



Agreement

☒ "I agree and understand that the documents being downloaded are Zscaler Confidential Information as defined in the NDA, End User Subscription Agreement (EUSA), or other subscription agreement between our company and Zscaler."

Name: Nivedita Dash

Email Address: Nivedita.Dash@unilever.com

Date:



ZSCALER, INC.

SOC 2 REPORT

FOR

ZSCALER CLOUD PLATFORM

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS
RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

APRIL 1, 2022, TO MARCH 31, 2023

Attestation and Compliance Services



This report is intended solely for use by the management of Zscaler, Inc., user entities of Zscaler, Inc.'s services, and other parties who have sufficient knowledge and understanding of Zscaler, Inc.'s services covered by this report (each referred to herein as a "specified user").

If the report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1 INDEPENDENT SERVICE AUDITOR’S
REPORT 1

SECTION 2 MANAGEMENT’S ASSERTION 5

SECTION 3 DESCRIPTION OF THE SYSTEM 7

SECTION 4 TESTING MATRICES 34

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Zscaler, Inc.:

Scope

We have examined Zscaler, Inc.'s ("Zscaler" or the "service organization") accompanying description of its Zscaler Cloud Platform system, in Section 3, throughout the period April 1, 2022, to March 31, 2023, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Zscaler'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Zscaler uses various subservice organizations for data center and cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Zscaler, to achieve Zscaler's service commitments and system requirements based on the applicable trust services criteria. The description presents Zscaler's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Zscaler's controls. The description 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

Zscaler 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 Zscaler's service commitments and system requirements were achieved. Zscaler has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Zscaler is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;

- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 suitability of the design and operating 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.

Description of Test of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in Section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects,

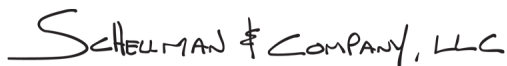
- a. the description presents Zscaler Cloud Platform system that was designed and implemented throughout the period April 1, 2022, to March 31, 2023, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Zscaler's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Zscaler's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Zscaler's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Zscaler's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Zscaler; user entities of Zscaler Cloud Platform system during some or all of the period of April 1, 2022, to March 31, 2023, business partners of Zscaler subject to risks arising from interactions with the Zscaler Cloud Platform 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; and
- 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.

SCHEFFMAN & COMPANY, LLC

Tampa, Florida
May 13, 2023

SECTION 2

MANAGEMENT'S ASSERTION



MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Zscaler Cloud Platform system, in Section 3, throughout the period April 1, 2022, to March 31, 2023, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Zscaler Cloud Platform system that may be useful when assessing the risks arising from interactions with Zscaler's system, particularly information about system controls that Zscaler has designed, implemented, and operated to provide reasonable assurance that its 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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Zscaler uses various subservice organizations for data center and cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Zscaler, to achieve Zscaler's service commitments and system requirements based on the applicable trust services criteria. The description presents Zscaler's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Zscaler's controls. The description does not disclose the actual controls at the subservice organizations.

We confirm, to the best of our knowledge and belief, that:

- a. the description presents Zscaler Cloud Platform system that was designed and implemented throughout the period April 1, 2022, to March 31, 2023, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Zscaler's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Zscaler's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that Zscaler's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Zscaler's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Zscaler, Inc. (“Zscaler” or “the Company”) was incorporated in 2007, during the early stages of cloud adoption and mobility, based on a vision that the Internet would become the new corporate network as the cloud becomes the new data center.

Enterprise applications are rapidly moving to the cloud to achieve greater information technology (IT) agility, a faster pace of innovation, and lower costs. Organizations are increasingly relying on Internet destinations for a range of business activities, adopting new external Software as a Service (SaaS) applications for critical business functions and moving their internally managed applications to the public cloud, or Infrastructure as a Service (IaaS). Enterprise users now expect to be able to seamlessly access applications and data, wherever they are hosted, from any device, anywhere in the world. Zscaler believes these trends are indicative of the broader digital transformation agenda, as businesses increasingly succeed or fail based on their IT outcomes.

Zscaler believes that securing the on-premises corporate network to protect users and data is becoming increasingly irrelevant in a cloud and mobile-first world where organizations depend on the Internet, a network they do not control and cannot secure, to access critical applications that power their businesses. Zscaler pioneered a new approach to security that connects the right user to the right application, regardless of network. Zscaler's Cloud Platform, which delivers security as a service, eliminates the need for traditional on-premises security appliances that are difficult to maintain and require compromises between security, cost, and user experience. Zscaler's cloud platform incorporates the security functionality needed to enable users to safely utilize authorized applications and services based on an organization's policies. Zscaler's solution is a purpose-built, multi-tenant, distributed cloud security platform that secures access for users and devices to applications and services, regardless of location.

Description of Services Provided

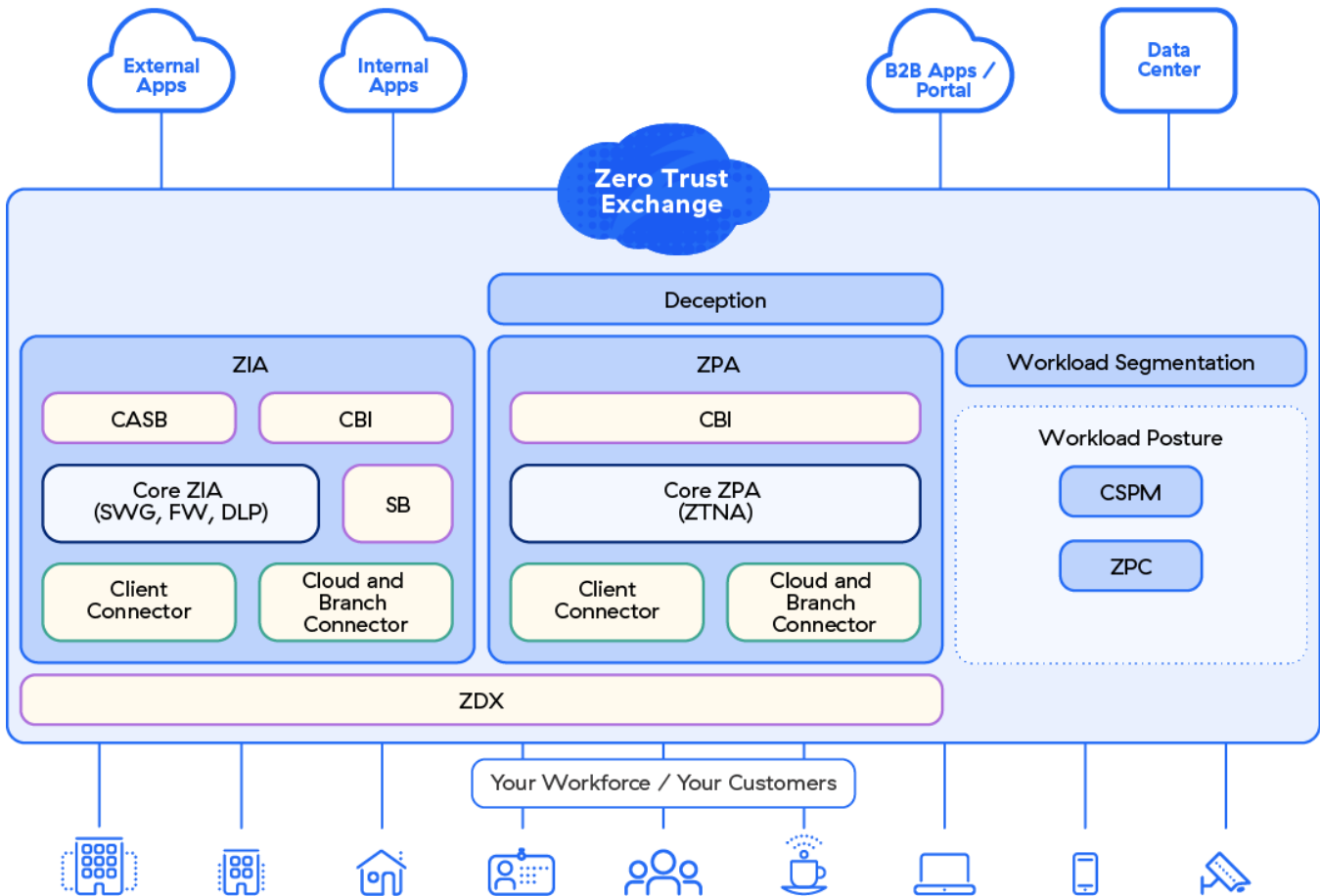
The Zscaler Cloud Platform consists of Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), Zscaler Business-to-Business (ZB2B), Zscaler Digital Experience (ZDX), Zscaler Shift (collectively referred to as the Zscaler Cloud Platform), Zscaler Cloud Security Posture Management (CSPM) Platform, Zscaler Workload Segmentation (ZWS), and Deception. A new in-scope product was also noted to include Zscaler Posture Control (ZPC).

Zscaler is a cloud-based information security platform, which is distributed across more than 150 data centers around the world, that helps organizations accelerate their IT transformation to the cloud. This enables the secure migration of applications from the corporate data center to the cloud and from a legacy “hub-and-spoke” network to a modern direct-to-cloud architecture. Zscaler's approach applies policies set by an organization to securely connect the right user to the right application, regardless of the network. Unlike traditional “hub-and-spoke” architectures, where traffic is backhauled over dedicated wide area networks (WANs) to centralized gateways, Zscaler's solution allows traffic to be routed locally and securely to the Internet over broadband and cellular connections.

[Intentionally Blank]

Nivedita Dash

Secure Access to the Internet and Applications



CSPM and "Advanced CSPM"

Zscaler Internet Access

Zscaler's ZIA solution securely connects users to externally managed applications, including SaaS applications and Internet destinations, regardless of device, location, or network. Zscaler's ZIA solution sits between users and the Internet and is designed to ensure malware does not reach the user and valuable corporate data does not leak out. Zscaler's ZIA solution enforces access based on granular access control policies, inspects unencrypted and encrypted internet traffic inline for malware and advanced threats, and prevents data leakage.

Policies follow the user to provide identical protection on any device, regardless of location; any policy changes are enforced for users worldwide. Zscaler's cloud security platform provides full inline content inspection of webpages to assess and correlate the risk of webpage objects, continuously discovering and blocking sophisticated threats.

Zscaler's ZIA solution includes broad functionality, which Zscaler categorizes by three areas:

Access Control

The access control functionality of Zscaler's ZIA solution enforces access and usage policies to externally managed applications, including SaaS application and internet destinations. This provides functionality that has traditionally been provided by stand-alone point products, such as:

- **Cloud Firewall:** Zscaler's cloud firewall was designed to protect users by inspecting internet traffic on ports and protocols, and it offers user level policies, application identification with deep packet inspection, and intrusion prevention.
- **Uniform Resource Locator (URL) Filtering:** Zscaler's URL filtering capabilities enable customers to enforce acceptable usage policies and protects organizations from users visiting unauthorized websites or illegally downloading content that can increase liability and impact their brand.

- **Bandwidth Control:** Zscaler's bandwidth control and traffic shaping capabilities ensure that business critical applications are prioritized over non-business critical applications, improving productivity and user experience. By enforcing quality of service in the cloud, Zscaler's platform can optimize "last-mile" utilization of a customer's network, providing significant value.
- **Domain Name System (DNS) Filtering:** Zscaler's DNS filtering solution provides a local DNS resolver and enforces acceptable use policies.

Threat Prevention

Zscaler's second area of functionality, threat prevention, protects users from threats using a range of approaches and techniques. Zscaler's threat prevention capabilities provide multiple layers of protection to prevent cyberattacks. Zscaler provides functionality that has traditionally been offered by disparate, stand-alone products, which are summarily described below:

- **Advanced Threat Protection:** Zscaler's advanced protection solution delivers real-time protection from malicious Internet content like browser exploits, scripts, zero-pixel iFrames, malware, and botnet callbacks. Over 120,000 unique security updates are performed each day to the Zscaler cloud to keep users protected. Once Zscaler detects a new threat to a user, Zscaler will block it for every user. Zscaler calls this the "cloud security effect." Advanced threat protection features include:
 - Botnet Protection: protection against botnets that could be secretly installed on user devices to perform malicious tasks at the instruction of command-and-control servers.
 - Malicious Active Content Protection: protection against websites that attempt to download dangerous content to a user's web browser.
 - Fraud Protection: protection against phishing sites that mimic legitimate sites, such as banking and e-commerce sites, in order to steal confidential information.
 - Cross-Site Scripting (XSS) Protection: protection against XSS, in which malicious code injected into websites is downloaded to a user's web browser from compromised web servers.
 - Suspicious Destinations Protection: block requests to any country based on International Organization for Standardization (ISO) 3166 mapping of countries to their IP address space. Websites are blocked based on the location of the web server.
 - Unauthorized Communication Protection: protection against communications like Internet relay chat (IRC) tunneling applications and "anonymizer" sites that are used to bypass firewall access and proxy security controls.
 - Peer-to-peer (P2P) Anonymizer Protection: block anonymizing applications such as Tor, an application that enables users to bypass policies controlling what websites they may visit or Internet resources they may access.
- **Cloud Sandbox:** Zscaler's cloud sandbox enables enterprises to block zero-day exploits and advanced persistent threats (APTs), by analyzing unknown files for malicious behavior, and can scale to every user regardless of location. Zscaler's sandbox was designed and built to be multi-tenant and allows customers to determine which traffic should be sent to the cloud sandbox. As an integrated cloud security platform, customers can set policies by users and destinations to prevent patient-zero scenarios by holding, detonating, and analyzing suspicious files in the sandbox before being sent to the user.
- **Anti-Virus:** Zscaler's anti-virus technology uses a signature database of files and objects on the Internet known to be unsafe and runs traffic through multiple anti-virus engines in a single pass.
- **DNS Security:** Zscaler's DNS security blocks access to known malicious sites, including command and control sites, and routes suspicious traffic to Zscaler's threat detection engines for content inspection.
- **Cloud Browser Isolation (CBI):** Zscaler's CBI stops active content and ransomware from reaching endpoint devices and prevents exfiltration of confidential data from business-critical applications.

Data Protection

Zscaler's third area of functionality, data protection, prevents unauthorized sharing or exfiltration of confidential information, reducing Zscaler's customers' business and compliance risk.

- **Data Loss Protection:** Zscaler's data loss protection enables enterprises to use standard or custom dictionaries using efficient pattern-matching algorithms to easily scale to users and traffic, including compressed or encrypted traffic, to prevent, monitor or block unauthorized or sensitive data exfiltration.
- **Cloud Data Loss Protection (DLP) with Exact Data Match (EDM):** Zscaler's data loss protection enables enterprises to easily scale DLP across any user and inside Secure Socket Layer (SSL) with improved detection by fingerprinting structured data with EDM.
- **Cloud Access Security Broker (CASB):** Zscaler's CASB prevents data exposure and ensures SaaS compliance with out-of-band CASB and discovers and controls unknown cloud applications with Inline CASB. Business policies can be defined with granular access control for specified cloud applications, such as the ability to upload or download files or post comments or videos based on different user or group identity. Zscaler partners with specific CASB vendors to extend their policy controls and visibility of out-of-band cloud applications.
- **CSPM:** Zscaler's CSPM (formerly Cloudneeti) platform is a multi-tenant SaaS product hosted on Microsoft Azure within CSPM's Azure subscription. The product is designed using highly scalable three-tier architecture with a web tier, serverless microservices tier and data and analytics tier with NoSQL database. The CSPM platform enables data security for any data type imported, stored, and exported during data collection, data analysis, remediations, single sign on, and integrations. Data protection, high-availability, and resiliency is considered as data and is replicated across multiple regions. Traffic to and from CSPM is encrypted at rest and in transit using transport layer security (TLS) for data-in-transit encryption and advanced encryption standard (AES) 256-bit encryption for data at rest.
- **CBI:** Zscaler's CBI functionality allows customers to eliminate exposure to risky web content and data exfiltration by separating browsing activity from the end user device by isolating traffic on user's devices through policy enforcement that re-directs traffic to a secure cloud browser running in a docker container which can restrict the types of actions performed (e.g., download, read, write, etc.) on files from untrusted sources.

Zscaler Private Access

Zscaler's ZPA solution offers authorized users secure and fast access to internally-managed applications hosted in enterprise data centers or the public cloud. Zscaler's ZPA solution's architecture does not expose the identity or location of these applications and provides only the necessary levels of access. While traditional remote access solutions, such as Virtual Private Networks (VPNs), connect a user to the corporate network, Zscaler's ZPA solution connects a specific user to a specific application, without bringing the user on the network, resulting in better security. Zscaler's ZPA Solution was designed around Zscaler's key tenants that fundamentally change the way users access internal applications:

- Connect users to applications without bringing users on the network;
- Never expose applications to the Internet;
- Segment access to applications without relying on traditional approach of network segmentation; and
- Provide remote access over the Internet without VPNs.

Zscaler's ZPA solution enforces a global policy engine that manages access to internally managed applications regardless of location. If access is granted to a user, Zscaler's ZPA solution connects the user's device only to the authorized application without exposing the identity or location of the application. Hence applications are not exposed to the Internet, further limiting threat exposure. This results in reduced cost and complexity, while offering better security and an improved user experience. ZPA functionality falls within three major areas:

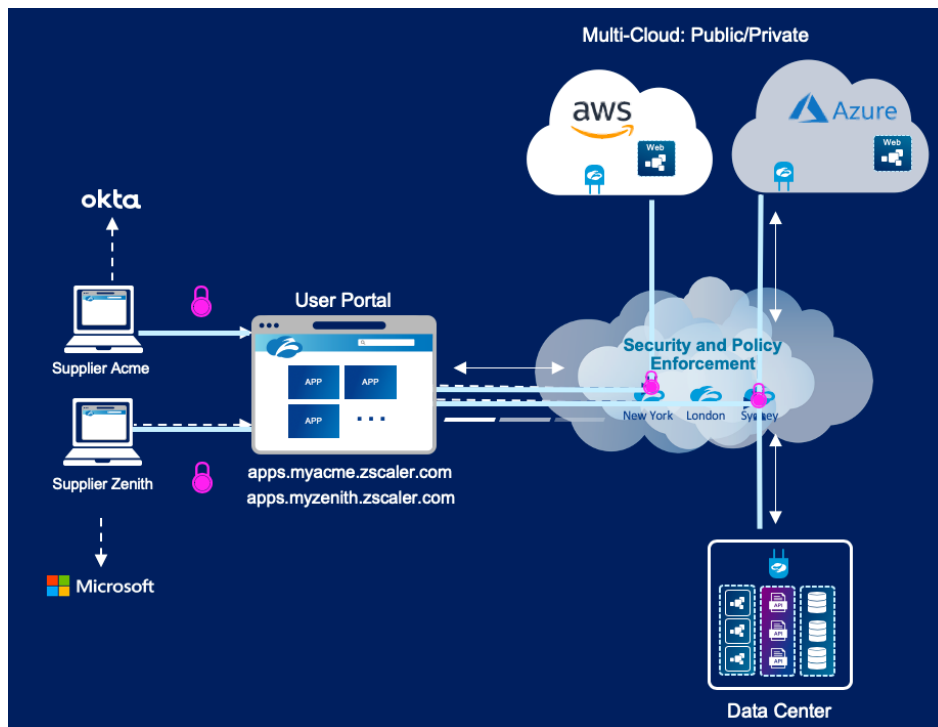
- **Secure Application Access:** Zscaler's ZPA Solution delivers seamless connectivity to internally managed applications and assets whether they are in the cloud, enterprise data center, or both. Administrators can set global policies from a single console, enabling policy-driven access that is agnostic to the network the users are on. By creating access to applications regardless of a user's network, Zscaler's ZPA solution

subsumes the need for traditional remote access VPNs, SSL VPNs, reverse proxies, and other similar products.

