System Organization Controls 3 (SOC 3) Report

Report on Zendesk's Description of System – Zendesk Customer Service Platform Relevant to the Security and Availability Trust Services Principles

For the Period of October 1, 2017 through March 31, 2018

Ernst & Young LLP
Suite 1600
560 Mission Street
San Francisco, CA
94104-2907

Tel: +1 415 894 8000
Fax: + 415 894 8099

Report of Independent Accountants

To the management of Zendesk, Inc.

Approach:

We have examined management's assertion that Zendesk, Inc. ("Zendesk") maintained effective controls to provide reasonable assurance that:

- the Zendesk Customer Platform Service System was protected against unauthorized access, use, or modification to achieve Zendesk's commitments and system requirements
- the Zendesk Customer Platform Service System was available for operation and use to achieve Zendesk's commitments and system requirements

during the period October 1, 2017 through March 31, 2018 based on the criteria for security and availability in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Zendesk's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Zendesk's relevant security and availability policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Zendesk's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations:

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security and availability are achieved.

Building a better working world

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

Opinion:

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

Ernst & Young LLP

May 8, 2018

zendesk

Management's Assertion Regarding the Effectiveness of Its Controls Over the Zendesk Customer Platform Service System Based on the Trust Services Principles and Criteria for Security and Availability

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

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

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

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period October 1, 2017 to March 31, 2018, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, and availability (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period October 1, 2017 to March 31, 2018 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Zendesk's commitments and system requirements
- the System was available for operation and use, to achieve Zendesk's commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the Zendesk Customer Platform Service System identifies the aspects of the Zendesk Customer Platform Service System covered by our assertion.

zendesk

Scope and Purpose of the Report

This report describes the control environment of Zendesk's cloud-based customer service platform ("Platform") for the period October 1, 2017 to March 31, 2018 for the Security and Availability Trust Services Principles.

The description is intended to provide a broad range of stakeholders with information and assurance about Zendesk's controls that affect the security and availability of the Platform that processes users' data. Stakeholders include the management or those charged with governance of the user entities and of the service organization, customers of the service organization, regulators, business partners, suppliers, and others who have an understanding of the service organization and its controls.

Company Overview

Zendesk is a cloud-based customer service platform, designed for companies that want to build customer relationships that are more meaningful, personal, and productive. Zendesk strives to bring businesses and customers closer together by enabling companies to provide great support and mature with self-service and proactive engagement. It is designed to be easy to use, customize, and scale.

Founded in 2007, Zendesk is the brainchild of three friends from Denmark who used an old kitchen door as a desk in a Copenhagen loft. They wanted to bring a bit of zen to the chaotic world of customer support through software that was nice to look at and easy to use. Since then, the company has grown, and the software powering the Platform is now built by engineers all over the world. The offices are bigger with real desks, but Zendesk has held on to the spirit with which it began: be genuine, listen to customers, and keep it beautifully simple.

Zendesk builds software for better customer relationships. It empowers organizations to improve customer engagement and better understand their customers. More than 125,000 paid customer accounts in over 160 countries and territories use Zendesk products. Based in San Francisco, Zendesk has operations in the United States, Europe, Asia, Australia, and South America. Learn more at www.zendesk.com. The company went public on May 15, 2014 and trades under the symbol NYSE: ZEN.

Services Provided

Our products allow businesses to be more reliable, flexible, and scalable. They help improve communication and make sense of massive amounts of data. Above all, they help you turn interactions into lasting relationships. These products include:

- **Support.** *Multi-channel customer service.*
    - Zendesk Support is a beautifully simple system for tracking, prioritizing and solving customer support tickets.
- **Guide.** *Knowledge base and self-service.*
    - Guide is a smart knowledge base for better self-service and empowered agents.
- **Chat.** *Live chat and messaging software.*
    - Chat provides a fast and responsive way to connect with customers in real time over websites, mobile apps, and popular messaging apps like Facebook Messenger, Twitter, and LINE.

- **Talk.** *Integrated call center software.*
  - Connect with customers on a call center solution built right into the Zendesk ticketing system.
- **Explore.** *Analytics and reporting.*
  - Zendesk Explore provides analytics to measure and understand the entire customer experience.
- **Connect + Outbound.** *Proactive campaigns.*
  - Zendesk Connect + Outbound makes customer relationships better with proactive messaging.
- **Inbox.** *Shared team inbox.*
  - Zendesk Inbox allows its customers to respond as one, talk amongst themselves and be there for its people.
- **Zendesk Apps Marketplace.** *A flexible platform that plays nice with others.*
  - Zendesk's API allows for effortless custom integrations in addition to the over 500 apps that currently plug into your tickets.
- **Embeddables.** *Bring customer support directly to your customers.*
  - Embeddables seamlessly integrate Zendesk functionality into any native environment, allowing businesses to put help right at their customers' fingertips.

Product Plans

Zendesk's family of products offer a variety of plans to connect with customers and meet the needs of any team.

- **Support.** *Multi-channel customer service.* Track, prioritize, and solve customer support tickets.

