DigitalOcean

System and Organization Controls 3 Report

Description of DigitalOcean's Cloud Infrastructure Platform
throughout the period January 1, 2023 - December 31, 2023
with Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To DigitalOcean, LLC:

Scope

We have examined DigitalOcean, LLC's ("DigitalOcean") accompanying assertion titled "Assertion of DigitalOcean, LLC Service Organization Management" ("assertion") that the controls within DigitalOcean's Cloud Infrastructure Platform system ("system") were effective throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that DigitalOcean's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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)*.

DigitalOcean uses various subservice organizations for data center hosting 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 DigitalOcean, to achieve DigitalOcean'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.

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

Service Organization's Responsibilities

DigitalOcean 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 DigitalOcean's service commitments and system requirements were achieved. DigitalOcean has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, DigitalOcean 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 DigitalOcean'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 DigitalOcean'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 DigitalOcean'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 DigitalOcean's Cloud Infrastructure Platform system were effective throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that DigitalOcean'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

Washington, District of Columbia
February 21,2024

ASSERTION OF DIGITALOCEAN SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within DigitalOcean, LLC's ("DigitalOcean") Cloud Infrastructure Platform system ("system") throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that DigitalOcean's service commitments and system requirements relevant to security and availability 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 January 1, 2023, to December 31, 2023, to provide reasonable assurance that DigitalOcean's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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)*. DigitalOcean's objectives for the system in 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 January 1, 2023, to December 31, 2023, to provide reasonable assurance that DigitalOcean's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE CLOUD INFRASTRUCTURE PLATFORM SYSTEM

Company Background

DigitalOcean, founded in 2012, is based in New York and provides cloud services to deploy, manage, and scale applications with the intent of removing infrastructure friction and providing predictability. The DigitalOcean cloud services provide its customers with a user interface and application programming interfaces (APIs), a robust set of features, tutorials, and a library of open-source resources.

Description of Services Provided

DigitalOcean's Cloud Infrastructure Platform allows users to build, deploy, and scale applications while leveraging the services of DigitalOcean for the handling, provisioning, and managing of infrastructure, databases, and operating systems. Furthermore, DigitalOcean's products and services are virtualized to help ensure it has the ability to scale to meet demand.

DigitalOcean provides Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Function as a service (FaaS) offerings. The various products for each of DigitalOcean's IaaS, PaaS, and FaaS offerings are described below:

IaaS Offerings

Droplets

Droplets are Linux-based virtual machines (VMs) that run on top of virtualized hardware. Each Droplet created is a new server customers can use, either standalone or as part of a larger, cloud-based infrastructure.

Volumes Block Storage

Volumes block storage are network-based block devices that provide additional data storage for Droplets. Droplets are moveable and can be resized at any time.

Spaces

Spaces is an S3-compatible object storage service that allows for storage of large amounts of data. Each Space is a bucket to store and serve files. The free, built-in Spaces content delivery network minimizes page load times, improves performance, and reduces bandwidth and infrastructure costs.

PaaS Offerings

Kubernetes

DigitalOcean Kubernetes (DOKS) is a managed Kubernetes service that allows for the deployment of Kubernetes clusters without the complexities of handling the control plane and containerized infrastructure. Clusters are compatible with standard Kubernetes toolchains and integrate natively with DigitalOcean load balancers and volume block storage.

Managed Databases

Managed Databases are a fully managed database cluster service. Using managed databases is an alternative to installing, configuring, maintaining, and securing databases manually.

App Platform

App Platform allows developers to publish code directly to DigitalOcean servers without having to manage the underlying infrastructure.

App Platform can either automatically analyze and build code from your GitHub, GitLab or public Git repositories and publish applications to the cloud or publish a container image already uploaded to DigitalOcean Container

Registry or Docker Hub. It also has lifecycle management features, vertical and horizontal scaling, push-to-deploy support, introspection and monitoring features, built-in database management and integration.

Container Registry

The DigitalOcean Container Registry (DOCR) offers the security of a private Docker image registry, with extra tool support that enables integration with Docker environments and DOKS clusters. These registries are private and co-located in the data centers where DOKS clusters are operated, to help ensure secure, stable, and performant rollout of images to your clusters.

