Nutanix, Inc.

System and Organization Controls (SOC) 3

Report on Nutanix, Inc.’s Assertion Related to Its Nutanix Cloud Manager Security Central System Relevant to Security, Availability, and Confidentiality

Throughout the Period
November 1, 2023 to October 31, 2024

Contents

I. Independent Service Auditor's Report on a SOC 3 Examination

Tel: 617-422-0700
Fax: 617-422-0909
www.bdo.com

One International Place
Boston, MA 02110

Independent Service Auditor's Report on a SOC 3 Examination

To the Management of
Nutanix, Inc.
San Jose, California

Scope

We have examined Nutanix, Inc.'s (Nutanix or service organization) accompanying assertion titled *Assertion of Nutanix, Inc.'s Management* (assertion) that the controls within Nutanix's Nutanix Cloud Manager Security Central System (the System) were effective throughout the period November 1, 2023 to October 31, 2024 to provide reasonable assurance that Nutanix's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) *s*et forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Nutanix uses subservice organizations to perform certain activities. A list of these subservice organizations and the activities performed is provided in Attachment A. The assertion indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nutanix, to achieve Nutanix's service commitments and system requirements based on the applicable trust services criteria. Nutanix's description of the boundaries of the System in Attachment A presents the types of complementary subservice organization controls assumed in the design of Nutanix's controls but 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

Nutanix 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 Nutanix's service commitments and system requirements were achieved. Nutanix has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, Nutanix 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 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 November 1, 2023 to October 31, 2024 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the System and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve the service organization'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 Nutanix'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.

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the operating effectiveness of controls is subject to the risks 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 Nutanix's system were effective throughout the period November 1, 2023 to October 31, 2024 to provide reasonable assurance that Nutanix's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Restricted Use

This report is intended solely for the information and use of Nutanix, user entities of Nutanix's system during some or all of the period November 1, 2023 to October 31, 2024, business partners of Nutanix subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.

- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

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

BDO USA, P.C.

December 16, 2024

II. Assertion of Nutanix, Inc.'s Management

Assertion of Nutanix, Inc.'s Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Nutanix, Inc.'s (Nutanix or the service organization) Nutanix Cloud Manager Security Central System (the System) throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Nutanix's service commitments and system requirements relevant to security, availability, and confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the System is presented in Attachment A, *Nutanix, Inc.'s Description of the Boundaries of Its Nutanix Cloud Manager Security Central System* and identified the aspects of the System covered by our assertion.

Nutanix uses subservice organizations to perform certain activities. A list of these subservice organizations and the activities performed is provided in Attachment A. The description of the boundaries of the System in Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nutanix, to achieve Nutanix's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the System presents the types of complementary subservice organization controls assumed in the design of Nutanix's controls. The description of the boundaries of the System does not extend to the actual controls at the subservice organizations.

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 Nutanix's service commitments and system requirements were achieved based on the trust services criteria relevant to the 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*. Nutanix's objectives for the System in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

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 were 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 Nutanix's service commitments and system requirements were achieved based on the applicable trust services criteria.

Nutanix, Inc.

December 16, 2024

Attachment A — Nutanix, Inc.'s Description of the Boundaries of Its Nutanix Cloud Manager Security Central System

Attachment A — Nutanix, Inc.'s Description of the Boundaries of Its Nutanix Cloud Manager Security Central System