- **Application Segmentation:** This architecture provides capabilities that enables user and application-level segmentation. As each user-to-application connection is segmented with micro-tunnels, each of which is a temporary session between a specific user and a specific application, lateral movement across the network is prevented which significantly reduces security risk. Similar to CASB application discovery reports for internet applications, Zscaler's ZPA Solution provides granular discovery of internally managed applications to aid the creation of segmentation policies. Because Zscaler's ZPA solution sits on the application layer and is name or domain-based, organizations can quickly and easily identify the internally managed applications that are running and then easily provision policies. Micro-tunnels subsume the need for internal firewalls, which are required for protecting against lateral malware propagation from machine to machine, and traditional network access control functionality since users are granted access only to applications for which they have permission and are not granted full access to the network.
- **Application Protection:** Zscaler's ZPA solution initiates and connects together outbound-only links between authenticated users and internally managed applications using micro-tunnels. Access is provided to users without bringing them onto the corporate network and without exposing applications to the Internet. Internally managed applications are not discoverable or identifiable. With no inbound connections and no public IP addresses, there is no inbound attack surface and therefore no threat of distributed denial of service (DDoS) attacks. With Zscaler's approach, Zscaler subsumes the need for a next-generation firewall. Similarly, by completely removing the need for an exposed IP address or DNS to the Internet, Zscaler subsumes the functionality of DDoS mitigation systems.

Zscaler Business-to-Business (ZB2B)

ZB2B is a cloud-delivered service that provides business customers with seamless, secure access to business-to-business (B2B) applications. The service takes a zero-trust network access (ZTNA) approach that uses business policy to reduce the attack surface of applications, preventing them from being exposed to the internet. Only authenticated (supporting modern security assertion markup language (SAML)-based identity provider (IDP)) and authorized users can see or access the B2B applications. The service is hosted by Zscaler, which removes the need to spend time managing network appliances. This reduction in operating expense (OpEx) helps to accelerate cloud initiatives. The cloud service automatically connects business customers to apps via the fastest route by leveraging the Zscaler platform's global cloud presence for higher availability, reliability, and scale.

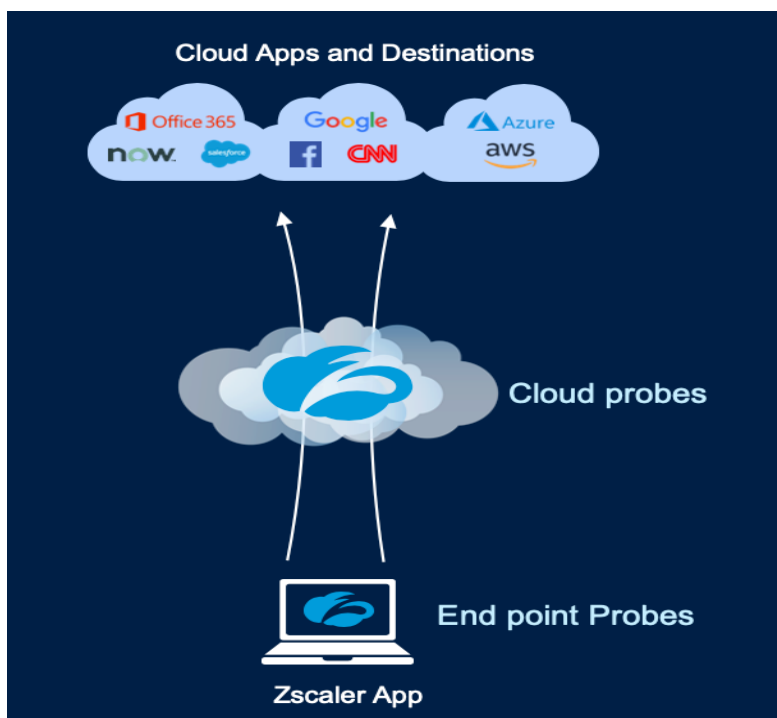


ZDX

ZDX solution enables organizations to monitor their users' digital experience. ZDX restores visibility across the complete user-to-cloud app experience and assists with issue isolation. By combining Zscaler's endpoint agent with its global cloud footprint, users receive end-to-end visibility, regardless of network or connection. From device level performance problems to network, Internet, and cloud app issues, ZDX provides relevant information to monitor and streamline troubleshooting, increase productivity, and gain back control of users' digital experience.

Key features of the ZDX solution include:

- Full-path visualization
- Zscaler digital experience score
- Efficient issue resolution
- SaaS management model



Zscaler Shift

Zscaler's Shift solution provides carrier-grade security and compliance for guest networks and open public wi-fi access. Zscaler's Shift solution offers multiple security features including content filtering, threat security, safe search, and SSL inspection. Additionally, Zscaler's Shift solution intelligently routes suspicious traffic to the Zscaler Cloud Platform for full in-line content inspection. Zscaler's Advanced Threat Protection blocks malicious active content, such as browser exploits, vulnerable ActiveX controls, malicious JavaScript, and cross-site scripting.

Security Features provided by Shift to implement an enterprise's policies include the following:

- Content Filtering
- Threat Security
- Safe Search
- SSL Inspection
- Whitelisting and Blacklisting URLs
- Shift Administration

Zscaler CSPM

The Zscaler CSPM Platform is designed to automatically identify and remediate application misconfigurations as a component of its cloud-delivered data protection capabilities. The platform delivers a breadth of innovations and product capabilities that automate security and compliance in the cloud, delivering continuous visibility and enforcing adherence to security policies and compliance frameworks:

- Zscaler CSPM is granted access to customer cloud environments (Amazon Web Services (AWS), Microsoft Azure, Office 365, or any other cloud service provider). It then collects actual configurations of cloud

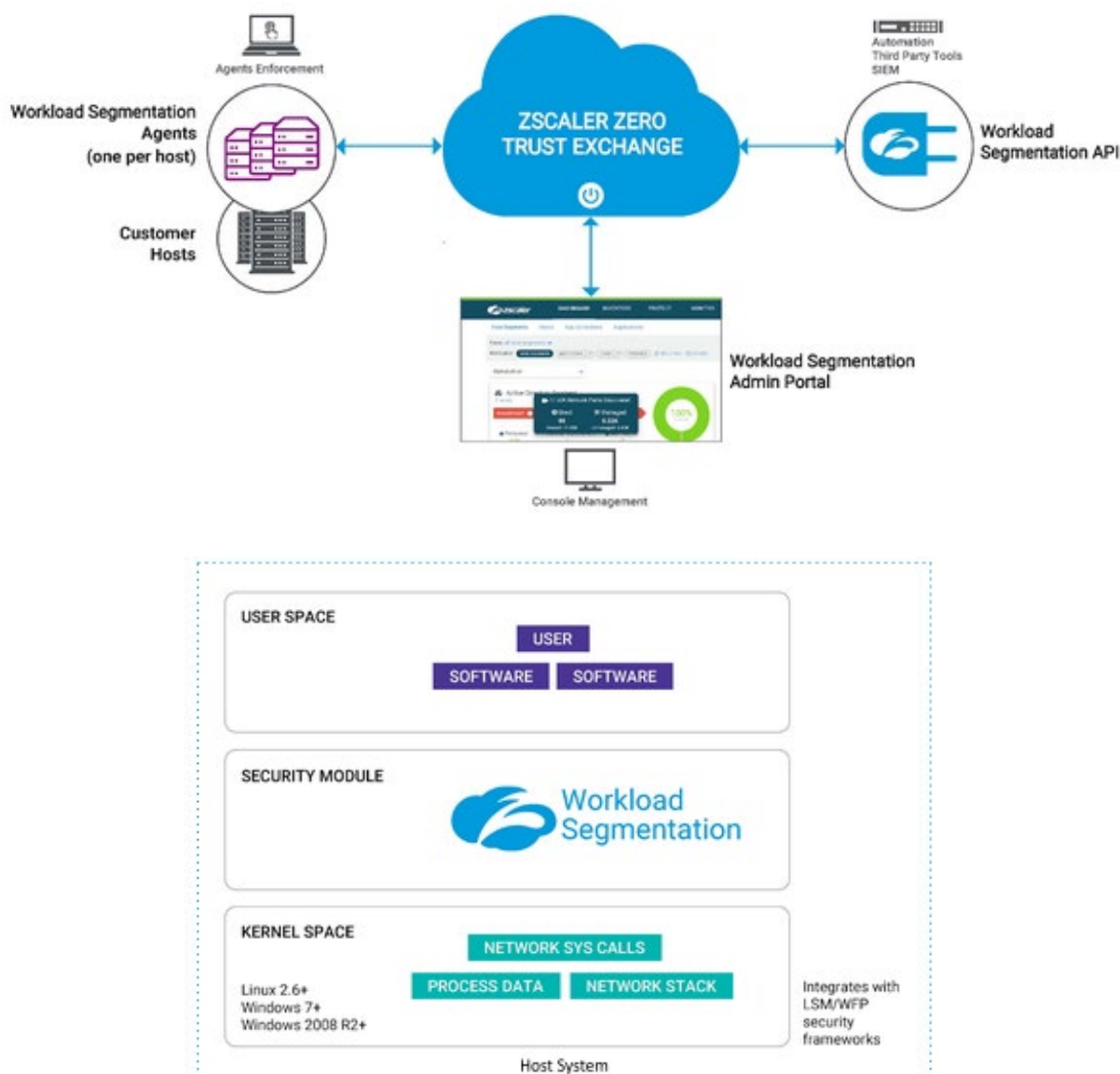
infrastructure over application program interfaces (APIs). A small subset of policies may require the installation of an agent.

- Zscaler CSPM compares discovered configurations against built-in security policies and identifies misconfigurations at the security policy and resource level. It also provides a mapping of security policies within various compliance frameworks. Dashboards and reports help users review this information.
- Zscaler CSPM enables various cloud governance features, including risk-based prioritization of the security posture, policy management (e.g., overrides, exceptions, third-party compensations), and configuration of private benchmarks for organizations that have multiple compliance standards or information security teams that need to customize the policy set for specific architecture.
- Remediation steps for each security policy and auto-remediation for a subset of security policies can be applied.

ZWS

The ZWS Platform is a new way to segment application workloads. The ZWS Platform enhances security by allowing workload segmentation to reveal risk and apply identity-based protection to workloads—without any changes to the network. The workload segmentation identity-based technology provides protection with policies that automatically adapt to environmental changes eliminating network attack surface.

- **Automated Segmentation:** Legacy involves multiple steps that can take months. ZWS micro segmentation happens in mere minutes — with just one click. From mapping data flows, to measuring exposure risk, to deploying policies for enforcement, the micro segmentation is quick and simple.
- **Policy Recommendation Engine:** Based on the cryptographic identities of software and machines communicating on networks, ZWS eliminates risk by building policy recommendations using patented machine learning technology.
- **Risk-Based Policy Management Policy Compression:** At the heart of ZWS' policies is a model of every application connection across an environment. Using a combination of exposure, reputation, behaviors, and software identity, ZWS creates risk-driven policies that are 25x fewer than those of traditional micro segmentation tools.
- **Exposure Analysis (Risk Analysis):** ZWS automatically builds a real-time application topology map and measures network exposure. As segmentation policies are applied, risk is reduced as attack paths are blocked and assets are protected.
- **Zero Trust Identity:** Software and machines in the environment are fingerprinted using a combination of cryptographic identity attributes. The identity of machines and software is the basis for every access control decision. Per the zero-trust model, if a software or a machine cannot be verified, it cannot communicate, regardless of previous permissions. This helps ensure the strongest level of protection for workloads, independent of network changes.
- **Adaptive Segments:** Segmentation using traditional controls requires ongoing manual policy management because it cannot easily account for software updates and new hosts being added to a segment. In contrast, ZWS segments are based on the identity of communicating software and not the network itself. This means that segments can adjust as new applications and hosts are added, verified, and permitted to communicate. The result: hardened security minus operational burden and complexity.
- **API:** Feeding customized ZWS application communication logs directly into a security information and event management (SIEM) enables customers to prioritize security events better, detect anomalous communication faster, and reduce alert fatigue, while monitoring the health of the ZWS implementation.



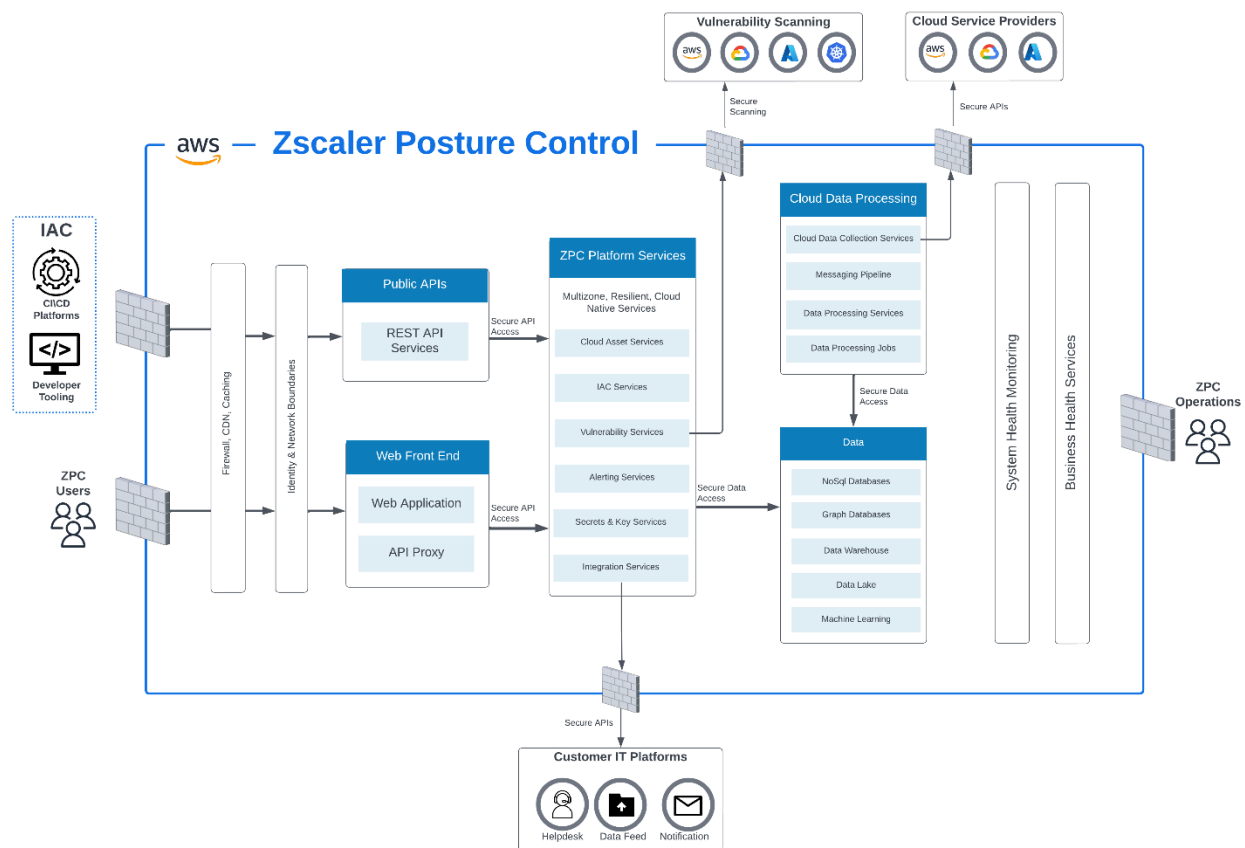
ZPC

Posture Control by Zscaler reimagines cloud-native application security with a 100% agentless solution that uses the power of machine learning to simply correlate hidden risks caused by the combination of misconfigurations, threats, and vulnerabilities across the entire cloud stack. It leverages the industry's most trusted security platform on the planet, Zscaler Zero Trust Exchange, to ensure security and a user-friendly experience. With security natively embedded as early as possible in the software development lifecycle, the security, development, and DevOps team can get 360-degree visibility across their entire multi-cloud footprint along with continuous compliance to ensure business agility.

- Agentless architecture.
- Zscaler ZPC is granted access to customer cloud environments (AWS, Microsoft Azure, Office 365, or any other cloud service provider). It then collects information regarding the cloud infrastructure and services, configurations, logs and more.
- APIs are used to collect information with no agents deployed.
- Agentless architecture is also used to provide vulnerability assessments over running workloads (Virtual Machines (VMs), containers, serverless) as well as public exposure identification.
- Rapidly pinpoint problems with the industry's simplest Cloud-Native Application Protection Platform (CNAPP) solution.

- 360-visibility: Gain full, in-depth visibility of risks across your entire multi-cloud footprint – including VMs, containers, and serverless workloads – all the way from build to run.
- Identify attack paths and detect ongoing attacks: Automatically correlate misconfigurations or activities that are seemingly low risk when viewed individually but can create serious risks combinations when viewed holistically. With a graph-based correlation and prioritization engine, you can expedite remediation and reduce alert fatigue by focusing on the risks that matter most.
- Powerful investigations: Proactively investigate any asset, identity, permission, or activity with in-depth contexts and derive custom policies for ongoing tracking.
- 100% agentless: Avoid developer friction and eliminate blind spots from incomplete coverage with an API-based, agentless approach. Scan VMs and containers in both registries and in production environments to correlate vulnerabilities and prioritize based on risk rather than on a CVSS score alone.
- Bring together security and DevOps teams with a native, end-to-end platform.
- Single, unified platform: Eliminate point products by unifying CSPM, CWPP with a single CNAPP that continuously secures every stage of the application lifecycle.
- Shift-left to shift-everywhere security: Break silos and get full lifecycle cloud security as early as the development phase with shift-left security. With security embedded as a foundation, you can then ensure that security shifts everywhere – from build, to deploy, to run time.
- Tool chain of your choice: Natively integrate security with a broad range of development platforms, such as VS Code, DevOps tools like GitHub and Jenkins to name a few, as well as security ecosystems such as ServiceNow, JIRA, and Splunk.
- Automate cloud security governance with built-in, custom compliance.
- Built-in, continuous compliance: Automatically map cloud application security posture to major industry and regulatory frameworks (e.g., CIS, NIST, HIPAA, PCI DSS) to provide automated, continuous reporting of cloud compliance.
- Custom private benchmarks: Customize existing frameworks and policies or create unique private benchmarks that's tailored to specific governance or organizational needs.
- Simple, granular reporting: Generate comprehensive assessment reports that span your current cloud estate and can be easily consumed.

