FIGMA, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR FIGMA PLATFORM

FOR THE PERIOD OF NOVEMBER 1, 2023, TO OCTOBER 31, 2024

Attestation and Compliance Services

INDEPENDENT SERVICE AUDITOR'S REPORT

To Figma, Inc.:

Scope

We have examined Figma, Inc.'s ("Figma", "Company") accompanying assertion titled "Assertion of Figma Service Organization Management" ("assertion") that the controls within the Figma Platform system ("system") were effective throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Figma'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, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Figma uses various subservice organizations for cloud hosting and identity access management services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Figma, to achieve Figma's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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.

Service Organization's Responsibilities

Figma 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 Figma's service commitments and system requirements were achieved. Figma has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Figma 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 whether 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 systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. 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 controls were not effective to achieve Figma's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Figma's 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.

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 Figma's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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 the Figma Platform system were effective throughout the period November 1, 2023, through October 31, 2024, to provide reasonable assurance that Figma's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Tampa, Florida
December 20, 2024

ASSERTION OF FIGMA SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Figma, Inc.'s ("Figma") Figma Platform system ("system") throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Figma's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below 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 November 1, 2023, to October 31, 2024, to provide reasonable assurance that Figma'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Figma's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 November 1, 2023, to October 31, 2024, to provide reasonable assurance that Figma's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE FIGMA PLATFORM SYSTEM

Company Background

Figma was founded in 2012 and provides a web-based Software-as-a-Service ("SaaS") interface design tool that allows users to easily brainstorm, create, collaborate, and securely share interface and application designs. Figma's mission is to make design accessible to everyone. Figma is compatible with web browsers and offers mobile, iOS, Android, and desktop applications so users can design and brainstorm on their preferred device. Figma has been adopted by many organizations ranging from startups to large multinational organizations. Figma is headquartered in San Francisco and operates offices worldwide. Learn more at www.figma.com.

Description of Services Provided

Figma Design

Figma is where teams come together to design, iterate, and test better products. The first design tool built for the Web, Figma combines powerful features with multiplayer functionality to make it faster, easier, and more fun for teams to design products together – from start to finish.

FigJam

FigJam is an online whiteboard for teams to brainstorm, meet, and work together. Purpose-built for exploration, FigJam makes everything from ideation to weekly syncs easier and more fun – whether you are working alone or collaborating with an extended team.

Dev Mode

Dev Mode is a workspace in Figma to efficiently translate designs into coded products. With Dev Mode, designers and developers can work in different modes in the same files, making it easier for developers to find the information they need while harnessing the tools they use every day. Built with developers' needs at the forefront, Dev Mode bridges the gap between design and development.

The systems in-scope for this report are Figma Design, FigJam, and Dev Mode (collectively referred as "Figma Platform system"), which are hosted in Amazon Web Services ("AWS"), and the supporting IT infrastructure and business process.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

Principal Service Commitments

Figma designs its processes and procedures to meet its objectives related to the System. Those objectives are based on the service commitments that Figma makes to user entities, the laws and regulations that govern the provision of the System and the financial, operational, and compliance requirements that Figma has established for the System.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the terms and conditions within the sign-up page in Figma and through the Software Services Agreement ("SSA") with customers. The description of the service offering, relevant components, boundaries, and customer responsibilities are documented on Figma's website https://www.figma.com/security/.

Figma's security, availability, and confidentiality commitments, and related operational requirements include the following:

Service Commitments	Description
Security	The System and customer data is protected against unauthorized access, use, or modification through a range of security processes and controls to identify issues and minimize impact. Figma creates, protects, and retains systems audit records to maintain integrity and enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate systems activity. Figma assigns responsibility for information security management to senior personnel. Figma deploys a log management solution and retains logs produced by intrusion detection systems for a minimum period of one year.
Availability	The System is available for operation and use as committed or agreed. Figma uses industry standards for redundancy, robustness, and scalability to maintain the availability of the platform. Further Figma implements and maintains contingency plans to address emergencies. Backups and recovery testing is done on a regular basis.
Confidentiality	The Company will not disclose information to any person or entity, except the Company's employees, agents, contingent workers, and service providers bound by non-disclosure obligations and have a need to know. Figma encrypts customer data in Figma's possession or control so that it cannot be read, copied, or changed by unauthorized personnel while in transit or storage. At the expiry or termination of service Figma will return or delete data as per customer specifications.