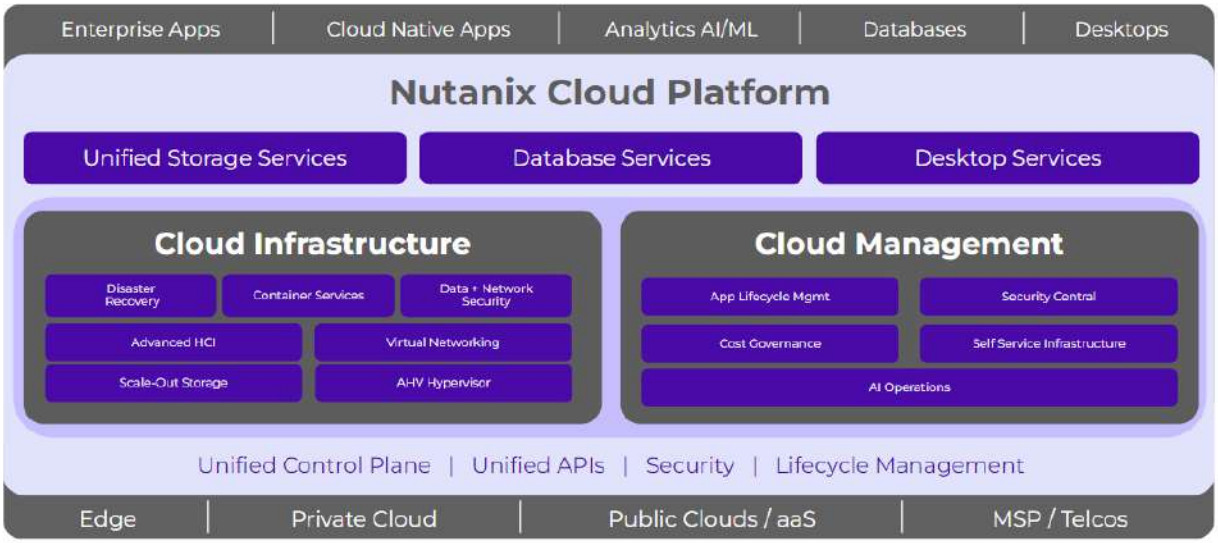
Company Background

Nutanix, Inc. provides a cloud platform, called the Nutanix Cloud Platform™, that consists of software solutions and cloud services that power a customer's IT infrastructure. Nutanix's solutions are designed to deliver a consistent cloud operating model across edge, private-, hybrid-, and multicloud environments for applications and data. Nutanix's solutions allow organizations to more simply move their workloads, including enterprise applications, high-performance databases, container-based modern applications, and analytics applications, between on-premises and public clouds.

Services Provided

Nutanix Cloud Platform

Nutanix Enterprise Cloud melds private, public, and distributed cloud operating environments and provides a single point of control to manage IT infrastructure and applications at any scale.



Nutanix Cloud Services

The Nutanix Cloud Services provide a native extension to the Nutanix Cloud Platform core infrastructure services, delivering integrated public cloud operations that can be quickly provisioned and automatically configured. The Nutanix Cloud Services include Nutanix Cloud Clusters (NC2)™ on AWS, Nutanix Cloud Clusters (NC2)™ on Azure, Nutanix Insights™, Nutanix Cloud Manager (NCM) Self-Service™, Nutanix Data Lens™, Nutanix Disaster Recovery as a Service (DRaaS)™, Nutanix Cloud Manager (NCM) Cost Governance™, and Nutanix Cloud Manager (NCM) Security Central™. The suite of Nutanix Cloud Services is summarized below.

- *Nutanix Cloud Clusters (NC2) on AWS* — The NC2 on AWS system powers an industry-first hybrid multi-cloud platform with native networking integration to AWS public clouds to

enable organizations to benefit from the flexibility, simplicity, and cost efficiency of running applications in private or public clouds.