[Intentionally Blank]

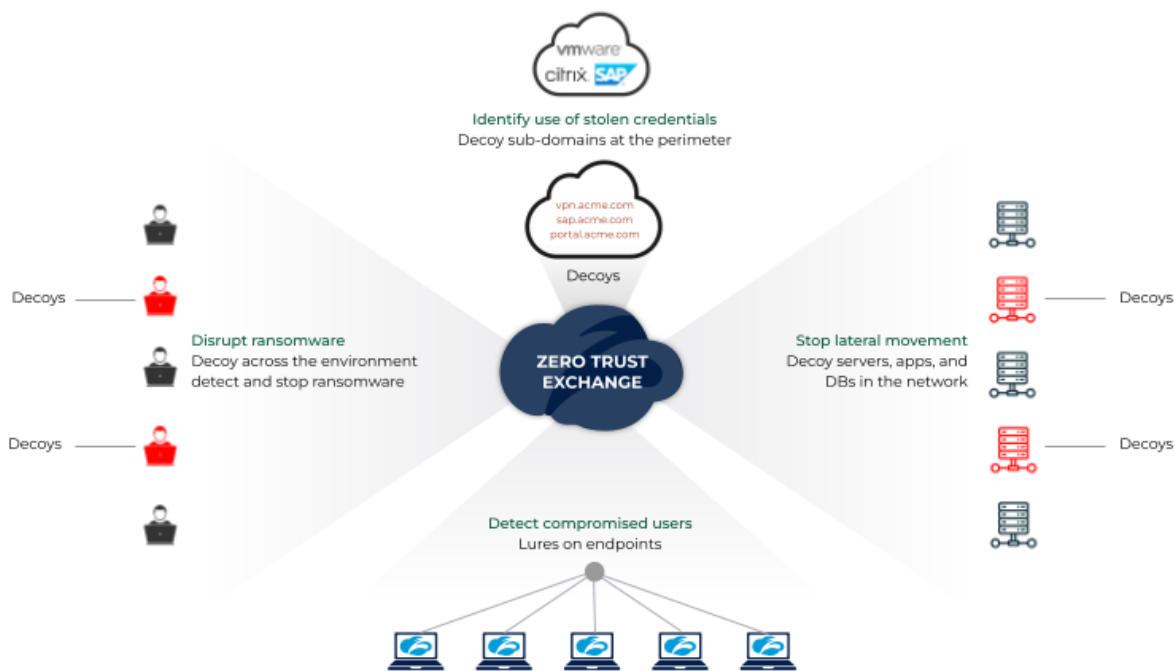


Zscaler Deception

Zscaler's Deception technology creates a layer of virtual decoys of critical IT assets and data across the enterprise. Unlike existing cyber security controls, Deception detects advanced attacks in real-time, and through any phase of a cyber-attack. Organizations use Zscaler Deception to detect compromised users, stop lateral movement and defend against human-operated ransomware, hands-on keyboard threats, supply chain attacks, and malicious insiders.

The Zscaler Deception platform can protect the environment by implementing:

- **Perimeter Deception** - Internet-facing decoys that heuristically detect pre-breach threats that are specifically targeting your organization.
- **Application Deception** - Server system decoys that host services like secure shell (SSH) servers, databases, file shares, and more.
- **Endpoint Deception** - A minefield for your endpoints. Includes decoy files, decoy credentials, decoy processes, etc.
- **Active Directory Deception** - Fake users in active directory that detect enumeration activity and malicious access.
Nivedita Dash
- **Cloud Deception** - Decoys web servers, databases, file servers, etc. that detect lateral movement in your cloud environments.



Description of ePHI Data Flows

Customers retain the ownership and control of their own company policy and data including information about their firewall rules, configurations, and strategies. The operations team is responsible for managing operational data such as system analytics and logs stored in databases and data files within the system as well as managing the associated infrastructure and log storage necessary to support the service. Zscaler has deployed secure methods and protocols for transmission of confidential and / or sensitive information over public networks. Proprietary customer metadata is secured and tokenized via patented methods.

The following table describes the information used and supported by the system.

| Data Used and Supported by the System | | |
|---------------------------------------|--|----------------|
| Data Description | Data Reporting | Classification |
| Proprietary customer metadata | May include unique user IDs (UUIDs), session authentication tokens, and transactions logs in encrypted / tokenized form. | Confidential |

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Zscaler designs its processes and procedures related to the Zscaler Cloud Platform system to meet its objectives for its Zscaler Cloud Platform services. Those objectives are based on the service commitments that Zscaler makes to user entities, the laws and regulations that govern the provision of the Zscaler Cloud Platform services, and the financial, operational, and compliance requirements that Zscaler has established for the services. The Zscaler Cloud Platform services are subject to the relevant regulatory and industry information and data security requirements in which Zscaler operates.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the following Zscaler documents which are available online: End User Subscription Agreement (EUSA) along with the accompanying Products Sheets and Service Level Agreements (SLAs) and Data Processing Agreement (DPA).

The principal security, availability, and confidentiality commitments are standardized and include the following:

- Maintain administrative, physical, and technical safeguards designed for the protection, confidentiality, and integrity of customer data.
- Complete annual third-party security and compliance audits of the environment, including, but not limited to, the following:
 - Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (System and Organization Controls (SOC) 2) examinations.
 - ISO / International Electrotechnical Commission (IEC) 27001:2013 (ISO 27001) certification reviews.
- Maintain an availability service level agreement for customers of 99.999% measured monthly.
- Monitor production systems 24/7 to ensure the availability and integrity of the data.
- Maintain disaster recovery processes to allow for continuation of data collection and to provide an effective and accurate recovery.
- Ensure ongoing availability and resilience of its processing systems and services, through Zscaler's global network of data centers and failover capabilities.
- Retain customer data for the duration of contracted services and as needed to fulfill the applicable business purposes and securely disposes of customer data as set forth in the EUSA and DPA.

Zscaler establishes system requirements that refer to how the system should function to support the achievement of the principal service commitments, comply with relevant laws and regulations and guidelines of industry groups, and achieve objectives that are relevant to the security, availability, and confidentiality trust services categories. These requirements include, but are not limited to, defined processes around the following:

- Maintain multiple, geographically separated data centers providing data mirroring, disaster recovery, and failover capabilities.
- Continuously monitor the production environment via network security controls designed to identify malicious traffic.
- Performance of region-specific mandatory background screening and segregation of duties.
- Transmission of users' unique login credentials, as well as data in the resultant connection, via encrypted connections.

In accordance with Zscaler's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

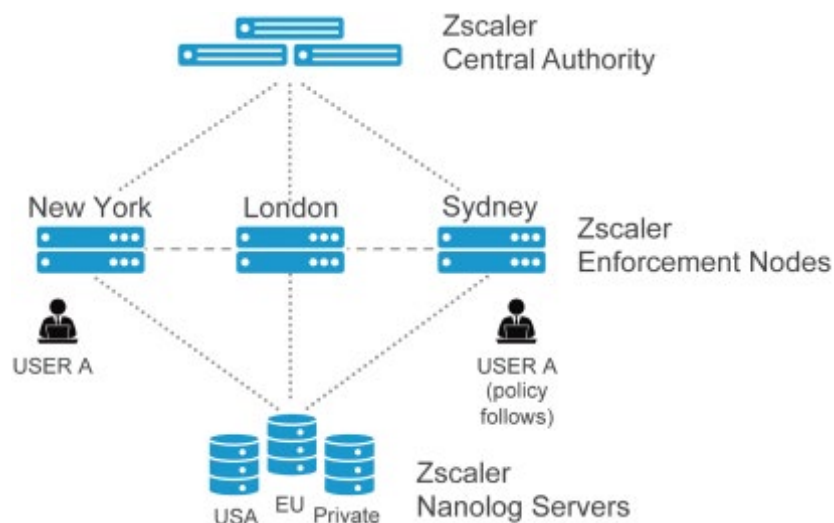
Zscaler's Technology and Architecture

Zscaler built a highly scalable, multi-tenant, globally distributed cloud capable of providing inline inspection that offers a full range of enterprise network security services. Zscaler designed a purpose-built three-tier architecture starting with Zscaler's core operating system (OS) and adding layers of security and networking innovations over time. Zscaler's Cloud Platform is protected by more than 100 issued and pending patents.

Proprietary Multi-tenant Global Cloud Architecture

Zscaler developed a proprietary security cloud that provides policy-based access to internet, SaaS, and internally managed applications. Zscaler's cloud is distributed across more than 150 data centers on five continents. The platform is designed to be resilient, redundant, and high performing. Zscaler's platform is built as software modules that run on standard x86 platforms without any dependency on custom hardware.

The platform modules are split into the control plane (Zscaler Central Authority), the enforcement plane (Zscaler Enforcement Nodes) and the logging and statistics plane (Zscaler Nanolog Servers) as described below:

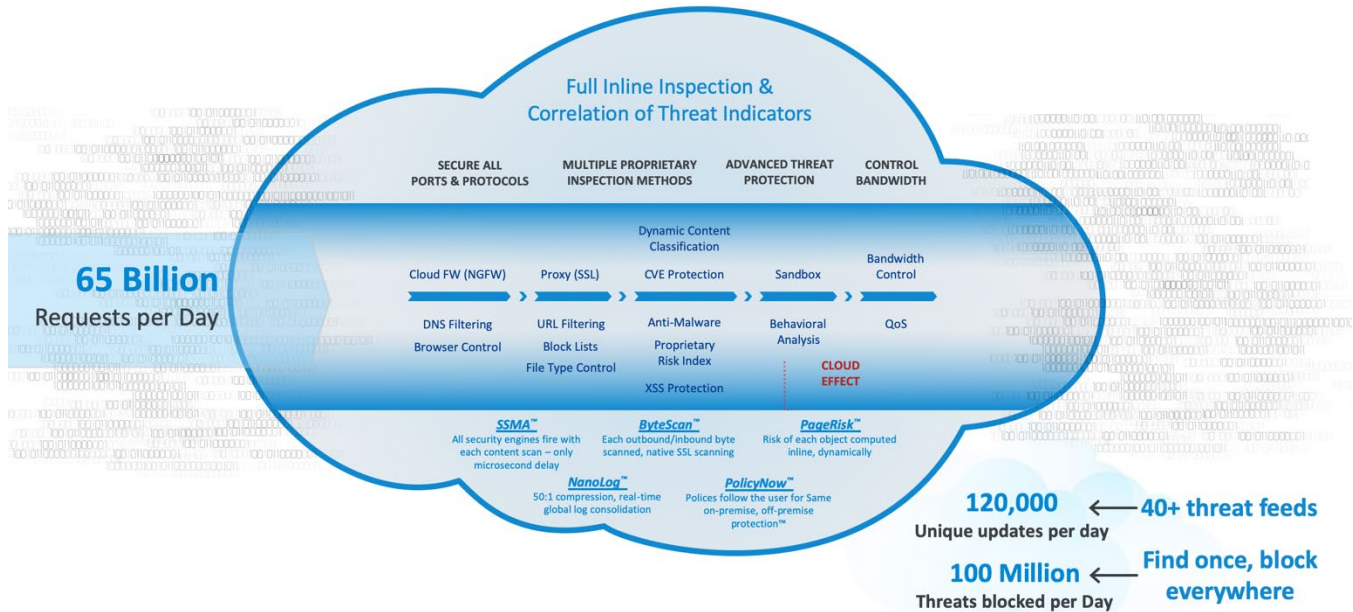


Zscaler Proprietary Multi-Tenant Global Cloud Architecture

- **Zscaler Central Authority:** The Zscaler Central Authority monitors Zscaler's security cloud and provides a central location for software and database updates, policy and configuration settings and threat intelligence. The collection of Zscaler Central Authority instances together act like the brain of the cloud, and they are geographically distributed for redundancy and performance.
- **Zscaler Enforcement Nodes:** Customer traffic gets directed to the nearest Zscaler Enforcement Node, where security, management and compliance policies served by the Zscaler Central Authority are enforced. The Zscaler Enforcement Node also incorporates Zscaler's differentiated authentication and policy distribution mechanism that enables any user to connect to any Zscaler Enforcement Node at any time to ensure full policy enforcement. The Zscaler Enforcement Node utilizes a full proxy architecture and is built to ensure data is not written to disk to maintain the highest level of data security. Data is scanned in random access memory (RAM) only and then erased. Logs are continuously created in memory and forwarded to Zscaler's logging module.
- **Zscaler Nanolog Servers:** Zscaler's Nanolog technology is built into the Zscaler Enforcement Node to perform lossless compression of logs, enabling Zscaler's platform to collect over 30 terabytes of unique raw log data every day. Logs are transmitted to Zscaler's Nanolog Servers over secure connections and multicast to multiple servers for redundancy. Zscaler's dashboards provide visibility into Zscaler's customer's traffic to enable troubleshooting, policy changes and other administrative actions. Zscaler's analytics capabilities allow customers to interactively mine billions of transaction logs to generate reports that provide insight on network utilization and traffic. Zscaler does not rely on batch reporting. Zscaler continuously updates Zscaler's dashboards and reporting and can stream logs to a third-party SIEM system.

as they arrive. Regardless of where users are located, customers can choose to have logs stored in the United States, the European Union, or Switzerland.

Advanced Cloud-Based Security Capabilities and Zenith of Scalability



Single-Pass, Inline Multi-Action Architecture for Better Security

- **ByteScan™ Technology:** ByteScan provides fast content scanning for detection of malicious sites and content, zero-day attacks, and data loss prevention. Zscaler's proprietary network stack enables interception of SSL traffic and can be integrated with a customer's public key infrastructure service, which manages encryption policies. ByteScan does not rely on traditional signature analysis.
- **Single-Scan, Multi-Action (SSMA™) Technology:** Zscaler's SSMA technology allows inspection engines to scan content in a single pass. This approach is starkly different from the chained model of physical or virtual appliances, whereby each security service independently processes packets, adding incremental latency at each hop. Due to Zscaler's SSMA technology, Zscaler's platform is able to apply policy-based security measures on a variety of security engines with minimal latency. SSMA also enables Zscaler's solution to be an extensible platform to add new technologies such as security intelligence and research advances.
- **PageRisk™ Technology:** Beyond identifying known or zero-day threats, Zscaler's PageRisk technology generates a Page Risk Index, which is a dynamically computed risk score based on potential indicators of compromise on objects in a file or a webpage. Zscaler dynamically computes the risk of webpage objects inline, checking for threats such as injected scripts, vulnerable ActiveX objects and zero-pixel iFrames, among others, as well as domain information. This ensures that unknown malware on well-reputed sites can be identified before harming users.
- **PolicyNow™ Technology:** PolicyNow technology ensures that policies follow the user. Any user of any organization can connect to a node in any geography. This provides protection regardless of the user location and also ensures global resiliency for Zscaler's cloud. Even if multiple data centers lose power or become unavailable, users can connect to the next closest node, and Zscaler's platform can continue to provide uninterrupted services.

Each hub data center is certified as ISO 27001, SOC 2, or a similar local certification as applicable. The Cloud Platform servers consist of Linux and Unix based operating systems.

The Zscaler Cloud Security Posture Management or CSPM (formerly Cloudneeti) application is a multi-tenant SaaS product hosted on Microsoft Azure within CSPM's Azure subscription. The product is designed using highly scalable three-tier architecture with a web tier, serverless microservices tier and data and analytics tier with NoSQL database. The CSPM application enables data security for each data type imported, stored, and exported during

data collection, data analysis, remediations, single sign on and integrations. Data protection, high-availability and resiliency is considered as data is replicated across multiple regions. Traffic to and from CSPM is encrypted at rest and in transit using TLS for data-in-transit encryption and AES 256-bit encryption for data at rest.

The Zscaler Workload Segmentation application is a multi-tenant SaaS product hosted on AWS within the Zscaler AWS corporate organization. The ZWS platform is designed using a highly scalable multi-tier architecture with a web tier, a containerized microservices backend tier, and a data tier with multiple data services including Kafka, PostgreSQL, Elasticsearch, and Redis. The ZWS application stores data securely with encryption at rest (AES-256) technology via the AWS Key Management Service (KMS) and data is highly available via replication and failover design methodologies. The ZWS platform uses a secure global network edge to enforce TLS authentication for each deployed ZWS agent as well as users of the ZWS console. Traffic into and out of the ZWS backend is encrypted via TLS.