System Requirements

Figma establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Figma's policies and procedures, system operation and boundaries, and terms and conditions with its customers. Information security policies are defined, posted, and available, delineating how Systems and data are protected. These include policies around how the System is operated, how employees are hired and trained, the use of encryption technologies to protect customer data at rest and in transit, and a formal process to grant and revoke access to customer data.

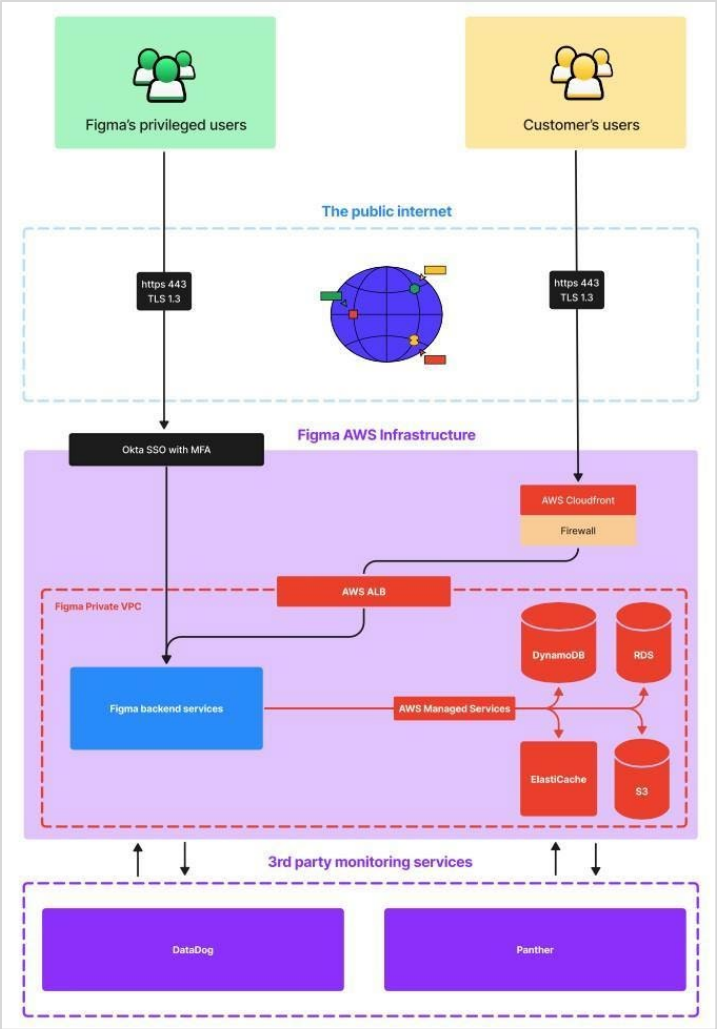
In accordance with the assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to each system user, in each individual case.

Infrastructure and Software

Infrastructure

The System is hosted on AWS in the United States and European Union (EU) across multiple regions and availability zones to support fault tolerance, high availability, and disaster recovery. The infrastructure is managed and configured using a configuration management software. AWS operates under a shared responsibility model. Under this model, Figma uses AWS for services related to server hosting, physical and environmental protection, network management, and disk storage supporting the System. Furthermore, Figma is responsible for configuring and maintaining the System architecture in AWS to help ensure availability, security, and resiliency requirements. At Figma, Customer Data is defined as any application(s) and/or material(s) that are developed by Customer on the Figma Platform or uploaded to the Figma Platform by Customer, as well as any Personal Data pertaining to Customer's Authorized Users of the Figma Platform Processed by Figma on behalf of Customer under the Agreement. In other words, Customer Data is any data submitted to the Figma Platform. Customer Data is subject to technical safeguards, as described in Exhibit C of Figma's Software Services Agreement (https://www.figma.com/ssa/).

The System is based on a multi-tenant architecture that applies common and consistent management processes and controls for customers. The System is also designed with logical security controls in place where each customer's data is segregated from other customers' data. The infrastructure has been designed to provide high availability and critical infrastructure components are redundant across multiple AWS availability zones. Web servers and databases are deployed in multiple availability zones each consisting of one or more discrete data centers, with fully redundant power, networking, and connectivity housed in separate secured facilities. The System is built on Linux servers and runs on Amazon Relational Database Service "RDS." The following diagram shows major components of the System.



