netskope

REPORT ON NETSKOPE'S CLOUD SECURITY SAAS PLATFORM RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY FOR THE PERIOD APRIL 1, 2015 TO MARCH 31, 2016

Service Organization Controls 3 Report

COALFIRE CONTROLS

REPORT OF INDEPENDENT ACCOUNTANTS

To Netskope:

We have examined management's assertion that Netskope, during the period April 1, 2015 through March 31, 2016, maintained effective controls to provide reasonable assurance that:

- Netskope's Cloud Security SaaS Platform was protected against unauthorized access (both physical and logical)
- Netskope's Cloud Security SaaS Platform was available for operation and use, as committed or agreed
- Information designated as confidential was protected as committed or agreed

based on the criteria for the security, availability and confidentiality principles set forth in the American Institute of Certified Public Accountants' TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Netskope management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Netskope's relevant security, availability and confidentiality controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, Netskope's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

Coalfire Controls LLC

August 2, 2016
Coalfire Controls, LLC

Management's Assertion Regarding the Effectiveness of Its Controls Over the Cloud Security SaaS Platform Based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality

Netskope maintained effective controls over the Security, Availability and Confidentiality of its Cloud Security SaaS Platform to provide reasonable assurance that:

- Netskope's Cloud Security SaaS Platform was protected against unauthorized access (both physical and logical)
- Netskope's Cloud Security SaaS Platform was available for operation and use, as committed or agreed.
- Information designated as confidential was protected as committed or agreed

during the period April 1, 2015 through March 31, 2016, based on the criteria for the security, availability and confidentiality principles set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Our attached System Description of the Cloud Security SaaS Platform identified the aspects of the Cloud Security SaaS Platform covered by our assertion.

Sanjay Beri
Netskope Officer or Authorized Representative

CEO
Title

OVERVIEW OF SERVICE PROVIDED

Netskope is a California-based company that provides real-time analytics and policies for third-party applications used by its customers. The service Netskope provides allows for the termination of private SaaS application traffic to a cloud endpoint that allows for auditing and policy enforcement on the use of these applications. This service enables businesses to use SaaS applications while still being complaint with business and or auditing policies.

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

INFRASTRUCTURE

All services are hosted upon physically owned systems within SOC 2/SSAE16, ISO 27001, and LEED compliant data centers. Currently two data center co-location providers are Equinix and InterNAP within the United States, Europe and Asia/PAC. These locations provide redundant power input feeds with generator backup, redundant cooling and monitored humidity. This physical environment helps ensure system uptime and that physical access to the system is secured.

Three different network IP transit providers are utilized to connect Netskope's network across the world. For Internet IP transport, Level 3 communications and InterNAP are utilized. These two carriers provide divergent network paths. From InterNAP, Netskope gets a single hand-off as the Company acts as a tier-three provider being connected to ten tier-one carriers. Between these two providers, Netskope can offer both resiliency and low latency access into the Company's network.

The cloud network is designed to offer three principal components: security, availability, and dynamic resource provisioning. To offer these three components a network core was needed that could provide all three. A cloud-focused switching infrastructure is used to interact with the virtualization infrastructure to drive the network dynamically. This allows for automated security and networking provision driven by service allocation.

Services are protected by both stateless and stateful firewalls. Stateless firewalls are used to filter out unwanted traffic at the network edge. All services are secured using stateful firewalls. Transactions are logged and audited to ensure they are within expected usage of the network policy.

Virtualization is achieved for the majority of Netskope's services. All components of the service stack are virtualized except for the dataplane systems. Virtualization offers Netskope and its customers an excellent layer of software resilience and dynamic scale.

SOFTWARE

The base operating system used for the product is Ubuntu Linux. This covers all control plane and data plane software components written by Netskope. Some software components are built using the Mac OS X, Apple iOS, Android and Microsoft Windows. These are specifically client software components that are installed by users to access SaaS applications through the Netskope system. The network infrastructure components are all Linux-based operating systems.

Netskope utilizes three types of databases - a full stack of key-value pair, document based NOSQL, and relational database software. This is a very typical stack of database services today.

The dataplane is custom written software that intercepts customer data connections and passes on the contents of that data to an inspection and auditing engine. This is used to ensure that the contents of the traffic meet the security criteria of the customer and it audits the information accessed through the service. The software identifies which type of document is downloaded and by who. This detected information is sent to the event management platform for storage and later investigation through the WebUI.