- *Nutanix Cloud Clusters (NC2) on Azure*— The NC2 on Azure system powers an industry-first hybrid multi-cloud platform with native networking integration to Azure public clouds to enable organizations to benefit from the flexibility, simplicity, and cost efficiency of running applications in private or public clouds.
- *Nutanix Insights* — Nutanix Insights is a predictive health and automated support offering to enable support automation for the IT administrator, facilitating simplification of support ticket management.
- *NCM Self-Service (formerly Calm)* — NCM's hosted Self-Service is an application orchestration service that delivers infrastructure and application management for the IT administrator to manage the internal end user, with the ability for the IT administrator to start, stop, and scale an application based on business requirements and internal-end-roles.
- *Nutanix Data Lens* — Nutanix Data Lens provides a cloud-hosted analytics and monitoring service for Nutanix Files file servers. Nutanix Data Lens functions on a global level, in a cluster-neutral environment, without being tied to a single Nutanix cluster.
- *Nutanix Disaster Recovery as a Service (DRaaS) (formerly Xi Leap)* — Nutanix DRaaS protects applications and data in a customer's Nutanix environment without the need to purchase and maintain a separate infrastructure stack. By utilizing the customer's existing Nutanix Cloud Platform infrastructure services, Nutanix DRaaS eliminates complexity across environments. Customers are able to select any virtual machine (VM) and set up the desired protection policy (i.e., replication schedule and recovery plan) from within the Nutanix management console. VMs are replicated in the background and available for retrieval of applications and data in a public cloud environment in the event of a customer site failure. Nutanix DRaaS also enables partial failover of applications for server maintenance or during rack failures. Network connectivity and common management between environments are preserved, allowing customers to manage the source and target sites as a single environment. In addition, Nutanix DRaaS provides testing functionality, enabling customers to routinely examine their disaster recovery readiness. Network-isolated testing environments are available to test the entire recovery process without impact to the primary environment.
- *NCM Cost Governance (Cost Governance) (formerly Beam)* — NCM Cost Governance is a multi-cloud optimization service that provides organizations with deep visibility and rich analytics detailing cloud consumption patterns. NCM Cost Governance delivers one-click cost optimization across a customer's cloud environment.
- *NCM Security Central (Security Central) (formerly Flow Security Central)* — NCM Security Central is a Nutanix multi-cloud governance service that provides organizations with visibility, optimization, and automated control needed to enforce cloud governance controls across the Nutanix Cloud Platform core infrastructure, AWS™, and Microsoft Azure™. NCM Security Central enables customers to directly enforce policies that improve cloud security from a single "pane of glass."

Scope and Boundaries of the System

This is a SOC 3 report and includes a description of the boundaries of Nutanix's NCM Security Central System and the controls in place to meet the criteria for security, availability, and confidentiality

set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*, throughout the period November 1, 2023 to October 31, 2024 which may be relevant to the users of the System. It does not encompass all aspects of the services provided or procedures followed for other activities performed by Nutanix.

Nutanix uses subservice organizations to perform certain services. A list of these subservice organizations and the services performed is provided in the following table. The description of the boundaries of the System does not extend to the actual controls at the subservice organizations.

Subservice Organization	Services Performed
Amazon Web Services, Inc. (AWS)	To provide hosting of the production servers and workload instances.
Okta, Inc. (Okta)	To provide identity management services.

System Incidents

A system incident is an incident that leads to the loss of, or disruption to, operations, services, or functions and results in Nutanix's failure to achieve its service commitments or system requirements. Such an occurrence may arise from a security event, security incident, failure to comply with applicable laws and regulations, error, or other means. In determining whether a system incident occurred resulting in Nutanix's failure to achieve one or more of its service commitments or system requirements, considerations may include, but are not limited to, the following:

- Whether the occurrence resulted from one or more controls that were not suitably designed or operating effectively.
- Whether public disclosure of the occurrence was required (or is likely to be required) by cybersecurity laws or regulations.
- Whether the occurrence had a material effect on the service organization's financial position or results of operations and required disclosure in a financial statement filing.
- Whether the occurrence resulted in sanctions by any legal or regulatory agency.
- Whether the occurrence resulted in the service organization's withdrawal from material markets or cancellation of material contracts.

Incidents and events relevant to Nutanix's service commitments and system requirements based on the applicable trust services criteria are important in monitoring, identifying, and evaluating if a system incident has occurred; however, incidents and events relevant to Nutanix's service commitments and system requirements based on the applicable trust services criteria do not always rise to the level of a system incident. The evaluation of an incident or event relevant to Nutanix's service commitments and system requirements based on the applicable trust services criteria will make that determination.

Nutanix did not identify any system incidents that occurred during the period November 1, 2023 to October 31, 2024 resulting in Nutanix's failure to achieve one or more of its service commitments or system requirements based on these considerations.