Production Infrastructure

Data Storage: AWS Simple Storage Service ("S3") and RDS) are managed services provided by AWS. Figma maintains RDS databases to store Customer Data and meta-data associated with the Figma Platform. Figma's usage and maintenance of RDS only applies to Figma's U.S. AWS environment. AWS S3 is the primary datastore for images, components, and other contents of the Figma Platform. Figma's usage and maintenance of S3 applies to both Figma's U.S. and EU AWS environments. Figma customers who are on the Enterprise plan can choose to localize key parts of the Figma System data in the EU (https://help.figma.com/hc/en-us/articles/15643274574871-Enable-localized-file-hosting-in-the-EU). Customer Data in RDS and S3, regardless of where it's stored, is encrypted at rest, backed up, and replicated across availability zones and regions.

Network Connections: Content Delivery Networks ("CDNs"), load balancers, and Envoy proxies are used to connect to the service within AWS. Customer traffic is routed through AWS CloudFront, with features such as AWS Shield and AWS Web Application Firewall ("WAF") to protect against distributed denial-of-service "DDoS" attacks and other types of malicious traffic. Figma's production environment is hosted on a virtual private cloud ("VPC") which

is shared between customers, and isolates Figma's production environment from other development and administrative environments. Customer traffic into and out of the production environment uses Transport Layer Security ("TLS") connections to secure data in transit.

Application Servers: The Figma Platform application servers run on AWS Elastic Cloud Compute ("EC2"), AWS Lambda, Amazon Elastic Kubernetes Service ("EKS"), and AWS Fargate, and use encrypted Elastic Block Store ("EBS") volumes. AWS Security Groups are used to restrict communication between servers and databases within the VPC.

Corporate Infrastructure

Figma employees access the production network securely using a Figma-managed laptop authenticated with a unique username, password, and multi-factor authentication. Figma employees are not allowed to work from certain countries or regions that are subject to U.S. sanctions. Only privileged users are allowed to administer changes to the Corporate Infrastructure.

Software

Figma leverages a range of third-party tools and services to build, support, secure, maintain, and monitor the Figma Platform and processes. These tools include but are not limited to:

- Infrastructure and Hosting: Figma's platform is hosted on AWS, providing scalable and secure infrastructure, including hosting, storage, databases, and network security.
- Development and Operations: GitHub supports secure source code management and development workflows, to help ensure efficiency and control in the software development lifecycle.
- Security and Monitoring: Infrastructure and application monitoring are handled using industry-standard tools such as Datadog, enabling proactive detection and response to potential security and performance issues.
- Identity and Access Management: Access controls are implemented using Okta and Opal, to enforce user authentication, authorization, and privileged access.

People

Figma has a clearly established organizational structure that outlines reporting lines and areas of authority. The people listed below consist of the personnel involved in the governance, operation, and use of the Figma Platform:

- Engineering and Product:
    - Design, test, deployment, and maintenance of the Figma Platform
    - Provide scalability and reliability of the Figma Platform
    - Perform research and development activities
    - Optimize data capabilities and workflows
- Security and Security Compliance:
    - Security of the Figma Platform and the corporate / production infrastructure
    - Management of threats, vulnerabilities, and incidents
    - Provide anti-abuse against malicious actors
    - Perform risk mitigation and risk treatment
    - Perform third-party vendor risk management
    - Security governance and policy management
    - Deliver new-hire and annual security awareness and privacy training

- Legal:
    - Ensure Figma and the Figma Platform maintains compliance with applicable statutory, regulatory, and contractual obligations
    - Negotiate contractual obligations with third parties and partner ecosystem
    - Manage relationships with the board of directors
- Information Technology (IT):
    - Provision, maintain, and properly dispose of corporate laptops
    - Manage business applications and employee / contingent workers identities
    - Manage physical technology in global offices
- People Operations (HR):
    - Facilitate the employee / contingent workers onboarding process
    - Facilitate the employee / contingent workers termination process
    - Assist in the recruiting of employees:
        - Perform background checks in accordance with local laws
        - Manage and oversee global offices
- Product Support:
    - Directly support customers and their use of the Figma Platform
    - Create public and internal documentation related to the use of the Figma Platform

Procedures

Processes include the automated and manual procedures involved in the operation and maintenance of the Figma Platform. Procedures are developed, documented, and socialized for a variety of processes, including those related to Engineering, Security, IT, People Operations, etc., as detailed in this System Description. These processes are drafted in alignment with Figma's Information Security Policies and are reviewed and updated as necessary to continue aligning with Figma's structure and business needs.

