NUTANIX™

YOUR ENTERPRISE CLOUD

System and Organization Controls (SOC) 3

Report on Nutanix's Xi Beam System Relevant to Security, Availability and Confidentiality

For the Period November 1, 2019 to October 31, 2020

NUTANIX™

YOUR ENTERPRISE CLOUD

TABLE OF CONTENTS

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Management of Nutanix

Scope

We have examined Nutanix's accompanying assertion titled "Assertion of Nutanix Management" (assertion) that the controls within Nutanix's Xi Beam system (system) were effective throughout the period November 1, 2019, to October 31, 2020, 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) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

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 service 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 system 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 Nutanix's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Nutanix'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 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 the service organization'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 Nutanix's Xi Beam system were effective throughout the period November 1, 2019, to October 31, 2020, 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.

Burke & Associates CPAs LLP

Tampa, FL
January 15, 2021

YOUR ENTERPRISE CLOUD

ASSERTION OF NUTANIX MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Nutanix's Xi Beam system (system) throughout the period November 1, 2019, to October 31, 2020, to provide reasonable assurance that Nutanix's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment A 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, 2019, to October 31, 2020, 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) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (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 are achieved.

We assert that the controls within the system were effective throughout the period November 1, 2019, to October 31, 2020, to provide reasonable assurance that Nutanix's service commitments and system requirements were achieved based on the applicable trust services criteria.

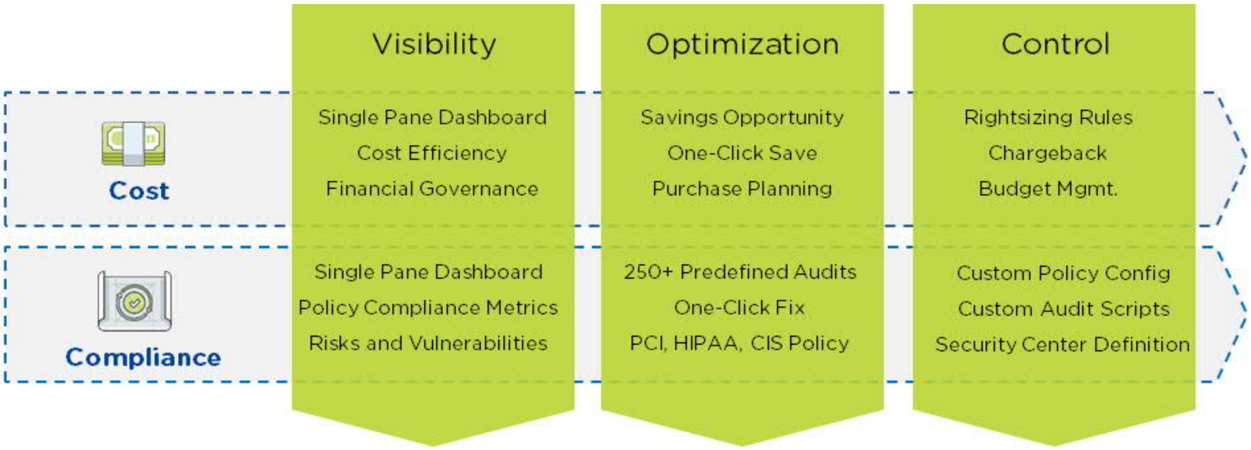
Attachment A: Xi Beam System

The scope of this report is the Xi Beam system, which includes the processes, infrastructure and software that store, access, operate, or transmit customer data. Specifically, the system environment includes production servers, test servers, as well as personnel that support the Xi Beam system.

Xi Beam is a Nutanix multi-cloud governance service that provides organizations with the necessary visibility, optimization, and automated control needed to enforce complete cloud governance across Nutanix's Enterprise Cloud, Amazon Web Services, and Microsoft's Azure Cloud. Xi Beam enables customers to visualize cloud consumption across both public and private clouds, directly enforce policies that improve cloud security, and control cloud costs, all from a single "pane of glass."

- Xi Beam uses machine intelligence to continuously provide cloud optimization recommendations to customers. Xi Beam proactively identifies idle and underutilized cloud resources and delivers specific resource right-sizing and purchase recommendations that provide opportunities for cost savings. Customers can right-size resources with just one click.
- Xi Beam provides visibility to customer security compliance efforts by automating various out-of-the-box and custom audit checks that help to detect and fix cloud security issues. Xi Beam can perform numerous audit checks to provide insight to a customer's compliance status which can then be used by customers to assess where their security in reference to industry standards, regulatory policies and cloud security best practices.

Xi Beam is supported by Nutanix's Customer Support organization. Nutanix Support professionals carry industry certifications in virtualization, networking, Unix administration and various enterprise applications.



	Visibility	Optimization	Control
Cost	Single Pane Dashboard Cost Efficiency Financial Governance	Savings Opportunity One-Click Save Purchase Planning	Rightsizing Rules Chargeback Budget Mgmt.
Compliance	Single Pane Dashboard Policy Compliance Metrics Risks and Vulnerabilities	250+ Predefined Audits One-Click Fix PCI, HIPAA, CIS Policy	Custom Policy Config Custom Audit Scripts Security Center Definition

The Xi Beam system provides two modules for optimizing a customer's cloud presence: one for Cost Governance and the other for Security Compliance. These elements are developed by the Nutanix Xi Beam team and are hosted in an AWS virtual private cloud.