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

| Primary Infrastructure | | | |
|---|--|---|--|
| Production Application | Business Function Description | Operating System Platform | Physical Location |
| Z-admin Portal | Customer access management tool. | Zscaler Operating System (ZOS) and Linux-based OS | Multiple third-party data center providers |
| Atlantic | | | |
| Production Servers | Linux servers supporting the in-scope systems. | | |
| Databases Servers | Databases supporting the logics of the in-scope systems. | | |
| Zscaler Private Access technology for remote Administration | Provide remote access to the in-scope systems with multi-factor authentication. | | |
| AWS Identity and Access Management (IAM) Console | Allows system administrators to manage and maintain the in-scope servers, database, and services. | | AWS |
| Microsoft Azure Active Directory | Allows system administrators to manage and maintain access to cloud resources and data. | Windows OS | East US (Virginia) |
| Azure SQL resource groups | Logical containers containing a collection of resources and provides levels of isolation and data security. Role-based access utilized to control access to resource groups. | | |
| Azure Cosmos Database | Fully managed non-relational (NoSQL) database service supporting the scalability, analytics, and data storage of the CSPM environment. | | |
| ZWS Console | Customer access management tool. | Linux-based OS | AWS |
| Production Servers (AWS ECS) | Linux servers supporting the in-scope systems. | | |

| Primary Infrastructure | | | |
|---|--|---------------------------|-------------------|
| Production Application | Business Function Description | Operating System Platform | Physical Location |
| Databases Servers (AWS relational database service (RDS)) | Fully managed database service supporting the scalability, analytics, and data storage of the ZWS environment. | Linux-based OS | AWS |
| Confluent Kafka Platform | Real-time streaming data service providing the backbone of the ZWS platform. | | |
| Bastion host | Servers restrict access to the ZWS and Deception production servers. | | |
| AWS Elastic Kubernetes Service (EKS) | A fully automated Kubernetes cluster service on AWS. | AWS | |
| Snowflake Databases | Database used to store customer data. | Snowflake | Snowflake |

People

Employees supporting day-to-day activities include the following:

- Management – responsible for overall security, ensuring enforcement of controls, change approvals, risk assessment, selection, and prioritization for mitigation, and providing oversight of the Zscaler Cloud Platform control environment. Management's role is to ensure personnel are appropriately trained, and that systems and processes are in place to meet system uptime, system-wide security, and consistent service execution. This includes the chief technology officer who oversees engineering organizations, the senior vice president of operations who is responsible for all operational aspects of the service, and the senior vice president of engineering who is responsible for the development of the service. Management is responsible for ensuring risk assessments are performed annually and periodically review the status of cloud security posture based on inputs from internal auditing and event-based activities.
- Network operations center (NOC) – The NOC is responsible for monitoring operations of the Zscaler Cloud Platform environment. They are also responsible for responding to alerts generated by monitoring systems based on operational triggers and first tier response to incidents. The NOC is responsible for monitoring problems or incidents and ensuring that they are resolved. The NOC team is manned 24x7 with employees across the globe.
- Security operations center – Zscaler's global security operations center consists of a computer emergency readiness team (CERT) and a ThreatLabZ team (Zscaler's research and development security lab). The CERT Team and ThreatLabZ team are responsible for monitoring and analyzing security alerts and distributing information to information security and business unit management personnel.
- Operations – consists of system engineering, networking, and program management teams responsible for provisioning and deploying the cloud environment to its production ready state before turning it over to the NOC for continuous monitoring. This includes each aspect of deployment to production as per the design for both public and private service deployments. The operations team is also responsible for access management to the cloud production environment.
- Cloud deployment and change management – responsible for managing changes to the production environment. Changes to the production environment follow standard Zscaler service continuity customer notification protocol and production changes are documented, reviewed, approved, and tracked via the internal ticketing system before implementation.
- Engineering – responsible for development of core services, applications, and service patches, as well as third tier response to service issues.

- Customer care – responsible for fielding customer calls regarding cloud environments, triaging of customer reported issues, and initiating internal tickets for resolution by engineering and operations as required and communicating with customers regarding any scheduled or unscheduled outages or issues through the Zscaler technical assistance center (ZTAC).

Procedures

Access Authentication and Authorization

Access to system information, including confidential information, is protected by authentication and authorization mechanisms. The operations and security teams are responsible for assigning and maintaining access rights to the production environment. In order to gain access to the ZIA and ZPA production environments, a user must authenticate first via VPN, then via SSH in order to enforce public-private key authentication. In addition, administrative access privileges within the production environment are restricted to authorized personnel. ZPA production resources are AWS security rulesets designed to filter unauthorized Internet traffic and to deny any activity not previously defined. Furthermore, AWS Elastic cloud compute (EC2) security groups are utilized to filter unauthorized inbound and outbound network traffic from the Internet.

In order to gain access to the CSPM production environment, a user must have an account and authenticate to Microsoft Azure via a unique username, password, and multifactor authentication (MFA). Role based access is utilized to control access to production resource groups within Microsoft Azure. In addition, administrative access privileges within the production environment are restricted to authorized personnel. A web application firewall and managed rulesets are designed to filter unauthorized Internet traffic and to deny any activity not previously defined.

In order to gain access to the ZWS production environment, a user must have an account and authenticate against JumpCloud directory-as-a-service via unique username, password, and MFA. Role and environment-based access is granted for system level login via SSH via both User and Device groups within JumpCloud. SSH authorization is limited to key-based only. Access to the ZWS AWS account is gated via the Zscaler corporate identity access management Okta tenant and only granted to authorized members of the ZWS engineering team. Access to bastion hosts is limited to one source IP address via security group rules applied to the instance.

In order to gain access to the Deception production environment, a user must have an account and authenticate to AWS via a unique username, password, and MFA then via SSH in order to enforce public-private key authentication. In addition, administrative access privileges within the production environment are restricted to authorized personnel. AWS security rulesets are designed to filter unauthorized Internet traffic and to deny any activity not previously defined.

In order to gain access to the ZPC production environment, a user must have an account and authenticate to AWS via a unique username, password, and MFA then via SSH in order to enforce public-private key authentication. In addition, administrative access privileges within the production environment are restricted to authorized personnel. AWS security rulesets are designed to filter unauthorized Internet traffic and to deny any activity not previously defined.

Access Requests and Access Revocation

Management has established controls to ensure that access to confidential data is restricted to those who require access. A formal process has been established for managing user accounts and controlling access to Zscaler's resources within the production environment. New employees are granted a standard level of access based on their job role. Prior to granting an individual access above the standard level of access provided upon employment, the access request must be reviewed and approved by the employee's manager.

Upon notification of an employee termination, human resources (HR) personnel create a termination checklist which is shared with the IT department to ensure that employees do not retain system access subsequent to their termination date. Management requires access requests and access revocations to be formally documented to ensure activities are completed for the addition, modification, and revocation of system and software access privileges. On at least a quarterly basis, management and development operations personnel perform a user access review to verify users with access to the production systems are authorized.

Change Management

Zscaler maintains documented application and infrastructure change management policies and procedures to communicate the company's expectations regarding the change management process to Zscaler personnel, and to ensure that any unauthorized changes are not made to production systems. Additionally, Zscaler documents Agile workflow diagrams for each type of change as well as guidance for documenting change attributes within the ticketing system. The cloud engineering teams meet on a quarterly basis to discuss and communicate current and upcoming changes and their effects on the system as well as policy development to reflect change management processes.

Changes are documented and tracked using an automated ticketing system which serves as the system of record for managing the change process. These changes may impact systems, applications, systems software, infrastructure, or any other aspect of the information processing environment. Source code is stored within a version control system and access to the source code is restricted to authorized engineering and development operations personnel. Changes must follow a formal review and approval process prior to implementation. Production branch protections are configured to require code review from development personnel, quality assurance (QA) approval indicating successful testing, and approval of the product owner and global administrator prior to merging to the production branch. Changes to operating systems, and system / application software are authorized, tested, and approved by authorized personnel prior to implementation. Development, testing, and production environments are logically separated as well as code repositories and deployment pipelines. The ability to migrate changes into production environments is restricted to authorized engineering personnel. Emergency changes are subject to the same change management requirements related to peer review, QA testing, and approval; however, a quicker turnaround may be achieved depending on the priority of the change. In an effort to protect production data, production data is not utilized for change development and testing efforts.

Data Backup

Production servers supporting the ZIA are hosted and replicated across global third-party data center providers. ZPA production servers are hosted within AWS. Documented policies and procedures are in place governing data backup and restoration processes.

Realtime Replications

Automated replication systems are configured to perform near real-time replication of client data from the production application servers to replication data storage servers distributed across global third-party data center facilities (for ZIA), Snowflake (ZPC), and AWS (for ZPA, ZPC, and Deception). The automated replication systems are configured to send e-mail notifications to operations personnel regarding the site replication when replication issues are identified. Operations personnel review the replication e-mail notifications for any issues through to resolution.

Zscaler provides an intra-data center to inter-data center redundancy for its production cloud for the CSPM product. Real-time replication and high availability are supported across multiple regions. Automated multi-region replication is configured within Azure DevOps and identified replication issues are configured to be sent via e-mail alert notifications to operations personnel.

Data Restorations and Disaster Recovery

As a part of Zscaler's business continuity and disaster recovery program for the production environment and platforms, Zscaler maintains an up-to-date business continuity and disaster recovery plan and conducts disaster recovery exercises at least once per year. Operations personnel perform data restoration tests on an annual basis to help ensure the recoverability of production data which are done in tandem with the disaster recovery process. Internal production data is used for restoration tests and is intended to simulate real situations as much as practical. Upon completion of the restore, the operations personnel test and verify that the data restoration is successful. Results of the data restoration efforts are maintained within the automated ticketing system. The testing includes confirming that the account and its data can be accessed, is validated against the source, and appears accurate once restored.

System Availability and Uptime

Zscaler has documented incident response procedures in place to address operational requirements for the response and resolution of incidents. Internal and external monitoring tools are configured to monitor production servers for unplanned downtimes which may be the result of various system performance and availability

metrics related to network and firewall availability, central processing units (CPUs), process load, and server utilization. The enterprise monitoring tools are configured to send alert notifications in the event that predefined thresholds are exceeded. An incident ticketing system is utilized to log and track system incidents through to resolution. Details are captured within the incident ticket to include service impact, root cause, and steps taken to resolve the issue. Support personnel may also generate incident reports to support post-incident responsibilities and review preventative measures for recurrence and monitoring. A NOC team is in place to monitor the enterprise monitoring applications for any events 24 hours per day, seven days a week, 365 days per year.

In addition to receiving incident reports from support, internal and external monitoring systems are configured to monitor and notify operations personnel of unplanned downtime events. An external system is employed to check connectivity and application responsiveness. Internally implemented monitoring tools are configured to monitor server responsiveness and notify operations personnel in the event of an unplanned downtime. Additionally, external users (i.e., customers) have the ability to report incidents on a public-facing portal which feeds into Zscaler's automated ticketing system to track resolution efforts.

System status, including scheduled maintenance and known issues, are displayed on the Zscaler trust page available at trust.zscaler.com.

Incident Response

Incident response and escalation procedures are in place to guide personnel in identifying and reporting system failures, incidents, and complaints. The operations or IT teams are responsible for monitoring security incidents, analyzing security alerts, distributing information to appropriate information security and business unit management personnel, and ensuring they are resolved in a timely manner. An automated ticketing system is utilized to document and track incidents and remediation activities. Incidents are assessed and assigned a severity rating. Incidents that require changes to the system follow the standard change control process. Additionally, customer incidents are reported through a public-facing portal and are tracked within an automated ticketing system to manage system incidents, response, and resolution.

System Monitoring

Zscaler utilizes a third party to perform penetration tests on an annual basis. Several tools are utilized for vulnerability scanning of applications, production cloud infrastructure, open-source components, and source code. Findings identified as a result of vulnerability scanning and penetration testing are documented and monitored through resolution by operations or IT personnel. Zscaler has implemented a set of logging and monitoring tools that are configured to collect data from system infrastructure components to monitor system performance, potential security threats and vulnerabilities, resource utilization, and alert IT operations upon detection of unusual system activity or service requests. Additionally, an intrusion prevention feature is utilized to monitor, block, and alert security events based on configured rulesets.

Enterprise monitoring applications are in place to monitor the performance and availability of the in-scope systems and alert operations personnel via on-screen alert when predefined thresholds are exceeded. The system is configured to send alert notifications to operations personnel when predefined thresholds are exceeded on monitored systems.

Data

Customers retain the ownership and control of their own company policy and data including information about their firewall rules, configurations, and strategies. The operations team is responsible for managing operational data such as system analytics and logs stored in databases and data files within the system as well as managing the associated infrastructure and log storage necessary to support the service. Zscaler has deployed secure methods and protocols for transmission of confidential and / or sensitive information over public networks. Proprietary customer metadata is secured and tokenized via patented methods.

The following table describes the information used and supported by the system.

| Data Used and Supported by the System | | |
|---------------------------------------|--|----------------|
| Data Description | Data Reporting | Classification |
| Proprietary customer metadata | May include unique user IDs (UUIDs), session authentication tokens, and transactions logs in encrypted / tokenized form. | Confidential |

Significant Changes During the Period

The Zscaler ZPC was first operational on December 12, 2022.

Subservice Organizations

The data center hosting services provided by multiple third-party data center providers and the cloud hosting services provided by AWS and Microsoft Azure were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at third-party data center service providers, alone or in combination with controls at Zscaler, and the types of controls expected to be implemented at third-party data center service providers, AWS, and Microsoft Azure to achieve Zscaler's service commitments and system requirements based on the applicable trust services criteria.

| Control Activity Expected to be Implemented by Third-Party Data Center Service Providers, AWS, and Microsoft Azure | Applicable Trust Services Criteria |
|--|---|
| AWS and Microsoft Azure are responsible for notifying Zscaler of unusual activity, violations, and / or security breaches identified that impact Zscaler systems and customers. | CC2.1 – CC2.3 CC4.1 CC7.3 – CC7.5 |
| AWS and Microsoft Azure are responsible for monitoring and managing the logical access control systems to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zscaler applications reside. | CC6.1 – CC6.3 CC6.5 – CC6.6 CC7.2 |
| The third-party data centers, AWS, and Microsoft Azure are responsible for restricting physical access to data center facilities, backup media, and other system components including routers and servers. | CC6.4 – CC6.5 CC7.2 |
| AWS and Microsoft Azure are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Zscaler systems reside. | CC6.7 |
| AWS and Microsoft Azure are responsible for monitoring any configuration changes of the logical access controls system for the underlying network, virtualization management, and storage devices where the Zscaler's applications reside. | CC7.1 |
| The third-party data centers, AWS, and Microsoft Azure, are responsible for monitoring the capacity demand and ensuring capacity resources are available and functioning to meet Zscaler's availability commitments and requirements. | A1.1 |
| The third-party data centers, AWS, and Microsoft Azure, are responsible for ensuring the data center facilities are equipped with environmental security safeguards. | A1.2 |

CONTROL ENVIRONMENT

The control environment at Zscaler is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

Integrity and Ethical Values

Zscaler has developed a code of conduct and an employee handbook that is available to employees on the Zscaler intranet. The code of conduct and the employee handbook address the acceptable business practices, conflicts of interest and expected standards of ethical and moral behavior. These documents are provided to each new employee prior to commencement of employment. Prior to the commencement of employment, U.S. employees are required to sign an acknowledgement form that they agree to abide by the employee handbook and code of conduct. There is an established "tone at the top", and accountability is maintained through the leadership team to provide guidance on acceptable behavior within the organization. This tone is communicated and practiced by executives and management throughout the organization. The importance of high ethics and controls is discussed with newly hired employees throughout both the interview and orientation processes.

Board of Directors and Audit Committee Oversight

Zscaler has a board of directors, comprised of a majority of independent members, that meets at least once quarterly and is consulted and involved in every significant business decision, including providing oversight on risk matters.

The audit committee is comprised of industry veterans with experience in compliance issues and meets annually to discuss internal control performance. During these meetings, significant issues and process improvement areas are discussed. Significant action items are raised to the board of directors to provide support for the organization's continued improvement efforts.

Organizational Structure and Assignment of Authority and Responsibility

Zscaler has established clear lines of reporting, which facilitate the flow of information to the correct personnel. Roles and responsibilities are segregated based on functional requirements. Zscaler has an organization chart that sets forth the Company's lines of reporting. The organization chart is updated as necessary and made available to Zscaler personnel via the corporate intranet.

Management and employees are assigned levels of authority and responsibility to facilitate effective internal control.

Commitment to Competence

Zscaler management defines competence as the knowledge and skills necessary to accomplish tasks that define employee's roles and responsibilities. Zscaler's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific control activities that Zscaler has implemented in this area are described below:

- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- An information system security and management policy is formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements.

- U.S.-based new employees must sign an employee handbook acknowledgement form after reviewing the employee handbook indicating that they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate security policies.

Accountability

Zscaler's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel. Specific control activities that Zscaler has implemented in this area are described below:

- Management formally documents an organizational strategy within its information security management system (ISMS) policies and updates them on an annual basis to align internal control responsibilities, performance measures, and incentives with company business objectives.
- Internal audits are performed annually in accordance with ISO 27001 requirements. The audit results are documented and reviewed by management.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- Board of directors meetings are held on a quarterly basis to review internal control performance.
- An employee sanction procedure is in place communicating that an employee may be terminated for noncompliance with a policy and / or procedure.

Zscaler's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that Zscaler has implemented in this area are described below:

- Management has established pre-hire screening procedures to govern the new hire process for employees.
- Management has established employee termination procedures to govern the termination process.

RISK ASSESSMENT

Objective Setting

The risk assessment process involves a dynamic process that includes identification and analyzation of risks that pose a threat to the organization's ability to perform the in-scope services. The process first starts with determining the organization's objectives as these objectives are key to understanding the risks and allows the identification and analyzation of those risks relative to the objectives. Management formally documents organizational strategy within ISMS policies and updates them on an annual basis to align internal control responsibilities, performance measures, and incentives with company business objectives. Management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to ensure they align with company's mission and are utilized as part of the annual risk assessment process. Additionally, management holds quarterly company-wide strategy meeting that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.

Risk Identification and Analysis

Zscaler identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. Zscaler's risk assessment process includes an analysis of possible

threats and vulnerabilities relative to each of the objectives. The risk identification process includes consideration of both internal and external factors and their impact on the achievement of the objectives. Appropriate levels of management are involved in the risk assessment process. Identified risks are analyzed through a process that includes estimating the potential significance of the risk. Zscaler's risk assessment process includes considering how the risk should be managed and whether to accept, avoid, mitigate, or share the risk.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud, incentives, pressures, and opportunities for employees
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. Additionally, the risk assessment that is performed on an annual basis considers the potential for fraud.

Risk Mitigation

Policies and procedures are in place to guide personnel in risk mitigation activities, including the following: monitoring processes and development of policies, procedures, and communications to meet the entity's objectives during response, mitigation, and recovery efforts. Internal audit personnel perform a risk assessment on an annual basis that includes an evaluation of risk mitigation control activities for risks arising from potential business disruptions. Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans are reviewed, updated, and approved annually based on the business impact analysis during the annual risk assessment process.

Vendors are evaluated in accordance with the vendor screening process and approved by management prior to processing customer data. Signed nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties. The compliance team reviews vendor audit reports on at least an annual basis to ensure that third-party providers are in compliance with the organization's requirements. Internal audit periodically performs monitoring in the form of onsite visits or conducting risk assessments of third-party vendors with whom confidential information was shared, including whether the third party is complying with agreed upon confidentiality commitments.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security, availability, and confidentiality categories.

Selection and Development of Control Activities

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Zscaler's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Zscaler Cloud Platform system.

INFORMATION AND COMMUNICATION SYSTEMS

Pertinent information must be identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial, and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to inform business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

Internal Communications

Zscaler has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include training for new employees on company policy and commitments, security awareness training for employees, and the use of e-mail messages and internal collaboration tools to communicate time-sensitive information. Employees are encouraged to communicate to their manager and / or senior management.

External Communications

Zscaler has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their transactions and communication of significant events. These methods include the public-facing website to communicate relevant information regarding the design and operation of the system and Zscaler's commitments to external customers. The website also features a portal where customers can communicate with Zscaler for support of the system or to report any incidents or concerns related to the operation or security of the system. When communicating with vendors, Zscaler requires that third parties sign a nondisclosure agreement of confidentiality before sharing any confidential information.