Access, Authentication, and Authorization

Logical access controls are in place to prevent unauthorized access to Customer Data and resources within the production and corporate environment. Upon hire, each Figma employee is set up with a Figma-managed device and a unique corporate account which acts as a single source of identity to access in-scope systems which access or impact Customer Data. Certain restricted IT personnel maintain separate administrative accounts which are only used for administrative activities.

By default and at a minimum, access to in-scope systems must stem from a Figma-managed device, use a unique username and password, and undergo a multi-factor authentication step. Further authentication mechanisms, such as Secure Socket Shell ("SSH"), may be required to access certain services or functionality of the in-scope systems.

To help ensure that access remains appropriate over time, Figma performs a quarterly privileged user access review for in-scope systems which access or impact Customer Data. Inappropriate users are flagged and either removed from the in-scope system entirely or their access is modified.

Customers may configure their access to the Figma Platform as required for their needs. This may include using a basic e-mail and password, logging in with Google Single Sign-on ('SSO"), or using Security Assertion Markup Language ("SAML") SSO. Multi-factor authentication can also be optionally configured and enforced with an individual's Figma account. Native customer passwords are hashed and then the resulting hash value is stored in the database.

Customer Data and access to that data is logically separated via the use of globally unique identifiers ("IDs"). Roles and permissions can be set on the user, team, and organization level, as well as on the file, folder, and project level. These assigned roles and permissions are linked for database / datastore organization, as well as to restrict access appropriately and prevent application attacks. More information on sharing and permissions can be found at https://help.figma.com/hc/en-us/sections/1500001331382-Sharing-and-permissions.

Access Requests and Access Revocation

Base applications are assigned according to a new hire's role and/or department. Requests for new internal user accounts, or changes to existing internal accounts that elevate permissions beyond the default roles which are provided upon hire or defined in pre-approved role matrices, are documented and approved prior to access propagation. Certain high-risk roles are also time-bound so Figma personnel can only obtain access to these roles for a limited period of time, upon which they would need to re-request access to the specific role upon expiration.

Upon termination, Figma's People Operations team notifies IT to terminate the user's corporate account on their last day of work. Once their corporate account is terminated, access to the Figma network, including in-scope systems, is automatically removed. Additionally, personnel with a Figma-managed device are required to return their device back to Figma's IT team for re-imaging or destruction.

Virtual Firewalls

Figma uses virtual firewalls within AWS virtual private cloud ("VPC") as a protection mechanism to prevent access to or alteration of any information asset by unauthorized personnel. Figma configures each VPC with a specific IP address range, subnets, associated security groups, and routing tables, to prevent unauthorized inbound network traffic. Access to modify virtual firewall settings and other network device configurations is restricted to the appropriate personnel**.** Additionally, as part of the defense in depth strategy, Figma continuously monitors its cloud security configuration to ensure that only approved services (i.e., Amazon Load Balancers) are listening on the Internet and administrative ports like Remote Desktop Protocol ("RDP") are disabled.

Device Protection and Asset Management

Figma-managed devices are centrally registered and controlled via a mobile device management ("MDM") system. Figma's IT and Security teams are responsible for the proper configuration, management, and security of devices used to access Figma's corporate and production systems. Prior to provisioning a Figma-managed device to a new employee or contingent worker, it is registered via the MDM system with security policies technically configured and enforced. Figma-managed devices have system-enforced password complexity settings, hard-disk encryption, and anti-malware protection software installed and enforced. Malware signatures are updated continuously and any potentially known malware on any Figma-managed device is quarantined and investigated until the issue is resolved.

Additionally, the MDM allows Figma's IT and Security team to act on out-of-compliance devices, remotely wipe devices if they're lost or stolen, perform forensic analysis, and force push or block operating system updates until they're approved.

