procedures are in place to recover data in the event of accidental deletion, corruption, or unforeseen disruptions.

JFrog's resilience strategy ensures the continued operation and rapid recovery of business-critical services. The Disaster Recovery Plan (DRP) defines the protocols for maintaining services during significant regional cloud provider outages. This strategy focuses on meeting predefined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

The BCP's primary objective is to protect the continuity, confidentiality, integrity, and availability of JFrog's and third-party systems, while ensuring the safety of all personnel. The Business Continuity Plan (BCP) focuses on the human, operational, and business management elements of resilience, ensuring that JFrog's personnel and business processes can function during events such as Platform Disruption ranging from localized hardware failures to regional cloud provider outages (AWS, GCP, Azure), loss of third-party SaaS dependencies, or broader crises such as cyber-attacks, ransomware, geo-political instability, Public Health Emergency, or the loss of physical corporate facilities. Governance of the BCP is managed by a Crisis Management Team (CMT) who are responsible for evaluating incidents and mobilizing support, and allocating resources. To ensure recovery is prioritized effectively, JFrog performs an assessment of its essential business functions and infrastructure to identify mission-critical dependencies and the potential impact of various downtime scenarios.

Confidentiality Procedures

Customer confidentiality is a key factor in JFrog security strategy. JFrog understands that confidentiality issues are critical as they relate to services provided. Information handled by JFrog is considered private and subject to the highest levels of security (see Logical Access and Security above). JFrog discloses its confidentiality practices through various media, such as the JFrog website, its applications, and its contracts. JFrog notifies the impacted customers whenever a disclosed confidentiality practice is discontinued or changed to be less restrictive**.** Customers' sensitive data is encrypted within the JFrog application**.** Additionally, to maintain the levels of system confidentiality that conform with JFrog's confidentiality commitments, third-party infrastructure providers sign confidentiality agreements with JFrog**.** Logical access to stored data is restricted to authorized personnel. Data is stored in encrypted format using software supporting the advanced encryption standard (AES). Access permissions are reviewed on an annual basis**.** Moreover, the enterprise requires a minimum of AES 256-bit level encryption for data at rest and secures production data containers, using server-side encryption**.**

Related party and vendor systems are subject to review as part of the vendor risk management process. When available and applicable, attestation (i.e., SOC 2) reports are obtained and evaluated**.** Also, a confidentiality agreement is incorporated into contracts as it relates to contracts with infrastructure third party providers in accordance with JFrog security policy. JFrog places a heavy emphasis on logical security segregation built within its hosted applications to separate one tenant's users from others. Encryption between JFrog customers and the JFrog application is enabled using best practices and industry standards. JFrog customers are restricted to their own web interface environment (server), and do not have access to view data in other JFrog environments. An automatically generated log entry is produced after every access to a JFrog-hosted environment or database. Additionally, new vendors, business partners, and subcontractors are required to sign a standard NDA agreement, which contains clauses regarding confidentiality and the use of intellectual property. Upon customer request, or at the conclusion of a contractual agreement, JFrog shall delete customer's personal information pursuant to such contractual agreement, within a defined period in accordance with contractual obligations.

Privacy Procedures

JFrog has established a comprehensive privacy framework, including policies for data retention, personal data protection, and legal incident response. These policies are reviewed annually to maintain alignment with global data protection standards. Governance is overseen by a dedicated Privacy Team, which ensures that privacy requirements are integrated into business operations. To reinforce these standards, all employees and contractors undergo mandatory privacy and data protection training upon hire and annually thereafter.

Personal information is collected and processed in accordance with defined privacy objectives and contractual commitments. JFrog maintains the accuracy and integrity of personal data throughout its lifecycle. Access to databases containing personal information is restricted to authorized personnel and is subject to quarterly access reviews. JFrog follows formal procedures for the secure disposal and deletion of personal data upon customer request or contractual expiration, in accordance with applicable laws and agreements.

JFrog maintains transparency by disclosing its data collection and usage practices through a public Privacy Policy on its website. Procedures are in place to address inquiries and requests from data subjects, including the right to access, correct, or erase their personal information. JFrog assists customers in fulfilling their obligations regarding data subject rights under applicable data protection regulations

Privacy and security are inherent components of JFrog's Secure Software Development Life Cycle (SDLC). Secure coding practices and privacy risk assessments are integrated into the development process for all production changes. Furthermore, JFrog extends its privacy commitments to third parties through formal agreements and periodic compliance assessments. For international data transfers, JFrog utilizes approved legal mechanisms, such as Standard Contractual Clauses, to ensure continued protection across jurisdictions.

JFrog maintains a robust incident response procedure to detect and address unauthorized disclosures or data breaches. In the event of a validated breach, JFrog provides timely notification to affected parties and regulators as required by law. These notifications include the nature of the breach, potential consequences, and mitigation measures taken. JFrog works closely with impacted customers to support investigations and prevent recurrence through enhanced security measures.