FaaS Offerings

Functions

Functions are blocks of code configured to run on demand without the need to manage infrastructure. Functions are designed to allow end users to deploy code that can perform the same tasks as a traditional API without the requirement of configuring a server to manage the requests. Each function that an end user deploys is assigned a unique URL, which the end user can use to anonymously test the function. End users can further invoke their functions and inspect the logs and results directly from their terminal.

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

DigitalOcean designs its processes and procedures related to the Cloud Infrastructure Platform system to meet its business objectives for the DigitalOcean cloud offerings. Those objectives are based on service commitments that the organization makes to user entities, the laws and regulations that govern the provisioning of its cloud offerings, and the financial, operational, and compliance requirements that the organization has established for the services. The Cloud Infrastructure Platform system is subject to the relevant regulatory, industry, and data security requirements in which DigitalOcean operates.

The security and availability commitments to user entities are documented and communicated to customers in service agreements and company policies. The principal security commitments are standardized and include, but are not limited to, the following:

- Maintain written information security policies that define security controls based on DigitalOcean's assessment of risk to personal data that it processes and its information systems.
- Employ security technologies and measures designed to protect information from unauthorized access, use, or disclosure of DigitalOcean management network and assets.
- Encrypt customer data in transit between the DigitalOcean's management network and infrastructure.
- Conduct a variety of regular internal and external audits that are inclusive of security operations.
- Grant access to DigitalOcean assets based on least-privileges principles.
- Utilize logging and monitoring tools to analyze service, user, and security events.
- Maintain infrastructure within multiple availability zones in geographic regions physically separated from one another of DigitalOcean management network and assets.
- Maintain monitoring mechanisms over infrastructure to check server performance, data, traffic, and load capacity and to detect and route issues experienced by hosts in real time and employ orchestration tooling that has the ability to regenerate hosts.

Additionally, DigitalOcean provides service level agreements (SLAs) for the following products, which display its commitment to deliver a high level of availability for customers products, including Droplets, Volumes Block Storage, and Kubernetes Control Plane.

- Droplets: The DigitalOcean Droplet service provides a 99.99% uptime SLA per month.
- Block Storage: The DigitalOcean Volumes Block Storage service provides 99.99% uptime SLA per month.
- Kubernetes: The DOKS service provides 99.95% uptime SLA per month for the control plane when high availability (HA) is enabled for such clusters.

DigitalOcean establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. These requirements are communicated in DigitalOcean's information security policies, service agreements, and training documentation and include, but are not limited to, the following:

- Information security policies are documented and made available to workforce members.
- Enforcing authentication requirements for in-scope systems.
- Requiring formal approval by a workforce member's direct supervisor for access provisioning requests and revoking access to in-scope systems upon termination of personnel.
- Encrypting web communication sessions using the TLS encryption protocol.
- Collecting data from in-scope systems and production hosts to analyze system performance, resource utilization, and potential security vulnerabilities.
- Utilizing a vulnerability scanning tool and bug bounty program to identify and mitigate system vulnerabilities.
- Penetration tests are performed by third-party vendors annually to identify threats from sources outside the boundaries of the system and assess their potential impact to the system.

In accordance with DigitalOcean's 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 all system users, in each individual case.

Infrastructure and Software

The infrastructure supporting the DigitalOcean Cloud Infrastructure Platform production systems are hosted from multiple regional facilities ("regions") that reside in facilities that are managed by various collocated data centers. Available regions are located in the United States, United Kingdom, Singapore, Netherlands, Canada, India, Australia, and Germany. DigitalOcean offers an IaaS platform for software developers and provides a PaaS offering for application development. The production systems consist of multi-tier virtualized architecture comprised of web and database servers, storage and content delivery systems, and network and application monitoring tools. A firewall system is also used to restrict information from unauthorized sources and prevent unauthorized network connections.