Significant Changes to the System During the Period

The environment platform has been enhanced to improve scalability, automation, and security by introducing several new components. Kubernetes (K8s) has replaced the previous system for container orchestration and is now used for service discovery, enabling seamless microservice communication. Deployments are automated with Argo CD, utilizing a GitOps model for continuous integration and delivery. Additionally, Kops has been adopted for Kubernetes cluster management. Istio has been introduced to manage the service mesh, providing mutual Transport Layer Security (mTLS) for secure service-to-service authentication and advanced traffic control. An API Gateway now handles external traffic, offering centralized routing, security, and application programming interface (API) management. These updates collectively enhance the platform's efficiency, security, and scalability.

Components of the System Used to Provide the Services

Infrastructure

The Security Central System's production environment is deployed on the AWS infrastructure in its own virtual private cloud (VPC) with access controls for network and application-level security and is protected using a web application firewall service. Security Central System back-end services such as databases, logs, etc., are isolated into separate private networks for enhanced protection. Data sent to/from the Security Central System is transmitted securely using Transport Layer Security (TLS) and Hypertext Transfer Protocol Secure (HTTPS). Security Central System customers are not required to open any custom ports from their network or cloud. The Security Central System is secured with authentication, authorization, and tampering protection.

Software

Teleport

In the Security Central System, the engineers do not have persistent access to sensitive data or persistent access to perform high-risk operations. Teleport is the service that facilitates management's approval for requests of temporary privileged access.

Customer Portal (https://my.nutanix.com)

Among other purposes, the my.nutanix.com portal provides Security Central System customers with identity services, billing and payment services, and support infrastructure.

Vault

HashiCorp Vault is a secrets (passwords, API keys, certificates, etc.) management tool. The Security Central System uses it to store sensitive credentials as well as generate dynamic short-lived credentials for entities such as AWS, Postgres, Public Key Infrastructure certificates, etc. Vault's sealing and unsealing mechanism is offloaded to the AWS Key Management Service (KMS), which uses FIPS 140-2 validated hardware security modules. Communication among Vault servers is over TLS requiring a Vault token.

Telegraf

Telegraf is an open-source agent that can collect metrics across various domains and dimensions. The Security Central System runs Telegraf on its AWS Elastic Compute Cloud (EC2) instances that emit system metrics.

Nessus

Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services, and other network resources. After every scan, it provides a detailed report of vulnerabilities found and a comprehensive summary on how to remediate or mitigate them.

AWS GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts and workloads. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and Domain Name System logs.

Clutch

Clutch is an internal single-pane for management and access of Nutanix engineering teams that consume communications platform as a service (CPaaS). It provides modules with full-fledged Kubernetes support through which teams can manage their applications and workloads. It provides robust insights, auditing, alerting, and role-based access control (RBAC) for engineering teams and their resources. It also offers a software development kit (SDK), which is used to integrate Clutch with continuous integration/continuous delivery (CI/CD) pipelines and other use cases involving management of workloads. Besides Kubernetes, Clutch has modules for secrets management, scoped infrastructure access, approval systems for business processes, export/import of resources across different setups, etc.

Other Supporting Software and Tools

Other tools utilized in supporting the Security Central System:

- *Okta* — Multifactor authentication (MFA) solution
- *Ansible* — Configuration management tool
- *Kubernetes* — Container scheduling and orchestration
- *AWS Simple Storage Service (S3)* — Long-term report storage
- *Kibana* — File integrity change logging tool
- *Slack* — Automated alerting service
- *Jira* — Ticketing/tracking system
- *ServiceNow* — Ticketing/tracking system
- *AWS Config* — Asset management system

- *Akamai* — Distributed denial-of-service (DDoS) protection solution
- *Opsgenie* — Automated alerting services
- *Uptime* — Alerting service
- *Argo CD* — GitOps continuous delivery tool for Kubernetes
- *Kops* — Managing Kubernetes infra operations
- *Kubernetes (K8)* — Open-source system for automating deployment, scaling, and management of containerized applications
- *Apache Druid* — Column-oriented, open-source, distributed data store
- *Apache Pulsar* — All-in-one messaging and streaming platform
- *Curator* — Elasticsearch index management, backup, and restore
- *Reloader* — Manages Pod restarts for changes in ConfigMap and secrets
- *OpenSearch* — Search and analytics suite
- *Elasticsearch* — Database for Temporal
- *Temporal* — Open source workflow orchestration platform that maintains an application's state at scale and ensures correctness regardless of what's failing
- *Grafana* — Multi-platform open source analytics and interactive visualization web application that provides charts, graphs, and alerts for the web when connected to supported data sources

People

Personnel who are involved in the definition, development, operation, or support of the Security Central System are grouped into the following primary areas:

Engineering and Technical Operations

Members of the Engineering and Technical Operations team are organized around product components and are responsible for product development, bug fixes, and operations support. They are also responsible for support of the running platform instances, customer support, monitoring and alerting systems, internal automation and tools, and information security.