MONITORING

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

Ongoing Monitoring

Zscaler utilizes both manual and automated monitoring tools. Management personnel are involved in the day-to-day functioning of each department and provide hands on training, coaching, and correction. The management team holds meetings on a periodic basis within functional departments to discuss changes to the organization, changes to the production environment, and incidents or events identified by personnel or user entities.

Separate Evaluations

Management has implemented a self-assessment program to evaluate the performance of specific control activities and processes over time and confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the competence and authority. As a result of management's risk analysis process, each control activity within scope has been assigned a risk level associated with the assessed level of risk it is intended to mitigate. Controls that serve to mitigate multiple risks are assigned the highest level of assessed risk among the pertinent risks.

Management has determined that each risk assignment or category, will require structured inquiry, observation, inspection, or sample testing, or a combination of the aforementioned, based on the assigned risk level and the nature of the control, whether automated or manual, and the frequency of application (e.g., constant, daily, weekly, quarterly, etc.).

Subservice Organization Monitoring

The services provided by third-party vendors are monitored on a regular basis as part of the day-to-day operations. As they become available, Zscaler personnel receive and review documentation (SOC reports and/or security certifications) to help ensure security practices are being followed.

Internal and External Auditing

Zscaler monitors the requirements of certifications and regulatory demands, primarily by obtaining and maintaining an ISO compliance. Additionally, Zscaler performs internal audits of the control environment on an annual basis.

Zscaler supports many user entities in their efforts to meet the regulatory demands of their industry or governing agency. Zscaler has assisted user entities in successfully meeting the requirements of many certifications and regulatory demands, including ISO 27001.

Evaluating and Communicating Deficiencies

The nature, timing and extent of the self-assessment tests and results are documented for management review. Deviations or deficiencies associated with controls with a risk assignment of high are immediately escalated for corrective action. Other self-assessment results are reviewed within a week of the self-assessment test procedures, and corrective action, if required, is assigned to an individual and documented once those required actions are complete. Management reviews the deviations and corrective actions are tracked through the year and revisited during the annual risk assessment meeting.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Zscaler Cloud Platform system provided by Zscaler. The scope of the testing was restricted to the Zscaler Cloud Platform system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period April 1, 2022, through March 31, 2023.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

| Test Approach | Description |
|---------------|---|
| Inquiry | Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding. |
| Observation | Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures. |
| Inspection | Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.). |

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the applicable trust services criteria, are presented in the “Subservice Organizations” section within Section 3.