Change Management

The change management process at Figma is aimed at ensuring the stability, reliability, and security of code changes to the Figma Platform. Figma has a Secure Development Policy in place which establishes the requirements for change initiation, development, reviews, testing, deployment, and emergency changes.

Change Initiation

Changes to the Figma Platform are initiated by product development or Engineering teams when a change to the software, functionality, or specification of the product is required. Changes may also be initiated when a bug in the Figma Platform is identified, to remediate a vulnerability, or to mitigate or resolve an incident.

Change Development

Figma uses the Agile development methodology in which normal changes and development work is captured in Asana tasks. Code changes are managed through Figma's version control software, GitHub. Figma employee access to GitHub is restricted to authorized personnel in Engineering, Product, Security, and a few other teams who require read or write access to specific repositories as part of their normal job responsibilities.

The change process starts with a developer creating new or modifying source code files from Figma's primary repository in Github, where they create a feature branch. Once the development work is completed, developers test the change in their development environment prior to opening a pull request ("PR"). Figma maintains separate development, staging, and production environments, and code changes are developed and tested in separate environments prior to promotion to the production environment. Customer Data is not used in development, testing, or staging environments.

Once a GitHub PR is opened by a developer with the appropriate code changes, the developer requests for a peer review of the code changes. Source code changes require a peer review and approval prior to merging the change to the master branch, and this is technically enforced via Figma's defined branch protection rules. For additional protection, Figma ensures that new commits must originate from a Figma-managed endpoint as each commit is digitally signed for integrity, otherwise, the commit will be blocked from merging to the master branch. Additionally, any changes made without a peer review trigger automated alerts that are reviewed for appropriateness by the Security team.

Change Testing

Figma's source code is merged to the master branch undergoes automatic and continuous integration testing and is queued up for release by Figma's merge queue platform. Each release is subject to testing and must successfully pass all tests before being implemented into the production environment.

Figma also uses an automated static analysis testing tool to detect any known vulnerabilities in Figma's source code. If a vulnerability is identified, an alert is triggered, and a notification is sent to Figma's Security team to review.

Change Deployment

Figma Engineers use an internal web application service to deploy its changes to the production environment. Code changes are typically deployed to the staging environment for testing and validation before being promoted to the production environment. Emergency changes are the exception to this process and may be deployed directly to the production environment when necessary. Access to deploy changes to the production environment are restricted to authorized personnel using the Opal access approval process.

Emergency Changes

A production emergency change may be required to mitigate or fix a service or security incident, and an immediate release of code to the production environment outside of the routine code change and release process may be necessary. During production emergencies, a PR is allowed to be merged without peer approval to expedite the deployment process, and an automated ticket is created for post-deployment review by the Security team.

Capacity Monitoring

Figma maintains robust infrastructure monitoring for system capacity, reliability, availability, performance, response time, error rate, etc. Minimum thresholds and alerts have been defined in order to alert on-call personnel if the key indicators of any services exceed those thresholds. Any service disruptions or incidents are tracked, investigated, and resolved in accordance with Figma's Incident Management process and procedures. Any high or critical service incidents are communicated to customers at https://status.figma.com/. Historical performance metrics and incidents can also be found on that page. Additionally, Figma's Engineering team performs a capacity review to assess current and future CPU and memory usage for Figma's core services on a quarterly basis.

Data Backup and Disaster Recovery

Figma maintains a Business Continuity and Disaster Recovery program to protect, mitigate the impact, and quickly recover from disasters that could affect Figma's business operations and production infrastructure hosting the Figma Platform. Key elements of this program include business impact analyses of critical business activities and technologies, roles and responsibilities during a business continuity and/or a disaster recovery scenario, testing of Figma's Business Continuity and Disaster Recovery Plan, and monitoring of system performance. Figma's Business Continuity and Disaster Recovery Plan is tested, reviewed, and updated annually. Additionally, Figma has implemented network redundancies to eliminate single points of failure and ensure high service availability.

Customer user data and meta-data stored in RDS is replicated to prevent business disruption. Figma takes snapshots of its RDS databases daily, and retains them for up to 14 days, which allows for point in time recovery

of customer data at any point within the 14 day period. Customer user data and meta-data replication is enabled across 3 availability zones within both primary and failover regions. Customer design and FigJam file data stored in S3 is also replicated between primary and failover regions in case of a disaster impacting one of the regions. Figma tests its backup restoration process on an annual basis to determine the availability and recovery of the backup data.

