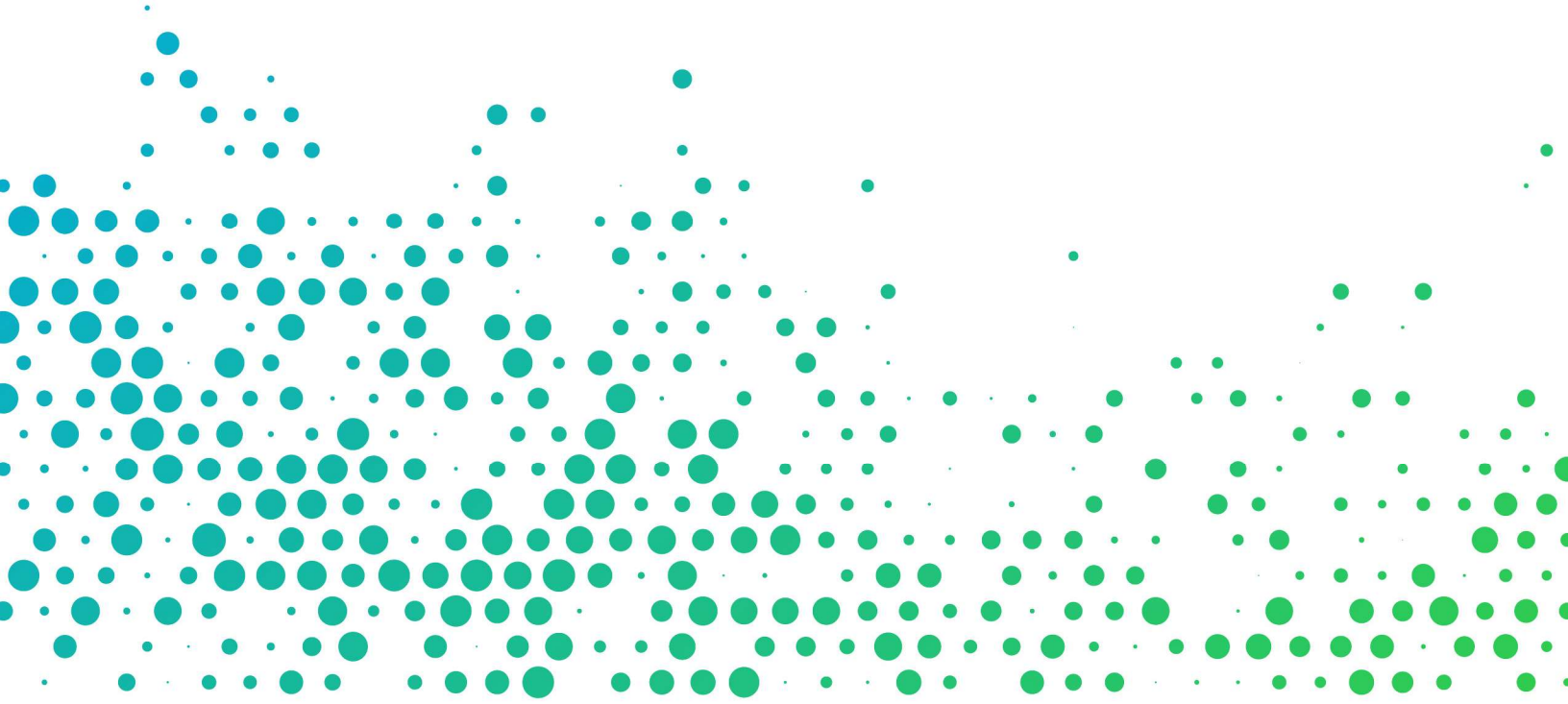
NUTANIX™

YOUR ENTERPRISE CLOUD

System and Organization Controls (SOC) 3

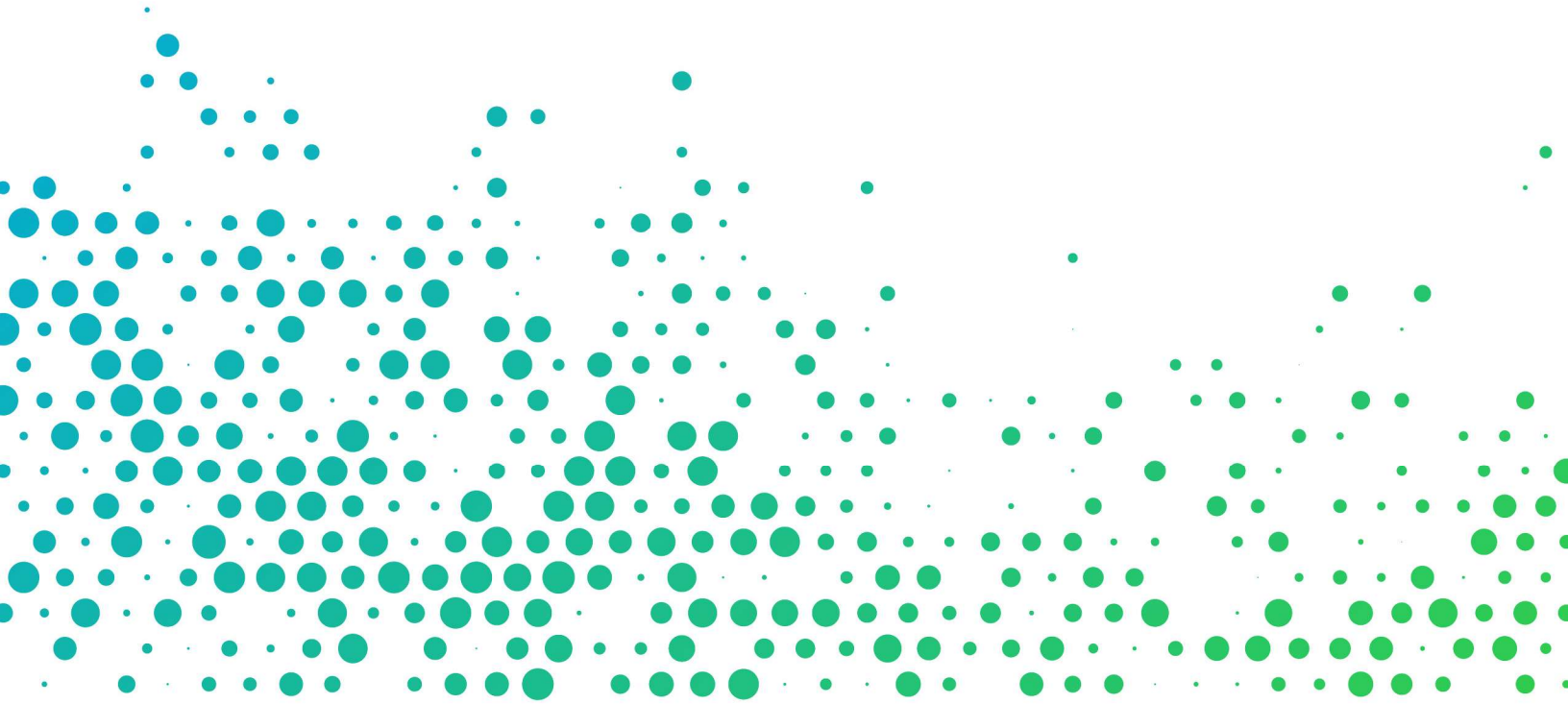
Report on Nutanix's Xi Leap System Relevant to Security, Availability and Confidentiality

For the Period April 1, 2020 to September 30, 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 Leap system (system) were effective throughout the period April 1, 2020, to September 30, 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 Leap system were effective throughout the period April 1, 2020, to September 30, 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 8, 2021

NUTANIX
YOUR ENTERPRISE CLOUD

ASSERTION OF NUTANIX MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Nutanix's Xi Leap system (system) throughout the period April 1, 2020, to September 30, 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 April 1, 2020, to September 30, 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 April 1, 2020, to September 30, 2020, to provide reasonable assurance that Nutanix's service commitments and system requirements were achieved based on the applicable trust services criteria.

Tel: 1 (855) 688-2649 | Fax: 1 (408) 916-4039 | Email: legal@nutanix.com

Attachment A: Xi Leap System

The scope of this report is the Xi Leap 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 Leap system.

Xi Leap, a disaster recovery service, protects the 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 Enterprise Cloud OS platform, Xi Leap 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 by the customer in a public cloud environment in the event of a customer site failure.

Xi Leap 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, Xi Leap 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.

Infrastructure

Nutanix's Xi Leap infrastructure consists of various components such as networking equipment, servers, and security tools. The Xi Leap system operates within secured datacenters provided by DRT and AWS located within the United States, Cyxtera in the United Kingdom, and Equinix in Germany and Japan.

The security and operations functions include authentication and privileged access management systems that allow authorized users access to the systems. There are logging and monitoring systems that alert on pre-performance and possible security issues.

Primary Software

Access Grant System (AGS)

In the Xi Leap system, the engineers do not have persistent access to sensitive data or persistent access to perform high risk operations. The privileged access is granted on demand using predefined workflows. AGS is the service that engineers and operators use to request privileged access.