SECURITY CATEGORY

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|--|--|----------------------|
| Control Environment | | | |
| CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | | | |
| CC1.1.1 | An information security management system policy and information security policy are formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. | Inspected the information security policy and information security management system policy to determine that an information security management system policy and information security policy were formally documented and reviewed during the period that identified information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. | No exceptions noted. |
| CC1.1.2 | Background checks are performed on new hires, to the extent permissible by local law, prior to the new hire employee's start date. | Inquired of the compliance manager regarding background verification checks to determine that background checks were performed on new hires, to the extent permissible by local law, prior to the new hire employee's start date. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|--|---|----------------------|
| | | Inspected the background checks documentation for a sample of employees hired during the period to determine that background checks were completed for each employee sampled. | No exceptions noted. |
| CC1.1.3 | U.S.-based employees must sign an employee handbook acknowledgement form after reviewing the employee handbook indicating that they have been given access to the employee manual and understand their responsibilities for adhering to the policies and procedures contained within the manual. | Inquired of the compliance manager regarding employee handbook acknowledgement to determine that U.S.-based employees signed and acknowledged the employee handbook to understand their responsibilities for adhering to the policies and procedures contained within the manual. | No exceptions noted. |
| | | Inspected the employee handbook acknowledgment for a sample of U.S.-based employees hired during the period to determine that each employee sampled indicated that they had been given access to the employee manual and understood their responsibilities for adhering to the policies and procedures contained within the manual. | No exceptions noted. |
| CC1.1.4 | An employee sanction procedure is in place communicating that an employee may be terminated for noncompliance with a policy and / or procedure. | Inspected the employee handbook to determine that an employee sanction procedure was in place communicating that an employee may be terminated for noncompliance with a policy and / or procedure. | No exceptions noted. |
| CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | | | |
| CC1.2.1 | The board of directors establishes and maintains a formal charter and set of bylaws which describes their responsibilities and oversight of management's system of internal control. | Inspected the audit committee charter, board of director bylaws, and the members of the board of directors to determine that the board of directors established and maintained a formal charter and set of bylaws which described their responsibilities and oversight of management's system of internal control. | No exceptions noted. |
| CC1.2.2 | The board of directors has members who are independent from management, as in accordance with the board of directors' bylaws, and are objective in evaluations and decision making. | Inspected the audit committee charter, board of director bylaws, and the members of the board of directors to determine that the board of directors had members who were independent from management and were objective in evaluations and decision making. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|---|----------------------|
| CC1.2.3 | Management compiles and provides internal control performance metrics to the board of directors on a quarterly basis. | Inspected the ISMS management review results for a sample of quarters during the period to determine that management compiled and provided internal control performance metrics to the board of directors for each quarter sampled. | No exceptions noted. |
| CC1.2.4 | An executive management team that is comprised of security personnel and executive staff meets on a quarterly basis to guide the company in managing security, availability, and confidentiality risks. | Inspected the internal audit committee performance metrics report provided to the board of directors for a sample of quarters during the period to determine that an executive management team comprised of security personnel and executive staff met to guide the company in managing security, availability, and confidentiality risks for each quarter sampled. | No exceptions noted. |
| CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | | |
| CC1.3.1 | An organizational chart is in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. This chart is communicated to employees and updated as needed. | Inquired of the compliance manager regarding the organizational structure to determine that an organizational chart was in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system and that the organizational chart was communicated to employees and updated as needed. | No exceptions noted. |
| | | Inspected the organizational chart on the company intranet to determine that an organizational chart was in place and communicated to employees via the company intranet. | No exceptions noted. |
| CC1.3.2 | Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs. | Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each job sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|--|--|----------------------|
| CC1.3.3 | Management compiles and provides internal control performance metrics to the board of directors on a quarterly basis. | Inspected the ISMS management review results for a sample of quarters during the period to determine that management compiled and provided internal control performance metrics to the board of directors for each quarter sampled. | No exceptions noted. |
| CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | | |
| CC1.4.1 | Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs. | Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each job sampled. | No exceptions noted. |
| CC1.4.2 | An information security management system policy and information security policy are formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. | Inspected the information security policy and information security management system policy to determine that an information security management system policy and information security policy were formally documented and reviewed during the period that identified information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. | No exceptions noted. |
| CC1.4.3 | U.S.-based employees must sign an employee handbook acknowledgement form after reviewing the employee handbook indicating that they have been given access to the employee manual and understand their responsibilities for adhering to the policies and procedures contained within the manual. | Inquired of the compliance manager regarding employee handbook acknowledgement to determine that U.S.-based employees signed and acknowledged the employee handbook to understand their responsibilities for adhering to the policies and procedures contained within the manual. | No exceptions noted. |
| | | Inspected the employee handbook acknowledgment for a sample of U.S.-based employees hired during the period to determine that each employee sampled indicated that they had been given access to the employee manual and understood their responsibilities for adhering to the policies and procedures contained within the manual. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|----------------------|
| CC1.4.4 | Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate security policies. | Inspected the security awareness training materials and the security awareness training completion documentation for a sample of current employees to determine that each employee sampled completed security awareness training during the period to understand their obligations and responsibilities to comply with the corporate security policies. | No exceptions noted. |
| CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | | | |
| CC1.5.1 | An organizational chart is in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. This chart is communicated to employees and updated as needed. | Inquired of the compliance manager regarding the organizational structure to determine that an organizational chart was in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system and that the organizational chart was communicated to employees and updated as needed. | No exceptions noted. |
| | | Inspected the organizational chart on the company intranet to determine that an organizational chart was in place and communicated to employees via the company intranet. | No exceptions noted. |
| CC1.5.2 | Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs. | Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each job sampled. | No exceptions noted. |
| CC1.5.3 | An employee sanction procedure is in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure. | Inspected the employee handbook to determine that an employee sanction procedure was in place communicating that an employee may be terminated for noncompliance with a policy and/or procedure. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|--|---|----------------------|
| Communication and Information | | | |
| CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | | | |
| CC2.1.1 | Documented policies and procedures are in place to guide personnel with regards to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are communicated to internal personnel via the company intranet. | Inspected the information security policies and evidence of communication via the company intranet to determine that documented information security policies and procedures were in place to guide personnel with regards to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems and were communicated to internal personnel via the company intranet. | No exceptions noted. |
| CC2.1.2 | A centralized logging system is configured to log access related events, which includes the following: <ul style="list-style-type: none"> Account management Logon events Object access Policy change Privileged use | Inspected the centralized monitoring system configurations and an example log generated during the period to determine that a centralized logging system was configured to log access related events, which included the following: <ul style="list-style-type: none"> Account management Logon events Object access Policy change Privileged use | No exceptions noted. |
| CC2.1.3 | Security monitoring tools are utilized to monitor for possible or actual security breaches. | Inquired of the compliance manager regarding security monitoring tools to determine that security monitoring tools were utilized to monitor for possible or actual security breaches. | No exceptions noted. |
| | | Inspected the security monitoring tool alerting configurations and example alerts generated during the period to determine that security monitoring tools were utilized to monitor for possible or actual security breaches. | No exceptions noted. |
| CC2.1.4 | Enterprise monitoring applications are in place to monitor the performance and availability of the in-scope systems and alert operations personnel via on-screen alert when predefined thresholds are exceeded. | Inspected the enterprise monitoring configurations and example alerts generated during the period to determine that enterprise monitoring applications were in place to monitor the performance and availability of the in-scope systems and alerted response center and data center operations personnel via on-screen alert when predefined thresholds were exceeded. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|--|----------------------|
| CC2.1.5 | Vulnerability assessments of the production environment are performed on a regular basis to identify potential security vulnerabilities. The security department reviews the results of the vulnerability assessments and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding the vulnerability assessment reviews to determine that the security department reviewed the results of the vulnerability assessments and classified, and prioritized issues identified for remediation. | No exceptions noted. |
| | | Inspected the vulnerability scan configurations, an example scan report completed during the period, and evidence of management review and prioritization of identified issues for remediation to determine that vulnerability assessments of the production environment were performed on a regular basis to identify potential security vulnerabilities and that the security department reviewed the results of the vulnerability assessments and classified and prioritized issues identified for remediation. | No exceptions noted. |
| CC2.1.6 | Penetration testing of the perimeter network and application is performed by an independent third-party vendor on an annual basis to identify potential security vulnerabilities. The security department reviews the results of the penetration test and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding penetration testing to determine that a penetration test of the perimeter network and application was performed, and that the security department reviewed the results of the penetration test and classified, and prioritized issues identified for remediation during the period. | No exceptions noted. |
| | | Inspected the penetration testing results and remediation ticket to determine that penetration testing of the perimeter network and application was performed by an independent third-party vendor to identify potential security vulnerabilities and that the security department reviewed the results of the penetration test and classified and prioritized issues identified for remediation during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|--|---|----------------------|
| CC2.1.7 | The entity's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management on at least an annual basis. | Inspected example security related advisories from the public-facing website and the most recent ISMS management review meeting minutes to determine that the entity's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management during the period. | No exceptions noted. |
| | AWS and Microsoft Azure are responsible for notifying Zscaler of unusual activity, violations, and / or security breaches identified that impact Zscaler systems and customers. | | |
| CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | | | |
| CC2.2.1 | Documented policies and procedures are in place to guide personnel with regards to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are communicated to internal personnel via the company intranet. | Inspected the information security policies and evidence of communication via the company intranet to determine that documented information security policies and procedures were in place to guide personnel with regards to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems and were communicated to internal personnel via the company intranet. | No exceptions noted. |
| CC2.2.2 | U.S.-based employees must sign an employee handbook acknowledgement form after reviewing the employee handbook indicating that they have been given access to the employee manual and understand their responsibilities for adhering to the policies and procedures contained within the manual. | Inquired of the compliance manager regarding employee handbook acknowledgement to determine that U.S.-based employees signed and acknowledged the employee handbook to understand their responsibilities for adhering to the policies and procedures contained within the manual. | No exceptions noted. |
| | | Inspected the employee handbook acknowledgment for a sample of U.S.-based employees hired during the period to determine that each employee sampled indicated that they had been given access to the employee manual and understood their responsibilities for adhering to the policies and procedures contained within the manual. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|--|---|----------------------|
| CC2.2.3 | Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate security policies. | Inspected the security awareness training materials and the security awareness training completion documentation for a sample of current employees to determine that each employee sampled completed security awareness training during the period to understand their obligations and responsibilities to comply with the corporate security policies. | No exceptions noted. |
| CC2.2.4 | Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs. | Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each job sampled. | No exceptions noted. |
| CC2.2.5 | Zscaler's information security policy includes a documented procedure to identify and respond to security breaches, including threats and vulnerabilities, and other incidents. The policy is annually reviewed and updated. | Inspected the information security policy and incident response procedure to determine that Zscaler's information security policy included a documented procedure to identify and respond to security breaches, including threats and vulnerabilities, and other incidents and that the policy was reviewed and updated during the period. | No exceptions noted. |
| CC2.2.6 | Incident reporting procedures are communicated to internal users through the company's intranet. | Inspected the incident reporting procedures and the list of policies on the company's intranet to determine that incident reporting procedures were communicated to internal users through the company's intranet. | No exceptions noted. |
| CC2.2.7 | An automated ticketing system is utilized to document and track incidents and remediation activities. | Inquired of the compliance manager regarding the automated ticketing system to determine that an automated ticketing system was in place to document and track incidents and remediation activities. | No exceptions noted. |
| | | Inspected a sample of incident tickets generated during the period to determine that an automated ticketing system was utilized to document and track incidents and remediation activities for each incident sampled. | No exceptions noted. |
| | AWS and Microsoft Azure are responsible for notifying Zscaler of unusual activity, violations, and / or security breaches identified that impact Zscaler systems and customers. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|--|--|----------------------|
| CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | | | |
| CC2.3.1 | The entity's security, availability, and confidentiality principal service commitments are documented and communicated to its customers and other external users in product overview documents on the customer-facing website. | Inspected the end user subscription agreement template and product overview documents on the customer-facing website to determine that the entity's security, availability, and confidentiality principal service commitments were documented and communicated to its customers and other external users in product overview documents on the customer-facing website. | No exceptions noted. |
| CC2.3.2 | The entity's confidentiality, data retention and disposal commitments, and the associated system requirements are documented in customer contracts. | Inspected the customer contracts for a sample of customers onboarded during the period to determine that the entity's confidentiality commitments and the associated system requirements were documented in customer contracts for each customer sampled. | No exceptions noted. |
| CC2.3.3 | Signed nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties. | Inquired of the compliance manager regarding agreements to determine that vendors were required to sign nondisclosure agreements of confidentiality and protection before sharing information designated as confidential with third parties. | No exceptions noted. |
| | | Inspected the signed non-disclosure agreements for a sample of in-scope vendors to determine that signed nondisclosure agreements of confidentiality and protection were required before sharing information designated as confidential with third parties for each vendor sampled. | No exceptions noted. |
| CC2.3.4 | Incident reporting procedures are communicated to external users through the customer-facing website. | Inspected the customer-facing incident reporting portal to determine that incident reporting procedures were communicated to external users through the customer-facing website. | No exceptions noted. |
| | AWS and Microsoft Azure are responsible for notifying Zscaler of unusual activity, violations, and / or security breaches identified that impact Zscaler systems and customers. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|--|----------------------|
| Risk Assessment | | | |
| CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | | |
| CC3.1.1 | Management formally documents an organizational strategy within the ISMS policies and updates them on an annual basis to align internal control responsibilities, performance measures, and incentives with company business objectives. | Inspected the ISMS policies to determine that management formally documented an organizational strategy within the ISMS policies to align internal control responsibilities, performance measures, and incentives with company business objectives and updated them during the period. | No exceptions noted. |
| CC3.1.2 | Management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to ensure they align with the company's mission and are utilized as part of the annual risk assessment process. | Inspected the evidence of the most recent ISMS management review and the most recent risk assessment documentation to determine that management formally documented and reviewed the company's commitments and the operational, reporting, and compliance objectives to ensure they aligned with the company's mission and were utilized as part of the risk assessment process during the period. | No exceptions noted. |
| CC3.1.3 | Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | Inspected the risk assessment methodology to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | No exceptions noted. |
| CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. | | | |
| CC3.2.1 | Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | Inspected the risk assessment methodology to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|---|----------------------|
| CC3.2.2 | A formal risk assessment is performed on an annual basis. Identified risks are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review. | Inspected the evidence of the most recent ISMS management review and the most recent risk assessment documentation to determine that a formal risk assessment was performed that identified risks were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review during the period. | No exceptions noted. |
| CC3.2.3 | Risk identification includes both internal and external factors and their impact on objectives. | Inspected the ISMS objectives and the most recent risk assessment documentation to determine that risk identification included both internal and external factors and their impact on objectives. | No exceptions noted. |
| CC3.2.4 | The annual risk assessment process includes the analysis of potential threats and vulnerabilities introduced from doing business with vendors / business partners. | Inspected the most recent risk assessment documentation to determine that the risk assessment process included the analysis of potential threats and vulnerabilities introduced from doing business with vendors / business partners and performed during the period. | No exceptions noted. |
| CC3.2.5 | Management identifies and assesses criticality of information assets, including threats and vulnerabilities, during the annual risk assessment process. | Inspected the most recent risk assessment documentation to determine that management identified and assessed criticality of information assets, including threats and vulnerabilities in risk assessment process, and performed during the period. | No exceptions noted. |
| CC3.2.6 | Vulnerability assessments of the production environment are performed on a regular basis to identify potential security vulnerabilities. The security department reviews the results of the vulnerability assessments and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding the vulnerability assessment reviews to determine that the security department reviewed the results of the vulnerability assessments and classified, and prioritized issues identified for remediation. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|--|----------------------|
| | | Inspected the vulnerability scan configurations, an example scan report completed during the period, and evidence of management review and prioritization of identified issues for remediation to determine that vulnerability assessments of the production environment were performed on a regular basis to identify potential security vulnerabilities and that the security department reviewed the results of the vulnerability assessments and classified and prioritized issues identified for remediation. | No exceptions noted. |
| CC3.2.7 | Penetration testing of the perimeter network and application is performed by an independent third-party vendor on an annual basis to identify potential security vulnerabilities. The security department reviews the results of the penetration test and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding penetration testing to determine that a penetration test of the perimeter network and application was performed, and that the security department reviewed the results of the penetration test and classified, and prioritized issues identified for remediation during the period. | No exceptions noted. |
| | | Inspected the penetration testing results and remediation ticket to determine that penetration testing of the perimeter network and application was performed by an independent third-party vendor to identify potential security vulnerabilities and that the security department reviewed the results of the penetration test and classified and prioritized issues identified for remediation during the period. | No exceptions noted. |
| CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | | | |
| CC3.3.1 | Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. | Inspected the risk assessment methodology document to determine that documented policies and procedures were in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|----------------------|
| CC3.3.2 | A formal risk assessment is performed on an annual basis. Identified risks are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review. | Inspected the evidence of the most recent ISMS management review and the most recent risk assessment documentation to determine that a formal risk assessment was performed that identified risks were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review during the period. | No exceptions noted. |
| CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | | | |
| CC3.4.1 | The entity's IT security group monitors the security impact of emerging technologies, and the impact of applicable laws or regulations are considered by senior management during the annual risk assessment process. | Inspected the most recent risk assessment documentation and example security related evidence from the public-facing website to determine that the entity's IT security group monitored the security impact of emerging technologies, and the impact of applicable laws or regulations were considered by senior management in the risk assessment process and performed during the period. | No exceptions noted. |
| CC3.4.2 | Management identifies and assesses changes that could significantly impact the system of internal control during the annual risk assessment process. | Inspected the risk assessment methodology document and the most recent risk assessment documentation to determine that management identified and assessed changes that could significantly impact the system of internal control during the risk assessment process and performed during the period. | No exceptions noted. |
| CC3.4.3 | Management compiles and provides internal control performance metrics to the board of directors on a quarterly basis. | Inspected the ISMS management review results for a sample of quarters during the period to determine that management compiled and provided internal control performance metrics to the board of directors for each quarter sampled. | No exceptions noted. |
| Monitoring Activities | | | |
| CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | | | |
| CC4.1.1 | Vulnerability assessments of the production environment are performed on a regular basis to identify potential security vulnerabilities. The security department reviews the results of the vulnerability assessments and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding the vulnerability assessment reviews to determine that the security department reviewed the results of the vulnerability assessments and classified, and prioritized issues identified for remediation. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|--|----------------------|
| | | Inspected the vulnerability scan configurations, an example scan report completed during the period, and evidence of management review and prioritization of identified issues for remediation to determine that vulnerability assessments of the production environment were performed on a regular basis to identify potential security vulnerabilities and that the security department reviewed the results of the vulnerability assessments and classified and prioritized issues identified for remediation. | No exceptions noted. |
| CC4.1.2 | Penetration testing of the perimeter network and application is performed by an independent third-party vendor on an annual basis to identify potential security vulnerabilities. The security department reviews the results of the penetration test and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding penetration testing to determine that a penetration test of the perimeter network and application was performed, and that the security department reviewed the results of the penetration test and classified, and prioritized issues identified for remediation during the period. | No exceptions noted. |
| | | Inspected the penetration testing results and remediation ticket to determine that penetration testing of the perimeter network and application was performed by an independent third-party vendor to identify potential security vulnerabilities and that the security department reviewed the results of the penetration test and classified and prioritized issues identified for remediation during the period. | No exceptions noted. |
| CC4.1.3 | Internal audits are performed annually in accordance with ISO 27001 requirements. The audit results are documented and reviewed by management. | Inspected the most recent internal audit documentation and management review meeting minutes to determine that internal audits were performed in accordance with ISO 27001 requirements and that the audit results were documented and reviewed by management during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|---|----------------------|
| CC4.1.4 | The compliance team reviews vendor audit reports on an annual basis to help ensure that third-party providers are in compliance with the organization's requirements. | Inspected the most recent vendor audit review performed by the compliance team for a sample of in-scope vendors to determine that the compliance team reviewed vendor audit reports to ensure that third-party providers were in compliance with the organization's requirements for each vendor sampled during the period. | No exceptions noted. |
| CC4.1.5 | Incident response and escalation procedures are in place to guide personnel in identifying and reporting system failures, incidents, and complaints. | Inspected the incident response plan and procedure to determine that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints. | No exceptions noted. |
| CC4.1.6 | An internal collaboration tool is accessible by internal users to report incidents, concerns, and complaints. Reports of concerns are reviewed by the information security team as issues are reported. | Inquired of the compliance manager regarding security incident report reviews to determine that reports of concerns were reviewed by the information security team as issues were reported. | No exceptions noted. |
| | | Inspected the customer escalation dashboard and an example incident ticket resolved during the period to determine that a security channel was accessible by internal users to report incidents, concerns, and complaints, and that reports of concerns were reviewed by the information security team as issues were reported. | No exceptions noted. |
| CC4.1.7 | Management compiles and provides internal control performance metrics to the board of directors on a quarterly basis. | Inspected the ISMS management review results for a sample of quarters during the period to determine that management compiled and provided internal control performance metrics to the board of directors for each quarter sampled. | No exceptions noted. |
| AWS and Microsoft Azure are responsible for notifying Zscaler of unusual activity, violations, and / or security breaches identified that impact Zscaler systems and customers. | | | |
| CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. | | | |
| CC4.2.1 | Management compiles and provides internal control performance metrics to the board of directors on a quarterly basis. | Inspected the ISMS management review results for a sample of quarters during the period to determine that management compiled and provided internal control performance metrics to the board of directors for each quarter sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|--|----------------------|
| CC4.2.2 | Vulnerability assessments of the production environment are performed on a regular basis to identify potential security vulnerabilities. The security department reviews the results of the vulnerability assessments and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding the vulnerability assessment reviews to determine that the security department reviewed the results of the vulnerability assessments and classified, and prioritized issues identified for remediation. | No exceptions noted. |
| | | Inspected the vulnerability scan configurations, an example scan report completed during the period, and evidence of management review and prioritization of identified issues for remediation to determine that vulnerability assessments of the production environment were performed on a regular basis to identify potential security vulnerabilities and that the security department reviewed the results of the vulnerability assessments and classified and prioritized issues identified for remediation. | No exceptions noted. |
| CC4.2.3 | Penetration testing of the perimeter network and application is performed by an independent third-party vendor on an annual basis to identify potential security vulnerabilities. The security department reviews the results of the penetration test and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding penetration testing to determine that a penetration test of the perimeter network and application was performed, and that the security department reviewed the results of the penetration test and classified, and prioritized issues identified for remediation during the period. | No exceptions noted. |
| | | Inspected the penetration testing results and remediation ticket to determine that penetration testing of the perimeter network and application was performed by an independent third-party vendor to identify potential security vulnerabilities and that the security department reviewed the results of the penetration test and classified and prioritized issues identified for remediation during the period. | No exceptions noted. |
| CC4.2.4 | Internal audits are performed annually in accordance with ISO 27001 requirements. The audit results are documented and reviewed by management. | Inspected the most recent internal audit documentation and management review meeting minutes to determine that internal audits were performed in accordance with ISO 27001 requirements and that the audit results were documented and reviewed by management during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|---|----------------------|
| Control Activities | | | |
| CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | | | |
| CC5.1.1 | Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | Inspected the risk assessment methodology to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. | No exceptions noted. |
| CC5.1.2 | A formal risk assessment is performed on an annual basis. Identified risks are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review. | Inspected the evidence of the most recent ISMS management review and the most recent risk assessment documentation to determine that a formal risk assessment was performed that identified risks were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review during the period. | No exceptions noted. |
| CC5.1.3 | Risks are formally documented, rated using a risk evaluation process, mitigation strategies and control activities developed for management review. | Inspected the most recent risk assessment documentation for identified risks and the most recent ISMS management review meeting minutes to determine that risks were formally documented, rated using a risk evaluation process, and mitigation strategies developed for management review. | No exceptions noted. |
| CC5.1.4 | Assigned risk owners select and develop control activities, documented in the mitigation plans, to mitigate the risks identified during the annual risk assessment process. | Inspected the most recent risk assessment documentation to determine that assigned risk owners selected and developed control activities, documented in the mitigation plans, to mitigate the risks identified in risk assessment process and performed during the period. | No exceptions noted. |
| CC5.1.5 | A statement of applicability aligned with the requirements of ISO 27001 is in place to document the linkage to the security controls. The statement of applicability is updated on an annual basis in conjunction with the risk assessment process. | Inspected the statement of applicability to determine that a statement of applicability aligned with the requirements of ISO 27001 was in place to document the linkage to the security controls and that the statement of applicability was updated in conjunction with the risk assessment process during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|--|---|----------------------|
| CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | | | |
| CC5.2.1 | Documented policies and procedures are in place to guide personnel with regard to the design and development of general technology control activities. | Inspected the information security policy and ISMS policy to determine that documented policies and procedures were in place to guide personnel with regard to the design and development of general technology control activities. | No exceptions noted. |
| CC5.2.2 | Assigned risk owners select and develop control activities over technology, documented in the mitigation plans, to mitigate the risks identified during the annual risk assessment process. | Inspected the most recent risk assessment documentation to determine that assigned risk owners selected and developed control activities over technology, documented in the mitigation plans, to mitigate the risks identified in the risk assessment process and performed during the period. | No exceptions noted. |
| CC5.2.3 | A statement of applicability aligned with the requirements of ISO 27001 is in place to document the linkage to the security controls. The statement of applicability is updated on an annual basis in conjunction with the risk assessment process. | Inspected the statement of applicability to determine that a statement of applicability aligned with the requirements of ISO 27001 was in place to document the linkage to the security controls and that the statement of applicability was updated in conjunction with the risk assessment process during the period. | No exceptions noted. |
| CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | | | |
| CC5.3.1 | Documented policies and procedures are in place to guide personnel with regards to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are communicated to internal personnel via the company intranet. | Inspected the information security policies and evidence of communication via the company intranet to determine that documented information security policies and procedures were in place to guide personnel with regards to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems and were communicated to internal personnel via the company intranet. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|--|----------------------|
| CC5.3.2 | An information security management system policy and information security policy are formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. | Inspected the information security policy and information security management system policy to determine that an information security management system policy and information security policy were formally documented and reviewed during the period that identified information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. | No exceptions noted. |
| CC5.3.3 | Operating policies and procedures are documented, updated on an annual basis, and communicated to relevant stakeholders that define information system baseline requirements, establish, and monitor alarm levels, and select measures, analytic techniques, and tools to be used in managing system security, availability, and confidentiality. | Inspected the information security policies and procedures available on the corporate intranet to determine that operating policies and procedures were documented, updated during the period, and communicated to relevant stakeholders that define information system baseline requirements, establish, and monitor alarm levels, and select measures, analytic techniques, and tools to be used in managing system security, availability, and confidentiality. | No exceptions noted. |
| CC5.3.4 | An employee sanction procedure is in place communicating that an employee may be terminated for noncompliance with a policy and / or procedure. | Inspected the employee handbook to determine that an employee sanction procedure was in place communicating that an employee may be terminated for noncompliance with a policy and / or procedure. | No exceptions noted. |
| Logical and Physical Access Controls | | | |
| CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. | | | |
| CC6.1.1 | Access requests to systems are documented on a standard access request form. | Inspected the access request documentation for a sample of employees hired during the period to determine that access requests to systems were documented on a standard access request form for each employee sampled. | No exceptions noted. |
| CC6.1.2 | The in-scope systems are configured to authenticate users with unique user credentials, enforce minimum password requirements, MFA, or SSH. | Inspected the SSH key, password, and authentication configurations for a sample of in-scope production systems to determine that each in-scope system sampled was configured to authenticate users with unique user credentials, SSH keys, and enforce predefined user account and minimum password requirements. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|--|----------------------|
| CC6.1.3 | Administrative access privileges within the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the listing of administrative users for the in-scope systems with the assistance of compliance manager to determine that administrative access privileges within the in-scope systems were restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| CC6.1.4 | Predefined security groups are utilized to assign role-based access privileges and segregate access to data for the in-scope systems. | Inspected the user account listings of the in-scope systems to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data for the in-scope systems. | No exceptions noted. |
| CC6.1.5 | A centralized logging system is configured to log access related events, which includes the following: <ul style="list-style-type: none"> Account management Logon events Object access Policy change Privileged use | Inspected the centralized monitoring system configurations and an example log generated during the period to determine that a centralized logging system was configured to log access related events, which included the following: <ul style="list-style-type: none"> Account management Logon events Object access Policy change Privileged use | No exceptions noted. |
| CC6.1.6 | The in-scope systems are configured to encrypt or tokenize confidential data at rest. | Inspected the data encryption configurations of the in-scope systems to determine that the in-scope systems were configured to encrypt confidential data at rest. | No exceptions noted. |
| CC6.1.7 | An information security and acceptable use policy are in place to guide personnel in the use of information assets. | Inspected the information security policies to determine that an information security and acceptable use policy were in place to guide personnel in the use of information assets. | No exceptions noted. |
| CC6.1.8 | A public key infrastructure / key management system is in place within the in-scope systems where: <ul style="list-style-type: none"> Keys are created on a secure system Keys access is restricted Keys are distributed securely | Inspected public key infrastructure / key management system policy and key management configurations for in-scope systems and determined that a key management system was in place within the in-scope systems where: <ul style="list-style-type: none"> Keys are created on a secure system Keys access is restricted Keys are distributed securely | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|--|--|----------------------|
| | AWS and Microsoft Azure are responsible for monitoring and managing the logical access control systems to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zscaler applications reside. | | |
| CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. | | | |
| CC6.2.1 | Access requests to systems are documented on a standard access request form. | Inspected the access request documentation for a sample of employees hired during the period to determine that access requests to systems were documented on a standard access request form for each employee sampled. | No exceptions noted. |
| CC6.2.2 | User access reviews for the in-scope systems are performed on at least a quarterly basis to help ensure that access to data is restricted to authorized personnel. | Inspected the user access review documentation for a sample of quarters during the period to determine that user access reviews for the in-scope systems were performed to ensure that access to data was restricted to authorized personnel for each quarter sampled. | No exceptions noted. |