Vulnerability Management

Figma performs both internal and external vulnerability assessments. Figma utilizes a web vulnerability scanning tool to perform automated weekly vulnerability scans on the external network and web application for Open Web Application Security Project ("OWASP") top 10 security vulnerabilities, vulnerable dependencies, etc. On an annual basis, Figma engages a third-party vendor to perform an annual penetration test on the Figma Platform. The results of the penetration test are provided to Figma and tickets are created for each vulnerability finding identified by the third-party vendor. A retest is performed by the third-party vendor once critical and high vulnerability findings are resolved. Additionally, Figma is part of a Bug Bounty Program hosted on a third-party security and hacker platform. Through this program, Figma pays money to ethical security researchers who responsibly disclose confirmed bugs and vulnerabilities directly to Figma.

Vulnerabilities identified through the vulnerability scans, penetration tests, vulnerability intelligence feeds, and Figma's Bug Bounty Program are analyzed, documented, and tracked in Figma's project management tool. Identified vulnerabilities may be re-categorized by Figma's Security team based on factors such as attack complexity, required privileges, user interaction, scope, etc. After potential vulnerability re-categorization, vulnerabilities are prioritized and remediated in accordance with Figma's internal Vulnerability Management Guidelines.

Security Monitoring and Logging

Figma has automated tools in place, such as a Security Information and Event Management (SIEM)/Cloud Security Posture Management (CSPM) tool, to aggregate and ingest security event logs. The Security team is responsible for maintaining and monitoring Figma's SIEM / CSPM, as well as connecting new critical systems to the SIEM / CSPM. Predefined thresholds and alerts are in place to notify on-call Security team members of potential incidents or malicious activity. If an on-call Security team member determines that an alert requires further investigation, an incident may be called and will follow Figma's Incident Management process and procedures.

Access to Figma's SIEM / CSPM and the security event logs therein are restricted to the Security team and certain personnel outside of the Security team who have a need-to-know. Security event logs are protected against tampering and unauthorized access as they are vaulted to a data warehouse where monitoring and alerting is in place for individuals accessing security event logs.

An Intrusion Detection System (IDS) is in place to continuously monitor Figma's AWS production environment for compromised accounts, anomalous behavior, malware, and other types of malicious activity. Predefined triggers and alerts have been set up to notify the Security team of potential malicious events. Figma deploys a log management solution and retains logs produced by intrusion detection systems for a minimum period of one year.

Incident Management

Figma's Security and Infrastructure Engineering teams maintain a company-wide Incident Response Plan that is reviewed and updated at least annually. This Incident Response Plan is available to employees through the Company intranet. The Incident Response Plan defines the types of incident categories and their associated severity levels, how to report an incident, roles and responsibilities during and after an incident, how to escalate an incident to the appropriate personnel, and how to perform a root cause analysis and draft a post-mortem document after an incident has been resolved.

Figma has an on-call rotation schedule in which any personnel on-call are responsible for performing incident management services and to initiate, manage, respond to, and track incidents. Incidents are documented and tracked within a third-party incident management tool. For critical and high severity incidents, a root cause analysis is performed to understand how the incident occurred, the length and duration of the incident, how Figma mitigated the incident, the types of internal or external communication required as part of the incident, and preventative actions Figma has taken or plans to take to prevent future similar incidents.

Incidents resulting in a confirmed breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data attributable to Figma are communicated to affected users in accordance with applicable privacy laws and regulations. Figma's Legal team manages the communication to affected customers and users, and other relevant stakeholders as needed.

Data

Data, as defined for the System, includes electronic data or information submitted by the customer to Figma. The customer defines and controls the data they load and store in the Figma Platform. This type of data is also referred to as Customer Data. Access to Customer Data is restricted to authorized Figma personnel based on role, or access is granted after receiving proper approval from management and/or the system owner.

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

Figma has deployed secure methods and protocols for the transmission of confidential or sensitive information over public networks. Databases and data stores housing sensitive Customer Data are encrypted at rest.