As part of the cloud computing and center data hosting services, the collocated data centers are responsible for providing the physical safeguarding of the IT infrastructure to help ensure that unauthorized access to the IT infrastructure does not occur, as well as providing environmental safeguards (e.g., uninterrupted power supply, temperature control, fire suppression, etc.) against certain environmental threats.

People

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.

- Security and Privacy – responsible for creating policies, standards, and procedures that relate to and enforce the risk, governance, privacy, and compliance posture of the organization.
- CloudOps / Product – responsible for designing, building, and maintaining products while adhering to data protection, privacy, and security standards.
- Data Center Operations – responsible for access provisioning and deprovisioning requests made to collocated data center providers.
- IT – responsible for management of employee endpoints and employee account lifecycle management.
- People Operations – responsible for talent acquisition, talent strategy, and total rewards.
- Legal – responsible for general counsel operations and external facing policies and terms.
- Customer Success and Support – responsible for troubleshooting and resolving customer software usage issues.

Procedures

HR and Training

DigitalOcean's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, disciplinary activities, and termination. Established pre-hire screening procedures are performed for new personnel based on DigitalOcean's hiring policies and procedures. Personnel are provided with information security policies, the acceptable use policy, and an employee handbook so that the responsibility and accountability for upholding business values and organizational policies / procedures is clear.

Access, Authentication, and Authorization

Access to DigitalOcean system information, including confidential information, is protected by authentication and authorization mechanisms, which are defined in documented policies and procedures to help guide personnel in logical security requirements. The documented policies and procedures provide guidance to personnel in information security practices such as password requirements, the acceptable use of company resources, access provisioning, and access removal.

Access Requests and Access Revocation

Access provisioning and deprovisioning procedures are formalized. A ticketing system is used to document, manage, and track access provisioning requests and access removal requests when an employee or contractor, collectively referred to as workforce members, is hired or terminated.

System Security and Monitoring

Logging and monitoring systems are in place to analyze, identify, and report possible or actual security vulnerabilities or malicious activity on production hosts to the security team. The logging and monitoring systems are configured to alert CloudOps or security team personnel of issues that meet and / or exceed predefined thresholds, at which point the identified findings are investigated and corrective actions are taken, as necessary.

Documented vulnerability management policies and procedures are in place at DigitalOcean to guide users in discovering vulnerabilities in the entity's assets and correcting them to help keep DigitalOcean's services, software, infrastructure, operating systems, and applications from being exploited. Furthermore, an independent security professional performs a penetration test on an annual basis to identify potential security vulnerabilities. A bug bounty program is also used to identify and report vulnerabilities and threats. Detected security vulnerabilities are triaged by the security team and monitored through resolution using the ticketing system.

Encryption and Anti-malware

Web communication sessions are encrypted and encrypted VPNs are used for remote access to help ensure the security and integrity of the data passing over the public network.

Incident Response

Documented incident response policies and procedures are in place, managed by the security incident response team, and made available to internal workforce members via the internal site detailing how an incident is handled through identifying, containing, remediating, and documenting security incidents. A ticketing system is utilized by the security incident response team to track and manage security incidents from response through to resolution.

Change Management

DigitalOcean has implemented policies and procedures to guide personnel in the request, documentation, and approval of DigitalOcean products and services to be added and subsequently managed within the software development platform. DigitalOcean utilizes an automated deployment tool to support a continuous integration / continuous deployment (CI / CD) model for managing infrastructure as code. A production pipeline is configured within the automated deployment tool for each added product or service as a component of the Operational Acceptance Review (OAR) process. Once a pipeline build is created within the automated deployment tool, changes made within the software development platform undergo the configured steps included in the build.

The ability to make such changes to pipeline builds for products and services with a defined severity level of one or two is restricted to authorized personnel. Additionally, pipeline builds are configured to require validation testing for changes to existing pipeline builds within the automated deployment tool to help ensure that alterations will not negatively impact the build and deployment of the infrastructure changes.

Business Continuity and Disaster Recovery

DigitalOcean service team owners maintain business continuity and disaster recovery plans that detail how managed services with customer-facing environments sustain availability in the event of a single datacenter failure. The business continuity and disaster recovery plans managed by service team owners with customer-facing environments are documented, assessed, and tested annually.

