REPORT ON NETSKOPE'S CLOUD SECURITY SAAS PLATFORM RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY FOR THE PERIOD APRIL 1, 2016 TO MARCH 31, 2017

SOC for Service Organizations - SOC 3

COALFIRE CONTROLS

REPORT OF INDEPENDENT ACCOUNTANTS

To the Management of Netskope:

Approach

We have examined management's assertion that Netskope maintained effective controls to provide reasonable assurance that:

- Netskope's Cloud Security SaaS Platform was protected against unauthorized access, use, or modification to achieve Netskope's commitments and system requirements,
- Netskope's Cloud Security SaaS Platform was available for operation and use to achieve Netskope's commitments and system requirements, and
- Netskope's Cloud Security SaaS Platform information is collected, used, disclosed, and retained to achieve Netskope's commitments and system requirements

during the period April 1, 2016 through March 31, 2017 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* (2016). This assertion is the responsibility of Netskope's 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. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes (1) obtaining an understanding of Netskope's relevant security, availability and confidentiality polices, processes and controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

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 inherent limitations in its internal controls, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability and confidentiality are achieved.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies and procedures may deteriorate.

Opinion

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

December 21, 2017
Coalfire Controls, LLC

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

We, as management of Netskope are responsible for designing, implementing and maintaining effective controls over the Cloud Security SaaS Platform (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal controls, such as the possibility of human error and the circumvention of controls. Because of inherent limitations in security controls, an entity may achieve reasonable, but not absolute, assurance that security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's security controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

We have performed an evaluation of the effectiveness of the controls over the System throughout the period April 1, 2016 through March 31, 2017, to achieve the commitments and System requirements related to the operation of the System using the criteria for security, availability and confidentiality (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (2016). Based on this evaluation, we assert that the controls were effective throughout the period April 1, 2016 through March 31, 2017 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Netskope's commitments and system requirements
- the System was available for operation and use, to achieve Netskope's commitments and system requirements
- the System information was collected, used, disclosed, and retained to achieve Netskope's commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the Netskope Cloud Security SaaS Platform identifies the aspects of the Netskope Cloud Security SaaS Platform covered by our assertion.

Sanjay Beri

Netskope
Officer or Authorized Representative

CEO

Title

OVERVIEW OF SERVICE PROVIDED

Netskope, Inc. (“Netskope”, “the Company”) 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 cloud based Software as a Service (SaaS) application traffic to a single Netskope 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 physical and virtual systems owned and managed by Netskope within well-known reliable and secure providers for data center co-location and cloud infrastructure services. 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. None of these providers have any logical access to any Netskope data located in the facilities referenced.

Six different network IP transit providers are utilized to connect Netskope’s network across the world. For Internet IP transport purposes, Level 3 communications, InterNAP, XO Communications, Global Telecom & Technology (GTT), NTT DATA Corporation (NTT), and Amazon Web Services (AWS) are utilized. These carriers provide divergent network paths with at least two separate providers used within each data center. 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 SaaS cloud infrastructure network is designed to offer three principal components: security, availability, and dynamic resource provisioning. 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.

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 Threat Management service provides protection against malware for cloud services, combining a cloud vantage point with multi-layered malware detection and remediation capabilities. Netskope analyzes cloud traffic and files, such as sync clients, mobile apps, and SSL-encrypted cloud services, providing insight to malware present in cloud services.

The Data Loss Prevention (DLP) service protects and prevents the loss of sensitive data in the cloud. Netskope's Cloud DLP is an accurate and precise DLP, with the ability to discover sensitive data in sanctioned cloud services and en route to or from any cloud service, sanctioned or unsanctioned, whether users are on premises, remote, on a mobile device, or accessing from a web browser, mobile app, or sync client. DLP detects sensitive data using 3,000+ data identifiers across structured and unstructured data, support for 500+ file types, metadata extraction, proximity analysis, fingerprinting, exact match, and more.

The WebUI component is used by customer administrators. This facilitates communication between the event query service and internal SQL and NOSQL data repositories 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 authenticate back to the proxy ensuring the users identity for auditing purposes.

PEOPLE

There are several groups involved in the operation of the system. Product managers (PM) 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 Quality Assurance (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.

The Information Security team is responsible for the security of the platform infrastructure and web application security.

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 use the logs to see if there are policy violations and 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 Secure Sockets Layer Virtual Private Network (SSL VPN) with multi-factor authentication (MFA). This prevents direct access to any of the hosts as they can only be accessed through this interface. 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. The user account that is used to access the system can only Secure Shell (SSH) to localhost through SSL VPN with MFA. The user account will not work if used to SSH to the host over the network.

System logs for both operating system events and the Netskope applications are forwarded to Netskope's centralized logging and monitoring solution for auditing and alerting as well as an additional data store for long term archiving. This allows for security auditing as well as application performance and functionality auditing. The logging solution forwards alerts through a cloud based pager/notification service to alert the DevOps staff of any potential issues. Netskope also monitors service health using an automated system health check system which is also linked to the pager/notification service for alerting DevOPS staff. Lastly, Pingdom is used as an external third-party monitor to generate uptime reporting to share with customers on the stability of Netskope's system.

DATA

There are three different types of databases used within the system: relational, memory-based key-value pair, and document based NOSQL. 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. A DR test is performed at least annually. 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.

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 multi-factor authentication over encrypted VPN connections. The Company has deployed SSL/TLS, VPNs, and SSH 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.