Certificate Management System (CMS)

Inter-service communication is authenticated and encrypted. This requires an infrastructure service that issues customer certificates and secure socket layer (SSL) certificates during service bootstrap sessions (Canaveral/DCM, etc.). CMS maintains the list of revoked certificates and the functionality to query for revocations.

Secret Store

Xi Secret Store provides REST Application Program Interfaces (Rest API) for secrets management; including cryptographic symmetric keys, asymmetric key pairs, X509 certificates and passwords etc.

Identity and Access Management Service (IAM)

IAM provides authentication between various system services within the Xi Leap system. IAM also supports multi-tenancy, meaning the identities are contained and isolated within a customer environment and can be managed independently.

Xi Internet Gateway (XIG)

XIG serves two purposes:

- DNS to Prism reverse proxy for each customer's Prism instance and other services in Xi datacenters.
- Allows only valid customers to reach their Prism instance so that customers don't have to deal with volumetric attacks.

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

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

Data Center Management (DCM)

DCM is used to manage nodes and clusters within the Xi Leap system.

Canaveral

Canaveral is a deployment control system responsible for coordinating deployments of software components between clusters, cells, and datacenters. Canaveral can use custom deployment controls or delegate control to other systems to perform the actual installation and upgrades. Canaveral is a multi-staged system. The main stages are:

- Build stage: Building packages from sources hosted on GitHub using third party build service Circle CI.
- Verification stage: Multi phase verification consisting of unit tests, system tests, performance tests and optional manual testing.
- Deployment stage: After successful verification, packages are deployed to Xi Leap with standard fleet management semantics

Other

Other tools utilized in supporting the Xi Leap system:

- Okta – Serves as the multi factor authentication (MFA) solution
- OpenVas – Vulnerability scanning tool
- Black Duck – Secure code development scanner
- FluentD – Log aggregator
- Splunk – Security alerts from multiple sources
- Epoch – Security alerts from multiple sources
- AWS S3 – Long-term log storage
- Akamai – Distributed denial-of-service (DDoS) protection solution
- Pager Duty – Automated alerting service
- JIRA – Ticketing/tracking system
- Service Now – Ticketing/tracking system
- SolarWinds – Monitors network devices
- Device42 – Asset management system
- Saltstack – Automated infrastructure configuration management solution
- ThousandEyes – Traffic monitoring

People

Nutanix personnel involved in the definition, development, operation, or support of the core Xi Leap service are grouped into four primary areas: Engineering, Security, Business Operations, and Customer Support.

Engineering

Members of the Engineering team are organized around product components and are responsible for product development, testing, bug fixes, and operations support for software and infrastructure.

Xi Reliability Engineering (XRE) Security

The XRE Security team is a group within engineering dedicated to the build and operation of common security services. These services serve to constantly assess, prevent, detect and respond to attacks on Nutanix products and cloud services. The team is responsible for defining and driving the security development lifecycle, developing Engineering-specific security trainings, performing threat model reviews, penetration tests, and building security tools. The Security team also manages security, availability, and confidentiality compliance efforts for Nutanix products and cloud services. In addition, each of the Nutanix Xi Cloud Services has its own “security champion” who is the interface between the product engineering team and the central XRE Security team.

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 Leap service 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 Leap 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 Leap 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).

Customer data within the Xi Leap system, remains the sole property of the customers.

Customer Data Retention and Destruction

Each customer is responsible for implementing its own disaster recovery strategy. Nutanix retains data in accordance with customer agreements and encrypts that data using customer-specific encryption keys. To safeguard customer data, those specific encryption keys are destroyed immediately upon notification of termination of Xi Leap services, thereby rendering that customer's data permanently useless and unreadable.

Access to Customer Data

Access to customer data is restricted to authorized personnel by role-based, multi factor authentication, and limited time assignment. Physical access to datacenter facilities is enforced by strong perimeter security and internal security controls to limit access to authorized individuals only.

Attachment B: Principal Service Commitments and System Requirements

Nutanix designs its processes and procedures related to the Xi Leap 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. These services are also described on the Nutanix's website, related marketing materials, and within the customer-facing web portal. Minimum system requirements that must be implemented by customers for use of the Xi Leap system are communicated via the System Technology Guide.

Nutanix formalizes the service commitments in the form of a Nutanix License and Services Agreement and a Xi Leap Service Level Agreement, which both are available on www.nutanix.com.

Nutanix establishes operational and compliance requirements that support the achievement of security commitments, compliance with relevant laws and regulations, and compliance with other Xi Leap 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 Leap system is designed and developed and operated. The policies also include 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 Leap system.