Media Disposal / Destruction

Asset removal and disposal policies are in place to guide personnel in the disposal of assets to help ensure data and software is unrecoverable prior to decommissioning physical assets. Third parties are contracted to destroy physical hardware maintained at collocated data centers prior to asset disposal. Contracted third parties provide a certificate of destruction upon completion of destruction services for physical production assets.

Vendor Management

Security management considers the identification and assessment of risks and mitigation activities associated with vendors and business partners during the risk assessment and mitigation activities. Furthermore, security personnel perform due diligence on vendors that could potentially store or access customer data by reviewing the vendor's third-party compliance reports or requiring a completed security questionnaire as a component of the onboarding process. DigitalOcean's security commitments and obligations, including those made the responsibility of DigitalOcean's vendors and business partners are further documented and communicated through the terms of service made available via the company's website. Ongoing relationships with vendors are evaluated during the contract renewal process, just as during onboarding.

Access to Collocated Facilities

New and modified workforce member access to collocated data centers is required to be documented within the ticketing system upon communication of the request to the respective collocated data center. Physical access termination requests for workforce members are documented in the ticketing system as a component of the termination process.

Data

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

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Droplet Metadata	Droplet metadata can be accessed using the client URL command line tool with a special static IP address.	Restricted
Droplet User Data	User data is provided to a droplet when it's created and cannot be modified thereafter. The data can be accessed using the client URL command line tool.	
Stored Files	Files are stored in buckets, which are used as part of the spaces object storage service. The data stored in the buckets is accessible by authorized user personnel controlled via restricted access keys.	
DOKS Cluster Metrics	DOKS includes metrics to provide insight into the health of a user's Kubernetes clusters and deployments. Metric data is made available via the user's DigitalOcean overview page that is accessible by authorized user personnel.	
App Platform Logs	Logs are captures of the activity related to the user's application. Logs are available to authorized user personnel via the control plane or from the command line.	
Infrastructure, Service, and Secondary Program Logs	Available to users via database storage for which access is restricted to authorized user personnel.	

Subservice Organizations

The data center hosting services provided by collocated data centers were not included within the scope of this examination.

The following table presents the applicable trust services criteria that are intended to be met by controls at collocated data centers, alone or in combination with controls at DigitalOcean, and the types of controls expected to be implemented at collocated data centers to achieve DigitalOcean's principal service commitments and system requirements based on the applicable trust services criteria.

Control Activities Expected to be Implemented by Collocated Data Centers	Applicable Trust Services Criteria
Collocated data centers are responsible for implementing controls that ensure physical access to data center facilities, backup data, and other system components such as virtual systems and servers is restricted.	CC6.4, CC6.5
Collocated data centers are responsible for implementing controls that ensure the data center facilities are equipped with physical and environmental security safeguards.	A1.2

Complementary Controls at User Entities

DigitalOcean's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the applicable trust services criteria related to DigitalOcean's services to be solely achieved by DigitalOcean's control procedures. Accordingly, user entities, in conjunction with the Cloud Infrastructure Platform system and related services, should establish their own internal controls or procedures to complement those of DigitalOcean.

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

#	Complementary User Entity Control
1.	User entities are responsible for ensuring the supervision, management, and control of the use of DigitalOcean's services by their personnel.
2.	User entities are responsible for understanding and complying with their contractual obligations to DigitalOcean.
3.	User entities are responsible for immediately notifying DigitalOcean of any actual or suspected security breaches, including compromised user accounts.
4.	User entities are responsible for the security and privacy of data while using DigitalOcean products.
5.	User entities are responsible for establishing and maintaining strong passwords and secure single sign-on and/or multi-factor authentication credentials to the DigitalOcean user interface.
6.	User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize DigitalOcean services.
7.	User entities are responsible for developing their own data backup procedures that address the inability to access or utilize DigitalOcean services.
8.	User entities are responsible for ensuring the supervision, management, and control of the use of DigitalOcean's services by their personnel.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security and availability are applicable to the Cloud Infrastructure Platform system.