| CC6.2.3 | IT personnel revoke terminated employees' access to the in-scope systems as a component of the termination process. | Inspected the termination ticketing documentation with the assistance of compliance manager for the in-scope systems for a sample of employees terminated during the period to determine that IT personnel revoked terminated employees' access to the in-scope systems as a component of the termination process for each employee sampled. | No exceptions noted. |
| CC6.2.4 | Documented access control policies and procedures are in place to guide personnel in the external user access provisioning process. | Inspected the access control procedures to determine that documented access control policies and procedures were in place to guide personnel in the external user access provisioning process. | No exceptions noted. |
| CC6.2.5 | A ticketing system is utilized to track the status of customer onboarding activities. | Inspected the onboarding ticketing documentation for a sample of customers provisioned during the period to determine that a ticketing system was utilized to track the status of customer onboarding activities for each customer sampled. | No exceptions noted. |
| | AWS and Microsoft Azure are responsible for monitoring and managing the logical access control systems to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zscaler applications reside. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|--|--|----------------------|
| CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | | | |
| CC6.3.1 | Access requests to systems are documented on a standard access request form. | Inspected the access request documentation for a sample of employees hired during the period to determine that access requests to systems were documented on a standard access request form for each employee sampled. | No exceptions noted. |
| CC6.3.2 | The in-scope systems are configured to authenticate users with unique user credentials, enforce minimum password requirements, MFA, or SSH keys. | Inspected the SSH key, password, and authentication configurations for a sample of in-scope production systems to determine that the in-scope systems were configured to authenticate users with unique user credentials, SSH keys, and enforce predefined user account and minimum password requirements. | No exceptions noted. |
| CC6.3.3 | Administrative access privileges within the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the listing of administrative users to the in-scope systems with the assistance of compliance manager to determine that administrative access privileges within the in-scope systems were restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| CC6.3.4 | Predefined security groups are utilized to assign role-based access privileges and segregate access to data for the in-scope systems. | Inspected the user account listings of the in-scope systems to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data for the in-scope systems. | No exceptions noted. |
| CC6.3.5 | User access reviews for the in-scope systems are performed on at least a quarterly basis to help ensure that access to data is restricted to authorized personnel. | Inspected the user access review documentation for a sample of quarters during the period to determine that user access reviews for the in-scope systems were performed to ensure that access to data was restricted to authorized personnel for each quarter sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|--|----------------------|
| CC6.3.6 | IT personnel revoke terminated employees' access to the in-scope systems as a component of the termination process. | Inspected the termination ticketing documentation with the assistance of compliance manager for the in-scope systems for a sample of employees terminated during the period to determine that IT personnel revoked terminated employees' access to the in-scope systems as a component of the termination process for each employee sampled. | No exceptions noted. |
| AWS and Microsoft Azure are responsible for monitoring and managing the logical access control systems to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zscaler applications reside. | | | |
| CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. | | | |
| | The third-party data centers, AWS, and Microsoft Azure are responsible for restricting physical access to data center facilities, backup media, and other system components including routers and servers. | | |
| CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | | | |
| CC6.5.1 | Media handling and disposal procedures are in place to guide personnel in the removal of data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable. | Inspected the information security policy to determine that media handling and disposal procedures were in place to guide personnel in removal of data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable. | No exceptions noted. |
| CC6.5.2 | A third-party vendor provides a certificate of destruction when physical production assets in the data centers require physical destruction. | Inspected an example media destruction certificate to determine that a third-party vendor provided a certificate of destruction when physical production assets in the data centers required physical destruction. | No exceptions noted. |
| CC6.5.3 | Customer data is retained and deleted upon termination or expiration of the subscription term in accordance with the end user subscription agreement. | Inquired of the compliance manager regarding the disposal of customer data to determine that customer data was retained and deleted upon termination or expiration of the subscription term in accordance with the end user subscription agreement. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|--|----------------------|
| | | Inspected the customer data retention and deletion process configurations and termination tickets for a sample customers terminated during the period to determine that customer data was retained and deleted upon termination or expiration of the subscription term in accordance with the end user subscription agreement for each customer sampled. | No exceptions noted. |
| | AWS and Microsoft Azure are responsible for monitoring and managing the logical access control systems to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zscaler applications reside. | | |
| | The third-party data centers, AWS, and Microsoft Azure are responsible for restricting physical access to data center facilities, backup media, and other system components including routers and servers. | | |
| CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | | | |
| CC6.6.1 | Security groups and firewall rules are defined on in-scope systems to filter unauthorized inbound network traffic from the Internet. | Inspected the security group configuration to determine that security groups were defined on in-scope systems to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |
| CC6.6.2 | Web servers utilize TLS encryption for web communication sessions. | Inspected the TLS certificate for an example web server to determine that web servers utilized TLS encryption for web communication sessions. | No exceptions noted. |
| CC6.6.3 | Security monitoring tools are utilized to monitor for possible or actual security breaches. | Inquired of the compliance manager regarding security monitoring tools to determine that security monitoring tools were utilized to monitor for possible or actual security breaches. | No exceptions noted. |
| | | Inspected the security monitoring tool alerting configurations and example alerts generated during the period to determine that security monitoring tools were utilized to monitor for possible or actual security breaches. | No exceptions noted. |
| CC6.6.4 | Vulnerability assessments of the production environment are performed on a regular basis to identify potential security vulnerabilities. The security department reviews the results of the vulnerability assessments and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding the vulnerability assessment reviews to determine that the security department reviewed the results of the vulnerability assessments and classified, and prioritized issues identified for remediation. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|--|----------------------|
| | | Inspected the vulnerability scan configurations, an example scan report completed during the period, and evidence of management review and prioritization of identified issues for remediation to determine that vulnerability assessments of the production environment were performed on a regular basis to identify potential security vulnerabilities and that the security department reviewed the results of the vulnerability assessments and classified and prioritized issues identified for remediation. | No exceptions noted. |
| CC6.6.5 | Penetration testing of the perimeter network and application is performed by an independent third-party vendor on an annual basis to identify potential security vulnerabilities. The security department reviews the results of the penetration test and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding penetration testing to determine that a penetration test of the perimeter network and application was performed, and that the security department reviewed the results of the penetration test and classified, and prioritized issues identified for remediation during the period. | No exceptions noted. |
| | | Inspected the penetration testing results and remediation ticket to determine that penetration testing of the perimeter network and application was performed by an independent third-party vendor to identify potential security vulnerabilities and that the security department reviewed the results of the penetration test and classified and prioritized issues identified for remediation during the period. | No exceptions noted. |
| CC6.6.6 | An encrypted VPN is utilized for remote access to help ensure the privacy and integrity of the data passing over public networks. | Inquired of the compliance manager regarding VPN encryption to determine that an encrypted VPN was utilized for remote access to help ensure the privacy and integrity of the data passing over public networks. | No exceptions noted. |
| | | Inspected the VPN system configurations to determine that an encrypted VPN was utilized for remote access to ensure the privacy and integrity of the data passing over public networks. | No exceptions noted. |
| | AWS and Microsoft Azure are responsible for monitoring and managing the logical access control systems to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zscaler applications reside. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|--|----------------------|
| CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | | | |
| CC6.7.1 | Policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted. | Inspected the information handling policy to determine that policies were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted. | No exceptions noted. |
| CC6.7.2 | Security groups and firewall rules are defined on in-scope systems to filter unauthorized inbound network traffic from the Internet. | Inspected the security group configuration to determine that security groups were defined on in-scope systems to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |
| CC6.7.3 | Web servers utilize TLS encryption for web communication sessions. | Inspected the TLS certificate for an example web server to determine that web servers utilized TLS encryption for web communication sessions. | No exceptions noted. |
| CC6.7.4 | Vulnerability assessments of the production environment are performed on a regular basis to identify potential security vulnerabilities. The security department reviews the results of the vulnerability assessments and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding the vulnerability assessment reviews to determine that the security department reviewed the results of the vulnerability assessments and classified, and prioritized issues identified for remediation. | No exceptions noted. |
| | | Inspected the vulnerability scan configurations, an example scan report completed during the period, and evidence of management review and prioritization of identified issues for remediation to determine that vulnerability assessments of the production environment were performed on a regular basis to identify potential security vulnerabilities and that the security department reviewed the results of the vulnerability assessments and classified and prioritized issues identified for remediation. | No exceptions noted. |
| CC6.7.5 | Penetration testing of the perimeter network and application is performed by an independent third-party vendor on an annual basis to identify potential security vulnerabilities. The security department reviews the results of the penetration test and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding penetration testing to determine that a penetration test of the perimeter network and application was performed, and that the security department reviewed the results of the penetration test and classified, and prioritized issues identified for remediation during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|--|----------------------|
| | | Inspected the penetration testing results and remediation ticket to determine that penetration testing of the perimeter network and application was performed by an independent third-party vendor to identify potential security vulnerabilities and that the security department reviewed the results of the penetration test and classified and prioritized issues identified for remediation during the period. | No exceptions noted. |
| CC6.7.6 | An encrypted VPN is utilized for remote access to help ensure the privacy and integrity of the data passing over public networks. | Inquired of the compliance manager regarding VPN encryption to determine that an encrypted VPN was utilized for remote access to help ensure the privacy and integrity of the data passing over public networks. | No exceptions noted. |
| | | Inspected the VPN system configurations to determine that an encrypted VPN was utilized for remote access to ensure the privacy and integrity of the data passing over public networks. | No exceptions noted. |
| AWS and Microsoft Azure are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Zscaler systems reside. | | | |
| CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. | | | |
| CC6.8.1 | Vulnerability assessments of the production environment are performed on a regular basis to identify potential security vulnerabilities. The security department reviews the results of the vulnerability assessments and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding the vulnerability assessment reviews to determine that the security department reviewed the results of the vulnerability assessments and classified, and prioritized issues identified for remediation. | No exceptions noted. |
| | | Inspected the vulnerability scan configurations, an example scan report completed during the period, and evidence of management review and prioritization of identified issues for remediation to determine that vulnerability assessments of the production environment were performed on a regular basis to identify potential security vulnerabilities and that the security department reviewed the results of the vulnerability assessments and classified and prioritized issues identified for remediation. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|---|----------------------|
| CC6.8.2 | Penetration testing of the perimeter network and application is performed by an independent third-party vendor on an annual basis to identify potential security vulnerabilities. The security department reviews the results of the penetration test and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding penetration testing to determine that a penetration test of the perimeter network and application was performed, and that the security department reviewed the results of the penetration test and classified, and prioritized issues identified for remediation during the period. | No exceptions noted. |
| | | Inspected the penetration testing results and remediation ticket to determine that penetration testing of the perimeter network and application was performed by an independent third-party vendor to identify potential security vulnerabilities and that the security department reviewed the results of the penetration test and classified and prioritized issues identified for remediation during the period. | No exceptions noted. |
| CC6.8.3 | Version control software is utilized to restrict access to application source code, provide rollback capabilities, and enforce segregation of duties. | Inspected the list of builds on the version control software to determine that version control software was utilized to restrict access to application source code, provide rollback capabilities, and enforce segregation of duties. | No exceptions noted. |
| CC6.8.4 | Write access to the version control software is restricted to user accounts accessible by authorized personnel. | Inquired of the senior program manager regarding write access to the version control software to determine that write access to the version control software was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| | | Inspected the version control software user account listings to determine that write access to version control software was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| CC6.8.5 | The ability to implement changes to the production environment is restricted to authorized personnel. | Inquired of the senior program manager regarding the ability to implement changes to the production environment to determine that the ability to implement changes to the production environment was restricted to authorized personnel. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|---|----------------------|
| | | Inspected the user listings for the deployment tools and the code repositories to determine that the ability to implement changes to the production environment was restricted to authorized personnel. | No exceptions noted. |
| System Operations | | | |
| CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. | | | |
| CC7.1.1 | Enterprise monitoring applications are in place to monitor the performance and availability of the in-scope systems and alert operations personnel via on-screen alert when predefined thresholds are exceeded. | Inspected the enterprise monitoring configurations and example alerts generated during the period to determine that enterprise monitoring applications were in place to monitor the performance and availability of the in-scope systems and alerted response center and data center operations personnel via on-screen alert when predefined thresholds were exceeded. | No exceptions noted. |
| CC7.1.2 | The monitoring tools are configured to send alert notifications to operations personnel when predefined thresholds are exceeded on monitored systems. | Inspected the monitoring tools configurations and example e-mail alerts generated during the period to determine that the monitoring tools were configured to send e-mail alert notifications to operations personnel when predefined thresholds were exceeded on monitored systems. | No exceptions noted. |
| CC7.1.3 | Operations personnel monitor the enterprise monitoring applications for reported events on a 24x7x365 basis. | Inquired of the compliance manager regarding enterprise monitoring to determine that operations personnel monitored the enterprise monitoring applications for reported events on a 24x7x365 basis. | No exceptions noted. |
| | | Inspected the enterprise monitoring dashboard and operations personnel shift schedule during the period to determine that operations personnel monitored the enterprise monitoring applications for reported events on a 24x7x365 basis. | No exceptions noted. |
| CC7.1.4 | Customer incidents are reported and are tracked within an automated ticketing system to manage system incidents, response, and resolution. | Inquired of the compliance manager regarding customer incident management to determine that customer incidents were reported and tracked within an automated ticketing system to manage system incidents, response, and resolution. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|--|----------------------|
| | | Inspected the incident reporting tool and a sample of customer incident tickets generated during the period to determine that customer incidents were reported and tracked within an automated ticketing system to manage system incidents, response, and resolution for each incident sampled. | No exceptions noted. |
| CC7.1.5 | Vulnerability assessments of the production environment are performed on a regular basis to identify potential security vulnerabilities. The security department reviews the results of the vulnerability assessments and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding the vulnerability assessment reviews to determine that the security department reviewed the results of the vulnerability assessments and classified, and prioritized issues identified for remediation. | No exceptions noted. |
| | | Inspected the vulnerability scan configurations, an example scan report completed during the period, and evidence of management review and prioritization of identified issues for remediation to determine that vulnerability assessments of the production environment were performed on a regular basis to identify potential security vulnerabilities and that the security department reviewed the results of the vulnerability assessments and classified and prioritized issues identified for remediation. | No exceptions noted. |
| CC7.1.6 | Penetration testing of the perimeter network and application is performed by an independent third-party vendor on an annual basis to identify potential security vulnerabilities. The security department reviews the results of the penetration test and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding penetration testing to determine that a penetration test of the perimeter network and application was performed, and that the security department reviewed the results of the penetration test and classified, and prioritized issues identified for remediation during the period. | No exceptions noted. |
| | | Inspected the penetration testing results and remediation ticket to determine that penetration testing of the perimeter network and application was performed by an independent third-party vendor to identify potential security vulnerabilities and that the security department reviewed the results of the penetration test and classified and prioritized issues identified for remediation during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|--|---|----------------------|
| CC7.1.7 | <p>A centralized logging system is configured to log access related events, which includes the following:</p> <ul style="list-style-type: none"> • Account management • Logon events • Object access • Policy change • Privileged use | <p>Inspected the centralized monitoring system configurations and an example log generated during the period to determine that a centralized logging system was configured to log access related events, which included the following:</p> <ul style="list-style-type: none"> • Account management • Logon events • Object access • Policy change • Privileged use | No exceptions noted. |
| <p>AWS and Microsoft Azure are responsible for monitoring any configuration changes of the logical access controls system for the underlying network, virtualization management, and storage devices where the Zscaler's applications reside.</p> | | | |
| <p>CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p> | | | |
| CC7.2.1 | <p>Incident response and escalation procedures are in place to guide personnel in identifying and reporting system failures, incidents, and complaints.</p> | <p>Inspected the incident response plan and procedure to determine that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints.</p> | No exceptions noted. |
| CC7.2.2 | <p>A centralized logging system is configured to log access related events, which includes the following:</p> <ul style="list-style-type: none"> • Account management • Logon events • Object access • Policy change • Privileged use | <p>Inspected the centralized monitoring system configurations and an example log generated during the period to determine that a centralized logging system was configured to log access related events, which included the following:</p> <ul style="list-style-type: none"> • Account management • Logon events • Object access • Policy change • Privileged use | No exceptions noted. |
| CC7.2.3 | <p>Enterprise monitoring applications are in place to monitor the performance and availability of the in-scope systems and alert operations personnel via on-screen alert when predefined thresholds are exceeded.</p> | <p>Inspected the enterprise monitoring configurations and example alerts generated during the period to determine that enterprise monitoring applications were in place to monitor the performance and availability of the in-scope systems and alerted response center and data center operations personnel via on-screen alert when predefined thresholds were exceeded.</p> | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|--|----------------------|
| CC7.2.4 | The monitoring tools are configured to send alert notifications to operations personnel when predefined thresholds are exceeded on monitored systems. | Inspected the monitoring tools configurations and example e-mail alerts generated during the period to determine that the monitoring tools were configured to send e-mail alert notifications to operations personnel when predefined thresholds were exceeded on monitored systems. | No exceptions noted. |
| CC7.2.5 | Security monitoring tools are utilized to monitor for possible or actual security breaches. | Inquired of the compliance manager regarding security monitoring tools to determine that security monitoring tools were utilized to monitor for possible or actual security breaches. | No exceptions noted. |
| | | Inspected the security monitoring tool alerting configurations and example alerts generated during the period to determine that security monitoring tools were utilized to monitor for possible or actual security breaches. | No exceptions noted. |
| CC7.2.6 | Vulnerability assessments of the production environment are performed on a regular basis to identify potential security vulnerabilities. The security department reviews the results of the vulnerability assessments and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding the vulnerability assessment reviews to determine that the security department reviewed the results of the vulnerability assessments and classified, and prioritized issues identified for remediation. | No exceptions noted. |
| | | Inspected the vulnerability scan configurations, an example scan report completed during the period, and evidence of management review and prioritization of identified issues for remediation to determine that vulnerability assessments of the production environment were performed on a regular basis to identify potential security vulnerabilities and that the security department reviewed the results of the vulnerability assessments and classified and prioritized issues identified for remediation. | No exceptions noted. |
| CC7.2.7 | Penetration testing of the perimeter network and application is performed by an independent third-party vendor on an annual basis to identify potential security vulnerabilities. The security department reviews the results of the penetration test and classifies and prioritizes issues identified for remediation. | Inquired of the compliance manager regarding penetration testing to determine that a penetration test of the perimeter network and application was performed, and that the security department reviewed the results of the penetration test and classified, and prioritized issues identified for remediation during the period. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|--|---|----------------------|
| | | Inspected the penetration testing results and remediation ticket to determine that penetration testing of the perimeter network and application was performed by an independent third-party vendor to identify potential security vulnerabilities and that the security department reviewed the results of the penetration test and classified and prioritized issues identified for remediation during the period. | No exceptions noted. |
| | The third-party data centers, AWS and Microsoft Azure are responsible for restricting physical access to data center facilities, backup media, and other system components including routers and servers. | | |
| | AWS and Microsoft Azure are responsible for monitoring and managing the logical access control systems to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Zscaler applications reside. | | |
| CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. | | | |
| CC7.3.1 | Incident response and escalation procedures are in place to guide personnel in identifying and reporting system failures, incidents, and complaints. | Inspected the incident response plan and procedure to determine that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints. | No exceptions noted. |
| CC7.3.2 | An automated ticketing system is utilized to document and track incidents and remediation activities. | Inquired of the compliance manager regarding the automated ticketing system to determine that an automated ticketing system was in place to document and track incidents and remediation activities. | No exceptions noted. |
| | | Inspected a sample of incident tickets generated during the period to determine that an automated ticketing system was utilized to document and track incidents and remediation activities for each incident sampled. | No exceptions noted. |
| CC7.3.3 | Incidents requiring a change to the system follow the standard change control process. | Inquired of the compliance manager regarding incidents requiring changes to the system to determine that incidents requiring a change to the system followed the standard change control process. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|--|---|----------------------|
| | | Inspected the change ticketing documentation for a sample of incidents that required changes to the system implemented during the period to determine that incidents requiring a change to the system followed the standard change control process for each change sampled. | No exceptions noted. |
| CC7.3.4 | Security monitoring tools are utilized to monitor for possible or actual security breaches. | Inquired of the compliance manager regarding security monitoring tools to determine that security monitoring tools were utilized to monitor for possible or actual security breaches. | No exceptions noted. |
| | | Inspected the security monitoring tool alerting configurations and example alerts generated during the period to determine that security monitoring tools were utilized to monitor for possible or actual security breaches. | No exceptions noted. |
| CC7.3.5 | Customer incidents are reported and are tracked within an automated ticketing system to manage system incidents, response, and resolution. | Inquired of the compliance manager regarding customer incident management to determine that customer incidents were reported and tracked within an automated ticketing system to manage system incidents, response, and resolution. | No exceptions noted. |
| | | Inspected the incident reporting tool and a sample of customer incident tickets generated during the period to determine that customer incidents were reported and tracked within an automated ticketing system to manage system incidents, response, and resolution for each incident sampled. | No exceptions noted. |
| AWS and Microsoft Azure are responsible for notifying Zscaler of unusual activity, violations, and/or security breaches identified that impact Zscaler systems and customers. | | | |
| CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | | | |
| CC7.4.1 | Incident response and escalation procedures are in place to guide personnel in identifying and reporting system failures, incidents, and complaints. | Inspected the incident response plan and procedure to determine that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|----------------------|
| CC7.4.2 | An automated ticketing system is utilized to document and track incidents and remediation activities. | Inquired of the compliance manager regarding the automated ticketing system to determine that an automated ticketing system was in place to document and track incidents and remediation activities. | No exceptions noted. |
| | | Inspected a sample of incident tickets generated during the period to determine that an automated ticketing system was utilized to document and track incidents and remediation activities for each incident sampled. | No exceptions noted. |
| CC7.4.3 | Customer incidents are reported and are tracked within an automated ticketing system to manage system incidents, response, and resolution. | Inquired of the compliance manager regarding customer incident management to determine that customer incidents were reported and tracked within an automated ticketing system to manage system incidents, response, and resolution. | No exceptions noted. |
| | | Inspected the incident reporting tool and a sample of customer incident tickets generated during the period to determine that customer incidents were reported and tracked within an automated ticketing system to manage system incidents, response, and resolution for each incident sampled. | No exceptions noted. |
| | AWS and Microsoft Azure are responsible for notifying Zscaler of unusual activity, violations, and/or security breaches identified that impact Zscaler systems and customers. | | |
| CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents. | | | |
| CC7.5.1 | Incident response and escalation procedures are in place to guide personnel in identifying and reporting system failures, incidents, and complaints. | Inspected the incident response plan and procedure to determine that incident response and escalation policies were in place to guide personnel in identifying and reporting system failures, incidents, and complaints. | No exceptions noted. |
| CC7.5.2 | Incidents requiring a change to the system follow the standard change control process. | Inquired of the compliance manager regarding incidents requiring changes to the system to determine that incidents requiring a change to the system followed the standard change control process. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|---|----------------------|
| | | Inspected the change ticketing documentation for a sample of incidents that required changes to the system implemented during the period to determine that incidents requiring a change to the system followed the standard change control process for each change sampled. | No exceptions noted. |
| CC7.5.3 | Automated replication systems are configured to perform near real-time replication of production data. | Inspected the replication system configurations for a sample of production databases to determine that automated replication systems were configured to perform near real-time replication of production data for each database sampled. | No exceptions noted. |
| CC7.5.4 | The automated replication systems are configured to send e-mail alert notifications to operations personnel when replication issues are identified. | Inquired of the compliance manager regarding replication alerting to determine that the automated replication system was configured to send e-mail alert notifications to operations personnel when replication issues were identified. | No exceptions noted. |
| | | Inspected the replication system alerting configurations and an example e-mail alert notification generated during the period to determine that the automated replication system was configured to send e-mail alert notifications to operations personnel when replication issues were identified. | No exceptions noted. |
| CC7.5.5 | Zscaler has a documented procedure that includes procedures to align the company's disaster recovery and business continuity plans with customer commitments. | Inspected the disaster recovery and business continuity plan and the availability commitments to determine that documented procedures were in place that included procedures to align the company's disaster recovery and business continuity plans with customer commitments. | No exceptions noted. |
| CC7.5.6 | Operations personnel perform disaster recovery tests on an annual basis to help ensure the recoverability of production data. | Inspected the most recent disaster recovery testing exercise results to determine that operations personnel performed disaster recovery tests to help ensure the recoverability of production data during the period. | No exceptions noted. |
| | AWS and Microsoft Azure are responsible for notifying Zscaler of unusual activity, violations, and/or security breaches identified that impact Zscaler systems and customers. | | |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|--|--|----------------------|
| Change Management | | | |
| CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. | | | |
| CC8.1.1 | Documented policies and procedures are in place to guide personnel on the in-scope systems change management and system development life cycle (SDLC) process. | Inspected the documented change management policies and procedures to determine that documented policies and procedures were in place to guide personnel on the in-scope systems change management and SDLC process. | No exceptions noted. |
| CC8.1.2 | The cloud engineering team meets on a quarterly basis to discuss and communicate the ongoing and upcoming projects that affect the system. | Inspected the meeting minutes for a sample of quarters during the period to determine that the cloud engineering team met to discuss and communicate the ongoing and upcoming projects that affect the system for each quarter sampled. | No exceptions noted. |
| CC8.1.3 | An automated ticketing system is utilized to document and track in-scope system change requests from development through implementation. | Inspected the change ticketing documentation for a sample of application and infrastructure changes implemented during the period to determine that an automated ticketing system was utilized to document and track in-scope system change requests from development through implementation for each application and infrastructure change sampled. | No exceptions noted. |
| CC8.1.4 | Application and infrastructure changes are peer reviewed and approved prior to implementation. | Inspected the change ticketing documentation for a sample of application and infrastructure changes implemented during the period to determine that application and infrastructure changes were peer reviewed and approved prior to implementation for each application and infrastructure change sampled. | No exceptions noted. |
| CC8.1.5 | Quality assurance (QA) testing efforts are performed for application changes prior to implementation. | Inspected evidence of QA testing for a sample of application changes implemented during the period to determine that QA testing was performed for application changes prior to implementation for each application change sampled. | No exceptions noted. |
| CC8.1.6 | Development, testing, and production environments are logically separated. | Inspected the segregation of development, testing, and production environments to determine that development, testing, and production environments were logically separated. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|--|----------------------|
| CC8.1.7 | Rollback procedures are documented for application changes to revert to previous versions of code when changes impair system operation. | Inspected the version control software configurations and the change tickets for a sample of application changes implemented during the period to determine that rollback procedures were documented for application changes to revert to previous versions of code when changes impaired system operation for each application and infrastructure change sampled. | No exceptions noted. |
| CC8.1.8 | Version control software is utilized to restrict access to application source code, provide rollback capabilities, and enforce segregation of duties. | Inspected the list of builds on the version control software to determine that version control software was utilized to restrict access to application source code, provide rollback capabilities, and enforce segregation of duties. | No exceptions noted. |
| CC8.1.9 | Write access to the version control software is restricted to user accounts accessible by authorized personnel. | Inquired of the compliance manager regarding write access to the version control software to determine that write access to the version control software was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| | | Inspected the version control software user account listings with the assistance of the compliance manager to determine that write access to version control software was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| CC8.1.10 | The ability to implement changes to the production environment is restricted to authorized personnel. | Inquired of the compliance manager regarding the ability to implement changes to the production environment to determine that the ability to implement changes to the production environment was restricted to authorized personnel. | No exceptions noted. |
| | | Inspected the user listings for the deployment tools and the code repositories with the assistance of the compliance manager to determine that the ability to implement changes to the production environment was restricted to authorized personnel. | No exceptions noted. |
| CC8.1.11 | Production data is not utilized for change development and testing efforts. | Inquired of the compliance manager regarding data used in development and testing to determine that production data was not utilized for change development and testing efforts. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|--|---|----------------------|
| | | Inspected the information security policy and the segregation of development, testing, and production environments to determine that production data was not utilized for change management and testing efforts. | No exceptions noted. |
| CC8.1.12 | Emergency changes follow the same change management policies and procedures for regular application and infrastructure changes. | Inquired of the compliance manager regarding emergency changes to determine that emergency changes followed the same policies and procedures used for regular application and infrastructure changes. | No exceptions noted. |
| | | Inspected the change tickets for a sample of emergency changes implemented during the period to determine that emergency changes followed the same policies and procedures used for regular application and infrastructure changes. | No exceptions noted. |
| Risk Mitigation | | | |
| CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | | |
| CC9.1.1 | Documented policies and procedures are in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security, availability, and confidentiality of data and service. | Inspected the risk assessment methodology document to determine that documented policies and procedure were in place to guide personnel in the assessment of the potential risks and vulnerabilities and the development of control activities related to the security, availability, and confidentiality of data and service. | No exceptions noted. |
| CC9.1.2 | A formal risk assessment is performed on an annual basis. Risks of potential business disruptions that are identified are formally documented for management review, the risk assessment includes clearly documented objectives and associated risks that address the security, availability, and confidentiality of the in-scope systems. | Inspected the risk assessment documentation to determine that a formal risk assessment was performed and that risks of potential business disruptions that were identified were formally documented for management review and included clearly documented objectives and associated risks that addressed the security, availability, and confidentiality of the in-scope systems during the period. | No exceptions noted. |
| CC9.1.3 | Risk identification includes both internal and external factors and their impact on objectives. | Inspected the ISMS objectives and the most recent risk assessment documentation to determine that risk identification included both internal and external factors and their impact on objectives. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|----------------------|
| CC9.1.4 | The annual risk assessment process includes the analysis of potential threats and vulnerabilities introduced from doing business with vendors / business partners. | Inspected the most recent risk assessment documentation to determine that the risk assessment process included the analysis of potential threats and vulnerabilities introduced from doing business with vendors / business partners and performed during the period. | No exceptions noted. |
| CC9.1.5 | Management identifies and assesses criticality of information assets, including threats and vulnerabilities, during the annual risk assessment process. | Inspected the most recent risk assessment documentation to determine that management identified and assessed criticality of information assets, including threats and vulnerabilities in risk assessment process, and performed during the period. | No exceptions noted. |
| CC9.2 The entity assesses and manages risks associated with vendors and business partners. | | | |
| CC9.2.1 | Documented access control policies and procedures are in place to guide personnel in the external user access provisioning process. | Inspected the access control procedures to determine that documented access control policies and procedures were in place to guide personnel in the external user access provisioning process. | No exceptions noted. |
| CC9.2.2 | Signed nondisclosure agreements of confidentiality and protection are required before sharing information designated as confidential with third parties. | Inquired of the compliance manager to determine that vendors were required to sign nondisclosure agreements of confidentiality and protection before sharing information designated as confidential with third parties. | No exceptions noted. |
| | | Inspected the signed non-disclosure agreements for a sample of in-scope vendors to determine that signed nondisclosure agreements of confidentiality and protection were required before sharing information designated as confidential with third parties for each vendor sampled. | No exceptions noted. |
| CC9.2.3 | The compliance team reviews vendor audit reports on an annual basis to help ensure that third-party providers are in compliance with the organization's requirements. | Inspected the most recent vendor audit review performed by the compliance team for a sample of in-scope vendors to determine that the compliance team reviewed vendor audit reports to ensure that third-party providers were in compliance with the organization's requirements for each vendor sampled during the period. | No exceptions noted. |