Event management platform is a logging solution that is used to receive logs from the cloud proxy and then save the logging information into the database. This platform also has the ability to have the data read by the admin WebUI which displays the information back to administrators to validate that the organization's users are in compliance.

The WebUI component is used by customer administrators. This facilitates communication between the event query service and mysql to display the status of which applications the users within that organization have accessed.

Addon software components are installed on users' PCs to configure their browsers to talk back to the cloud proxy. It manages the users' browsers to securely talk back to the correct proxy and seamlessly authenticate back to the proxy ensuring the users identity for auditing purposes.

PEOPLE

There are several groups involved in the operation of the system. Everything starts with the product managers (PM) who work with customers to determine their needs. These requirements are passed on to the development teams that make up the majority of the Company. The development teams create the various components within the systems. Each component has a development lead and the leads report up to the development manager.

The development manager's job is to work with the development teams as well as the external teams to help plan and manage software releases. This ensures that the software is released on time and that it can be tested and deployed in a secure and stable manner to be consumed by the customer.

The QA group is responsible for testing that the software works in a functional state based upon well defined software specifications. The QA group works with engineering to fix any software defects. Once the software is in a stable and presentable state the QA team works with the DevOps group to explain the changes that are needed for a successful deployment.

The DevOps team is responsible for the deployment and continuous operation of the system. They deploy the software to production to be consumed by the users and administrators. Any issues in production are monitored by this team and they work with development or QA to further diagnose any defects within the software.

Users of the system utilize it to make secure connections to various SaaS applications. These applications are secured by validating the identity of the user accessing the Netskope system to ensure that it is the correct user from the corresponding organization and then access to the SaaS applications will be audited to ensure they are within the compliance specifications of the business.

Customer administrators utilize the system for auditing purposes to ensure that users are complying with business policies. Administrators may simply use the logs to see if there are policy violations and also create policies to enforce these business rules. An example of these policies is forbidding the download of a PDF versus just reading it through a SaaS application.

PROCEDURES

Access to the system is controlled through SSL VPN with 2 factor authentication. This prevents direct access to any of the hosts as they can only be accessed through this platform. All access occurs through specific access control lists restricting which systems can be accessed by which users. All access and commands issued to the systems are logged and audited. These audit logs are stored for thirty days and can be reviewed by other administrators. This is useful for change control and security auditing. The user account that is used to access the system can only SSH to localhost through SSL VPN with 2 factor authentication. If used to SSH to the host over the network the user account will not work. Each system has an automation account that can access the system. This account can only access the system via an SSH key from a restricted network.

All system logs, both OS and Netskope system, are sent to Sumo Logic for auditing and alerting. This allows for security auditing as well as application auditing. Sumo Logic can send alerts through the VictorOPS service to alert the DevOps staff of any potential problems. Netskope also monitors service health using Nagios based health checks which are hooked up to VictorOPS as well for alerting DevOPS staff. Lastly Pingdom is used as well as a third party monitor to generate reporting to share with customers on the stability of Netskope's system.

DATA

There are three different types of data bases used within the system: a relational, memory-based key-value pair, and document based NOSQL database are used. The memory-based database is used to store temporary data such as memory caches of information, log buffering, and lookup tables. All of this information is either written to a permanent database or deleted when it is no longer used.

AVAILABILITY

An IT infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific predefined thresholds are met. Daily incremental backups are configured for the customer information database. The Company's disaster recovery (DR) strategy includes a fully redundant, geographically dispersed environment across multiple data centers with load balancing and active replication. If any single data center is unavailable, there is an active failover mechanism to redirect traffic to an alternate location without impact to application availability. The Company uses a multi-location strategy for its facilities to permit the resumption of operations at other Company facilities in the event of loss of a facility. A DR test is performed at least annually.

CONFIDENTIALITY

A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel. Administrator access to the production platform, applications, operating systems, and databases is restricted to authorized personnel. Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosure of information and other data to which the employee has been granted access. Business partners are subject to nondisclosure agreements or other contractual confidentiality provisions. The Company

permits access to production systems by authorized employees only with two-factor authentication over encrypted VPN connection. The Company has deployed SSL for transmission of confidential and/or sensitive information over public networks. Legal counsel reviews non-standard third-party service contracts to assess conformity of the service provider's confidentiality provisions with the Company's confidentiality policies.