Security and Compliance

Security and Compliance teams are groups within the engineering organization dedicated to the build and operation of leveraged security services. These services serve to constantly assess, prevent, detect, and respond to attacks on Nutanix cloud services. In addition, the teams are responsible for defining and driving the security development life cycle, developing engineering-specific security training, performing threat-model reviews, performing penetration tests, and building security tools. The Compliance team manages security, availability, and confidentiality compliance efforts for Nutanix products and cloud services.

Business Operations

Business Operations is responsible for corporate IT, human resources (HR), sales, and finance activities. These responsibilities include employee additions, moves and changes, overall corporate security oversight, and customer billing.

Customer Support

Nutanix Customer Support (https://www.nutanix.com/support-services) is a team of global support professionals who not only support Nutanix products and services, but also provide consulting services and training and certification.

Processes and Procedures

Management has developed and communicated to internal and external parties its policies, procedures, and guidelines that describe safeguards and requirements to protect against unauthorized access to System resources. Each policy is assigned an owner and is reviewed and updated at least annually or as necessitated by process changes. Organization-wide policies and procedures are located on Nutanix's intranet sites, and employees are expected to adhere to those policies and procedures in the delivery of the Security Central System service commitments. Formal policies and procedures include:

Nutanix Acceptable Use Policy

The purpose of this policy is to outline the acceptable use of computing resources and is applicable to Nutanix employees and contractors.

Information Security Management and Privacy Information Management Manual

This manual outlines how Nutanix manages and mitigates security risks to safeguard the confidentiality, integrity, availability, and privacy of Nutanix information and technological assets.

Security Incident Management Policy

The purpose of this policy is to facilitate a consistent and effective approach to the management of information security incidents, including communication on security weaknesses and events.

Systems Operation Policy

The purpose of this policy is to outline system operations requirements for Nutanix's computing resources.

Access Control Policy

The purpose of this policy is to provide guidance to relevant Nutanix personnel in configuring and implementing appropriate access controls for systems and services within Security Central environments.

Change Management Policy

The purpose of this policy is to provide guidance and methodology for change management practices, including, but not limited to, configuration changes made to the production systems, infrastructure, and applications.

Cryptographic Policy

The purpose of this policy is to define the requirements regarding the use of cryptographic protections for the assets of Nutanix's computing resources.

Security Awareness and Training Policy

The purpose of this policy is to establish methodologies and processes to provide security awareness and training to allow the organization to achieve security goals that help the workforce understand and adhere to Nutanix security practices.

Security Patch Management Procedure

The purpose of this procedure is to establish standards and guidelines for security patch management.

Information Classification Policy

The purpose of this policy is to outline the levels of information classification at Nutanix to protect the employee and Nutanix from unauthorized disclosure of information due to improper handling.

Data

Nutanix has defined data classification around four categories. These categories include customer data, personally identifiable information and end user identifiable information, administration sensitive data, and system metadata and operations data.

- *Customer Data*
    - Customer backups, universal VMs, users and role membership, customer-owned security information (certificates, encryption keys, Secure Socket Shell [SSH] keys, user credentials).
- *Personally Identifiable Information (PII) and End-User Identifiable Information (EUII)*
    - Customer names, email addresses, IP addresses that could identify an individual person, phone numbers, and physical addresses.
- *Administration Sensitive Data*
    - SSL certificates with private keys, data-at-rest encryption keys, SSH keys to the Security Central infrastructure, and auditing data.

- *System Metadata and Operations Data*
    - Customer IDs, customer VM names, role names, Security Central cluster information, service logs (not containing customer data, service configuration [without administration sensitive data]), IP addresses that only identify a company, or company address pool (and not an individual person).