Infrastructure

Xi Beam'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. Xi Beam back end services such as databases, logs, etc., are isolated into separate private networks for enhanced protection. Data sent to/from the Xi Beam system is transmitted securely using TLS and HTTPS. Xi Beam customers are not required to open any custom ports from their network or cloud. The Xi Beam application is secured with authentication, authorization, and tampering protection.

Primary Software

Teleport

In the Xi Beam 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.

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

Among other purposes, the my.nutanix.com portal provides Xi Beam customers with Identity Services, Billing and Payment Services, and Support Infrastructure.

Vault

Hashicorp Vault is a secrets (e.g. passwords, API keys, certificates, etc.) management tool. Xi Beam uses it to store sensitive credentials as well as generate dynamic short-lived credentials for entities such as AWS, Postgres, PKI certificates, etc. Vault's sealing/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. Xi Beam runs Telegraf on Xi Beam's AWS Elastic Compute Cloud (EC2) instances that emit system metrics.

Wazuh

Wazuh is an open-source security platform that performs real-time security threat detection, incident response, and compliance. Xi Beam uses many Wazuh features such as Security Analytics, Intrusion Detection, Log Data Analysis, File Integrity Monitoring, Vulnerability Detection, Configuration Assessment, Incident Response, Regulatory Compliance, Cloud and Container Security.

Xi Beam runs Wazuh agents on AWS EC2 servers, which stream logs to a central Wazuh manager with alerts configured to send notifications in real-time.

InsightVM

InsightVM is a licensed product from Rapid7 and is used for Vulnerability Assessment. InsightVM constantly receives signature updates as well as provides capabilities to detect zero-day vulnerabilities. After every scan, it provides a detailed report of vulnerabilities found and a comprehensive summary on how to fix/mitigate them.

AWS Guard-Duty

Amazon Guard Duty 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. Guard Duty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs.

Other tools utilized in supporting the Xi Beam system:

- Okta – Serves as the multi factor authentication (MFA) solution
- Veracode – Static application security testing tool
- Black Duck – Secure code development scanner
- Ansible – Configuration management tool
- Consul – Secure networking solution
- Nomad – Microservices deployment

- Terraform – Infrastructure deployment
- AWS S3 – Long-term report storage
- Kibana – File integrity change logging tool
- Slack – Automated alerting service
- JIRA – Ticketing/tracking system
- Service Now – Ticketing/tracking system
- AWS Config – Asset management system

People

Xi Beam personnel who are involved in the definition, development, operation, or support of the Xi Beam system are grouped into the following primary areas: Engineering and Technical Operations, Security and Compliance, Business Operations, and Customer Support.

Engineering and Technical Operations

Members of the Xi Beam Engineering team are organized around product components and are responsible for product development, bug fixes, and L3 operations support. They are also responsible for L1/L2 support of the running platform instances, L3 customer support, monitoring and alerting systems, internal automation and tools, and information security.

Security and Compliance

The Nutanix 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 team is responsible for defining and driving the security development lifecycle, developing engineering-specific security training, performing threat model reviews, penetration tests, and building security tools. The Compliance team manages security, availability, and confidentiality compliance efforts for Nutanix products and cloud services.

Business Operations

The Nutanix Business Operations organizations are responsible for corporate IT, human resources, 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.

Process and Procedures

Management has developed and communicated to internal and external parties, 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. These items include identity and access management, monitoring, system configurations, appropriate use of assets, third party reviews, change control, and incident management. Organization wide policies and procedures are located on Nutanix's intranet sites, which employees are expected to adhere to in the delivery of the Xi Beam system commitments.

Training

Security awareness training is provided upon hire and at least annually (or more frequently if mandated by specific regulations) for employees. When required, due to information system changes, security awareness training is provided to applicable system users. Nutanix provides role-based security awareness training to personnel with assigned security roles and responsibilities.

Data

Nutanix has defined data classification around four categories. These categories include customer data, personally identifiable information, Xi Beam sensitive data, and system metadata and operational 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, internet protocol (IP) addresses that could identify an individual person, phone numbers, and physical addresses.
- Xi Beam system administration sensitive data:
  SSL Certificate with private keys, data at rest encryption keys, SSH keys to Xi infrastructure and auditing data.
- System Metadata and operations data:
  Customer IDs, Customer VM names, role names, Xi cluster information, service logs (not containing customer data, service configuration (without Xi administration sensitive data), IP addresses that only identify a company or company address pool (and not an individual person).

Access to Customer Data

Xi Beam does not access customer data, and protection of that data remains the responsibility of the customer. The Xi Beam service 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 Xi Beam service is controlled by the customer.

Attachment B: Principal Service Commitments and System Requirements

Nutanix designs its processes and procedures related to the Xi Beam system to meet its business objectives. Those 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 services.

Service commitments to customers and other relevant user entities are documented and communicated in master agreements and the terms of supplemental agreements, as well as in the description of the service offering provided on Nutanix's website, in their marketing materials, and within their customer-facing web portal. Minimum system requirements that must be implemented by customers for use of the Xi Beam system are communicated via the System Technology Guide.

Nutanix formalizes the service commitments in the form of two service level agreements:

- SaaS Support SLA: https://www.nutanix.com/support-services/product-support/product-support-programs (scroll down to the "SaaS Support" section)
- SaaS 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 commitments, compliance with relevant laws and regulations, and compliance with other system requirements. Such requirements are communicated via Nutanix's system policies and procedures, system design documentation, and contracts with customers. Information security (IS) policies define an organization-wide approach to how systems and data are protected. These include policies around how the Xi Beam 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 on how to carry out specific manual and automated processes required for the ongoing development and operation of the Xi Beam system.