ADDITIONAL CRITERIA FOR AVAILABILITY

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|---|----------------------|
| A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives. | | | |
| A1.1.1 | Members of the cloud operations team meet on a quarterly basis to discuss system capacity events and plan for upcoming projects that could impact the availability of systems. | Inquired of the compliance manager regarding the weekly capacity meetings to determine that members of the cloud operations team met on a quarterly basis to discuss system capacity events and planned for upcoming projects that could impact the availability of systems. | No exceptions noted. |
| | | Inspected the capacity management meeting minutes and invite for a sample of quarters during the period to determine that members of the cloud operations team met to discuss system capacity events and planned for upcoming projects that could impact the availability of systems for each quarter sampled. | No exceptions noted. |
| A1.1.2 | Enterprise monitoring applications are in place to monitor the performance and availability of the in-scope systems and alert operations personnel via on-screen alert when predefined thresholds are exceeded. | Inspected the enterprise monitoring configurations and example alerts generated during the period to determine that enterprise monitoring applications were in place to monitor the performance and availability of the in-scope systems and alerted response center and data center operations personnel via on-screen alert when predefined thresholds were exceeded. | No exceptions noted. |
| A1.1.3 | The monitoring tools are configured to send alert notifications to operations personnel when predefined thresholds are exceeded on monitored systems. | Inspected the monitoring tools configurations and example e-mail alerts generated during the period to determine that the monitoring tools were configured to send e-mail alert notifications to operations personnel when predefined thresholds were exceeded on monitored systems. | No exceptions noted. |
| A1.1.4 | Operations personnel monitor the enterprise monitoring applications for reported events on a 24x7x365 basis. | Inquired of the compliance manager regarding enterprise monitoring to determine that operations personnel monitored the enterprise monitoring applications for reported events on a 24x7x365 basis. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|----------------------|
| | | Inspected the enterprise monitoring dashboard and operations personnel shift schedule during the period to determine that operations personnel monitored the enterprise monitoring applications for reported events on a 24x7x365 basis. | No exceptions noted. |
| A1.1.5 | Customer incidents are reported and are tracked within an automated ticketing system to manage system incidents, response, and resolution. | Inquired of the compliance manager regarding customer incident management to determine that customer incidents were reported and tracked within an automated ticketing system to manage system incidents, response, and resolution. | No exceptions noted. |
| | | Inspected the incident reporting tool and a sample of customer incident tickets generated during the period to determine that customer incidents were reported and tracked within an automated ticketing system to manage system incidents, response, and resolution for each incident sampled. | No exceptions noted. |
| | The third-party data centers, AWS, and Microsoft Azure, are responsible for monitoring the capacity demand and ensuring capacity resources are available and functioning to meet Zscaler's availability commitments and requirements. | | |
| A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | | | |
| A1.2.1 | An annual risk assessment is performed to identify threats and vulnerabilities that could impair the availability of the system. | Inspected the most recent risk assessment documentation to determine that a risk assessment was performed during the period to identify threats and vulnerabilities that could impair the availability of the system. | No exceptions noted. |
| A1.2.2 | Customer incidents are reported and are tracked within an automated ticketing system to manage system incidents, response, and resolution. | Inquired of the compliance manager regarding customer incident management to determine that customer incidents were reported and tracked within an automated ticketing system to manage system incidents, response, and resolution. | No exceptions noted. |
| | | Inspected the incident reporting tool and a sample of customer incident tickets generated during the period to determine that customer incidents were reported and tracked within an automated ticketing system to manage system incidents, response, and resolution for each incident sampled. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|---|---|----------------------|
| A1.2.3 | Enterprise monitoring applications are in place to monitor the performance and availability of the in-scope systems and alert operations personnel via on-screen alert when predefined thresholds are exceeded. | Inspected the enterprise monitoring configurations and example alerts generated during the period to determine that enterprise monitoring applications were in place to monitor the performance and availability of the in-scope systems and alerted response center and data center operations personnel via on-screen alert when predefined thresholds were exceeded. | No exceptions noted. |
| A1.2.4 | The monitoring tools are configured to send alert notifications to operations personnel when predefined thresholds are exceeded on monitored systems. | Inspected the monitoring tools configurations and example e-mail alerts generated during the period to determine that the monitoring tools were configured to send e-mail alert notifications to operations personnel when predefined thresholds were exceeded on monitored systems. | No exceptions noted. |
| A1.2.5 | Documented policies and procedures are in place governing data backup and restoration processes. | Inspected the master information security policy and the disaster recovery and business continuity plan to determine that documented policies and procedures were in place governing data backup and restoration processes. | No exceptions noted. |
| A1.2.6 | Automated replication systems are configured to perform near real-time replication of production data. | Inspected the replication system configurations for a sample of production databases to determine that automated replication systems were configured to perform near real-time replication of production data for each database sampled. | No exceptions noted. |
| A1.2.7 | The automated replication systems are configured to send e-mail alert notifications to operations personnel when replication issues are identified. | Inquired of the compliance manager regarding replication alerting to determine that the automated replication system was configured to send e-mail alert notifications to operations personnel when replication issues were identified. | No exceptions noted. |
| | | Inspected the replication system alerting configurations and an example e-mail alert notification generated during the period to determine that the automated replication system was configured to send e-mail alert notifications to operations personnel when replication issues were identified. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|--|----------------------|
| A1.2.8 | Operations personnel perform disaster recovery tests on an annual basis to help ensure the recoverability of production data. | Inspected the most recent disaster recovery testing exercise results to determine that operations personnel performed disaster recovery tests to help ensure the recoverability of production data during the period. | No exceptions noted. |
| The third-party data centers, AWS, and Microsoft Azure, are responsible for ensuring the data center facilities are equipped with environmental security safeguards. | | | |
| A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | | |
| A1.3.1 | Zscaler has a documented procedure that includes procedures to align the company's disaster recovery and business continuity plans with customer commitments. | Inspected the disaster recovery and business continuity plan and the availability commitments to determine that documented procedures were in place that included procedures to align the company's disaster recovery and business continuity plans with customer commitments. | No exceptions noted. |
| A1.3.2 | Operations personnel perform disaster recovery tests on an annual basis to help ensure the recoverability of production data. | Inspected the most recent disaster recovery testing exercise results to determine that operations personnel performed disaster recovery tests to help ensure the recoverability of production data during the period. | No exceptions noted. |

ADDITIONAL CRITERIA FOR CONFIDENTIALITY

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--|---|--|----------------------|
| C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. | | | |
| C1.1.1 | The entity's confidentiality, data retention and disposal commitments, and the associated system requirements are documented in customer contracts. | Inspected the customer contracts for a sample of customers onboarded during the period to determine that the entity's confidentiality commitments and the associated system requirements were documented in customer contracts for each customer sampled. | No exceptions noted. |
| C1.1.2 | Data retention and disposal commitments, and the associated system requirements are documented in system descriptions available on the company website. | Inspected the data retention policies and product sheets communicated via the company website to determine that data retention and disposal commitments, and the associated system requirements were documented in system descriptions available on the company website. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|--|--|----------------------|
| C1.1.3 | A data classification policy is in place to define data categories, protection levels, and handling measures for information utilized within the system. | Inspected the data classification policy to determine that a data classification policy was in place to define data categories, protection levels, and handling measures for information utilized within the system. | No exceptions noted. |
| C1.1.4 | Production data is not utilized for change development and testing efforts. | Inquired of the compliance manager regarding data used in development and testing to determine that production data was not utilized for change development and testing efforts. | No exceptions noted. |
| | | Inspected the information security policy and the segregation of development, testing, and production environments to determine that production data was not utilized for change management and testing efforts. | No exceptions noted. |
| C1.1.5 | Administrative access privileges within the in-scope systems are restricted to user accounts accessible by authorized personnel. | Inspected the listing of administrative users for the in-scope systems with the assistance of compliance manager to determine that administrative access privileges within the in-scope systems were restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality. | | | |
| C1.2.1 | The entity's confidentiality, data retention and disposal commitments, and the associated system requirements are documented in customer contracts. | Inspected the customer contracts for a sample of customers onboarded during the period to determine that the entity's confidentiality commitments and the associated system requirements were documented in customer contracts for each customer sampled. | No exceptions noted. |
| C1.2.2 | Documented data disposal policies are in place to guide personnel on the procedures for retention and disposal of data. | Inspected the data disposal policies and the end user subscription agreement to determine that documented data disposal policies were in place to guide personnel on the procedures for retention and disposal of data. | No exceptions noted. |
| C1.2.3 | Customer data is retained and deleted upon termination or expiration of the subscription term in accordance with the end user subscription agreement. | Inquired of the compliance manager regarding the disposal of customer data to determine that customer data was retained and deleted upon termination or expiration of the subscription term in accordance with the end user subscription agreement. | No exceptions noted. |

| Control # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-----------|--|--|----------------------|
| | | Inspected the customer data retention and deletion process configurations and termination tickets for a sample customers terminated during the period to determine that customer data was retained and deleted upon termination or expiration of the subscription term in accordance with the end user subscription agreement for each customer sampled. | No exceptions noted. |

Certificate Of Completion

Envelope Id: 7D03D07CB710415B8FB40735562BD598

Status: Delivered

Subject: Zscaler Compliance Report - SOC 2 TYPE 2 - 2022 Nivedita Dash

Source Envelope:

Document Pages: 86

Signatures: 0

Envelope Originator:

Certificate Pages: 4

Initials: 0

Zscaler Compliance

AutoNav: Enabled

Mohali, Punjab 160059

Envelopeld Stamping: Enabled

Compliance@zscaler.com

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

IP Address: 18.208.143.40

Record Tracking

Status: Original

Holder: Zscaler Compliance

Location: DocuSign

5/25/2023 5:34:21 AM

Compliance@zscaler.com

Signer Events**Signature****Timestamp**

Nivedita Dash

Sent: 5/25/2023 5:34:26 AM

Nivedita.Dash@unilever.com

Viewed: 5/25/2023 5:44:24 AM

Security Level: Email, Account Authentication
(None), Login with SSO**Electronic Record and Signature Disclosure:**

Accepted: 5/25/2023 5:44:24 AM

ID: d738de2b-73be-410f-9834-b734a365e0ac

In Person Signer Events**Signature****Timestamp****Editor Delivery Events****Status****Timestamp****Agent Delivery Events****Status****Timestamp****Intermediary Delivery Events****Status****Timestamp****Certified Delivery Events****Status****Timestamp****Carbon Copy Events****Status****Timestamp****Witness Events****Signature****Timestamp****Notary Events****Signature****Timestamp****Envelope Summary Events****Status****Timestamps**

Envelope Sent

Hashed/Encrypted

5/25/2023 5:34:26 AM

Certified Delivered

Security Checked

5/25/2023 5:44:24 AM

Payment Events**Status****Timestamps****Electronic Record and Signature Disclosure**

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Zscaler Inc. (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Zscaler Inc.:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: smendez@zscaler.com

To advise Zscaler Inc. of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at smendez@zscaler.com and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from Zscaler Inc.

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to smendez@zscaler.com and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Zscaler Inc.

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to smendez@zscaler.com and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Zscaler Inc. as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Zscaler Inc. during the course of your relationship with Zscaler Inc..