Access to Customer Data

The Security Central System does not access customer data, and protection of that data remains the responsibility of the customer. The Security Central System accesses only the metadata of the customer's cloud accounts for the purpose of delivering the optimization service, and access to that metadata by the Security Central service is controlled by the customer.

Complementary Subservice Organization Controls

In some instances, a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements were achieved without the subservice organizations performing certain activities in a defined manner. Such activities are referred to as complementary subservice organization controls (CSOCs). The following CSOCs are those controls that Nutanix's management assumed, in the design of the System, would be implemented by a subservice organization and are necessary, in combination with controls at Nutanix, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

Number	CSOC	Applicable Criteria
Amazon Web Services, Inc. and Okta, Inc.		
1.	Subservice organizations are responsible for having controls in place to identify potential threats that would impair the system and communicate those to Nutanix immediately.	CC4.1
2.	Subservice organizations are responsible for having controls in place to limit and restrict access to system-designated resources to only authorized personnel.	CC6.1
3.	Subservice organizations are responsible for having controls in place to limit and restrict access to facilities housing the system to only authorized personnel.	CC6.4
4.	Subservice organizations are responsible for having controls in place to automate the recovery of production hosts when necessary to maintain the availability of the system.	CC7.5
5.	Subservice organizations are responsible for having controls in place to monitor system processing capacity and implement additional capacity when necessary to maintain the availability of the system.	A1.1

Number	CSOC	Applicable Criteria
6.	Subservice organizations are responsible for having controls in place to install environmental protections, which include, but are not limited to: • Cooling systems. • Battery and generator backup in the event of power failure. • Smoke detectors. • Fire suppression systems. • Water detection.	A1.2
Amazon Web Services, Inc.		
7.	Subservice organization is responsible for discontinuing logical and physical protections over physical assets only after the ability to read or recover data from those assets has been diminished.	CC6.5

User Entity Responsibilities

User entities must perform specific activities in order to benefit from Nutanix's services. These activities may affect the user entity's ability to effectively use Nutanix's services but do not affect the ability of Nutanix to achieve its service commitments and system requirements. These activities may be specified in agreements between user entities and Nutanix, user manuals, and/or other communications. These activities are referred to as user entity responsibilities (UERs).

UERs are listed in the following table. They are the responsibility of the user entities of the System and are expected to be in operation at user entities to complement Nutanix's controls. The list of UERs does not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at user entities.

Number	UER
1.	Customers are responsible for notifying Nutanix of any changes to account owner designees in a timely manner.
2.	Customers are responsible for administering access to their Security Central System account.
3.	Customers are responsible for secure configuration and operations of their own cloud environments, including cloud provider accounts.

Attachment B — Principal Service Commitments and System Requirements

Attachment B — Principal Service Commitments and System Requirements

Nutanix designs its processes and procedures related to the Security Central System to meet its business objectives. These objectives are based on the service commitments that Nutanix makes to customers and other relevant user entities, and the operational and compliance requirements that Nutanix has established for the System. Service commitments to customers and other relevant user entities are documented and communicated in master agreements and supplemental terms agreements, as well as in the description of the service offering provided on Nutanix's website, in its marketing materials, and within its customer-facing web portal.

Nutanix formalizes the security, availability, and confidentiality service commitments in the form of two service-level agreements (SLAs):

- *Cloud Services Support Agreement*

  https://www.nutanix.com/support-services/product-support/product-support-programs (refer to the "Cloud Services Support" section)

- *Cloud Services Availability SLA*

  https://www.nutanix.com/content/dam/nutanix/documents/services/Nutanix%20Service%20Level%20Agreement.pdf

Nutanix establishes operational and compliance requirements that support the achievement of security, availability, and confidentiality commitments, compliance with relevant laws and regulations, and compliance with other System design requirements. Such requirements are communicated via Nutanix's System policies and procedures, System design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the Security Central System is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.

In addition to these policies, standard operating procedures have been documented to carry out specific manual and automated processes required for the ongoing development and operation of the Security Central System.