Additionally, Figma has separate environments for development and production that are completely isolated at the network level. Figma creates test data that does not contain any Customer Data and uses this test data for the development of the Figma Platform.

Encryption

Secure data transmission protocols are used to encrypt data when transmitted over any public network. Any attempt to access Figma using the insecure HTTP protocol is automatically redirected to use secure HTTPS protocol. Customer traffic into and out of the production environment uses Transport Layer Security ("TLS") connections to secure data in transit.

Figma storage services housing Customer Data are encrypted at rest by default and access is restricted to authorized personnel. Figma relies on AWS service control policies and infrastructure as code to define encryption for both AWS RDS and AWS S3. Customer user data and meta-data stored in RDS is encrypted at rest using AES-256 via AWS Key Management Service ("KMS"). Similarly, customer design and FigJam file data stored in S3 is encrypted at rest using AES-256 via server-side encryption with Amazon S3 managed keys.

Data Classification and Confidentiality of Information

All Figma employees and contingent workers share the responsibility of safeguarding information with an appropriate level of protection by observing the Data Classification and Handling Policy. Data and information are classified in terms of legal requirements, value, sensitivity, and criticality to Figma, and are labeled to manage appropriate handling based on the guidelines listed below.

Data Deletion and Retention

Confidentiality risks are addressed through policies and procedures covering the use, retention, disclosure, and disposal of Customer Data within backups and log data, data classification policies and procedures, confidentiality and information sharing agreements, remote access and transmission restrictions, and vendor risk assessments.

Customer Data is retained for the duration of the service according to the Figma Software Services Agreement (SSA). Upon termination, Figma will delete the account and associated Customer Data within 30 days of termination.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Data is Sensitive when the unauthorized disclosure, alteration, or destruction of that data could have a significant adverse effect on Figma or its personnel, customers, or vendors. This category includes information that Figma has a regulatory and legal obligation to safeguard in the most stringent manner.	• Customer Data and meta-data hosted on the Figma Platform (i.e., design file data) • System Access Credentials (i.e., username, password) • Cryptographic keys • Source Code • Trade secrets • Audit Logs	Sensitive
Internal data is information that is created and used in the normal course of business but is not generally publicly available. Internal data should not be disclosed to third parties outside of Figma without a business need and should be protected with reasonable and appropriate controls.	• Financial Information and Investment Plans • Company All-hands Presentation Decks • Internal Product Roadmaps • Project Plans • Policies and Procedures • Design and Work Specifications • Non-public Employee and Contingent Worker Information	Internal
Public information, as the name implies, is data that is already publicly available or becomes publicly available without the act or omission of Figma. Public data does not require any additional controls when used.	The following information, once made public by Figma: • Press Releases • Marketing Materials • Information in the Public Domain	Public

Subservice Organizations

Figma uses subservice organizations to perform certain services.

- AWS provides the infrastructure-as-a-service and platform-as-a-service environment that provides the physical and environmental safeguards, infrastructure support and management, and storage services for Figma.
- Okta is an identity and access management tool that provides single sign-on (SSO) and multifactor authentication (MFA) services.
- Perma Security Inc., (Opal) is an identity and access management platform used by Figma to perform user access reviews and provision user access.

The table below outlines the relevant trust services criteria that controls at AWS, Okta, and Opal are designed to meet, either independently or in conjunction with controls at Figma. It also specifies the types of controls these providers are expected to implement to support Figma's principal service commitments and system requirements in alignment with the applicable trust services criteria.

Ref.	Control Activities Expected to be Implemented by Subservice Organizations	Applicable Trust Services Criteria
CSOC-01	AWS, Perma Security Inc., and Okta are responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where Figma systems reside.	CC6.1 - 6.3, CC6.5 - CC6.6
CSOC-02	AWS, Perma Security Inc., and Okta are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 – CC6.5
CSOC-03	AWS, Perma Security Inc., and Okta are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Figma systems reside.	CC6.7
CSOC-04	AWS, Perma Security Inc., and Okta are responsible for monitoring the logical access control systems for the underlying network, virtualization management software, and storage devices for its cloud hosting services where Figma systems reside.	CC7.2
CSOC-05	AWS, Perma Security Inc., and Okta are responsible for ensuring the data center facilities are equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Figma Platform.