Support				
Essential	**Team**	**Professional**	**Enterprise**	**Elite**
• Email & social channels • Basic help center • Web widget & mobile SDK	Essential, plus… • Business rules • Performance dashboards • Public apps and integrations	Team, plus… • Multilingual content • CSAT surveys • Custom reports & dashboards	Professional, plus… • Custom agent roles • Multibrand support • Multiple ticket forms • Launch Success Program • Satisfaction Prediction	Enterprise, plus… • Unlimited light agents • 99.9% uptime SLA • 1-hour service level objective • Advanced encryption & security • Data center location

- **Talk.** Integrated call center software. *Call center software built right into Support.*

Talk				
Lite	**Team**	**Professional**	**Enterprise**	**Partner Edition**
• Limit of 1 phone number • Automatic ticket creation • Call recording & voicemail transcription	Lite, plus… • Multiple phone numbers • Warm transfer • Business hours • Text messaging	Team, plus… • Interactive Voice Response (IVR) phone trees • Call monitoring & barging • Callback from queue • Real-time analytics • Insights reporting	Professional, plus… • Launch Success Program • Monthly Diagnostics • Talk Usage 99.95% SLA • Failover on demand	Access to telephony integrations & CTI toolkit for: • Embedded softphone • Caller ID & history • Tickets with call data and agent assignment

- **Chat.** *Live chat software*. Chat with customers in real time.

Chat			
Lite	**Team**	**Professional**	**Enterprise**
• 1 concurrent chat • Chat rating • 30-day chat history	All Lite and… • Unlimited chats • 2 triggers • 2 departments • Widget customization • Public apps	All Team and… • Unlimited triggers • Unlimited departments • Operating hours • Chat and agent reports • Conversion Tracking • Private apps	All Professional and… • Widget unbranding • Real-time monitor • Roles and permissions • Skills-based routing • Web SDK • 24/7 support

- **Guide.** *Knowledge base and self-service*. Knowledge base software built right into Support.

Guide			
Lite	**Professional**	**Enterprise**	**Answer Bot**
• Knowledge base • Support Request form • Google Analytics reporting • Search, preview, and insert articles with the Knowledge Capture app	Lite, plus… • Custom themes • Multilingual content • Agent knowledge base • Community forums • Customer requests portal • Performance dashboards • Flag and create articles with the Knowledge Capture app	Professional, plus… • Team Publishing: Article lifecycle management, article update assignments, and publishing permissions • Content Cues to identify knowledge gaps • Multiple help centers • Integrated Knowledge Capture workflow	Add on Answer Bot to Guide Professional… • Automated replies to customers using knowledge base content • Trained deep learning models

While most customers primarily use Zendesk as an external customer service tool, it can also be leveraged by companies to provide support to their employees via internal service departments such as IT, HR, and Facilities. Zendesk aims to provide a holistic customer service tool that empowers companies to bring their employees and customers closer together through software that makes conversations easy and more productive.

System Components

The components that support the Zendesk system consist of infrastructure, software, people, processes, and data.

i. Infrastructure

Infrastructure consists of the physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks). The Zendesk Production Network is hosted in geographically distributed co-location datacenters as well as in Amazon Web Services (AWS). These datacenters consist of firewalls, switches, load balancers routers, servers, and databases that house or transmit Service Data, application code, as well as related system monitoring utilities. AWS S3 buckets contain customer ticket attachments, database backups, and logs while AWS EC2 instances are used to run proxy mediators and internally process a subset of Service Data.

Service Data is defined as any information that is created, inputted, submitted, posted, transmitted, stored, or displayed by customers, customer agents, and customers' customers – who are also referred to as Zendesk end-users.

Such information may include personal information or other sensitive information that customers, customer agents, or end-users choose to include. Service Data is subject to technical safeguards, as described in Zendesk's Master Subscription Agreement (https://www.zendesk.com/company/customers-partners/master-subscription-agreement/).

Datacenters

Zendesk utilizes globally distributed datacenters, located in the United States (US), Asia Pacific and the European Union (EU), where infrastructure is hosted. This provides customers with an option to host their Zendesk instance in a preferred geographic location, as part of the Datacenter Location Add-on. Zendesk hosts its infrastructure within Tier III+ and Tier IV third-party datacenter facilities owned and operated by RagingWire (Sacramento, California and Ashburn, Virginia), Equinix (Dublin, Ireland and Frankfurt, Germany) and Amazon Web Services (AWS) (AP Northeast, AP Southeast, US West, US East, EU Central, EU West). A Tier III+ data center includes redundant capacity components and concurrent maintainability which includes dual powered equipment and multiple uplinks. A Tier IV data center is designed to host mission critical servers and computer systems, with fully redundant subsystems (cooling, power, network links, storage, etc.) and compartmentalized security zones controlled by biometric or other access controls methods. All three providers house systems in secure, hardened facilities that employ onsite security guards, video surveillance, and biometric/keycard based access.

Pod Architecture

Each datacenter includes occurrences of the Platform, known as "Pods". These Pods help mitigate the impact of predictable failures such as hardware problems, and also allow for capacity scaling as Service Data and usage grows. Each datacenter consists of one or more Pods. Zendesk utilizes a mix of both virtualized and physical servers within a Pod.

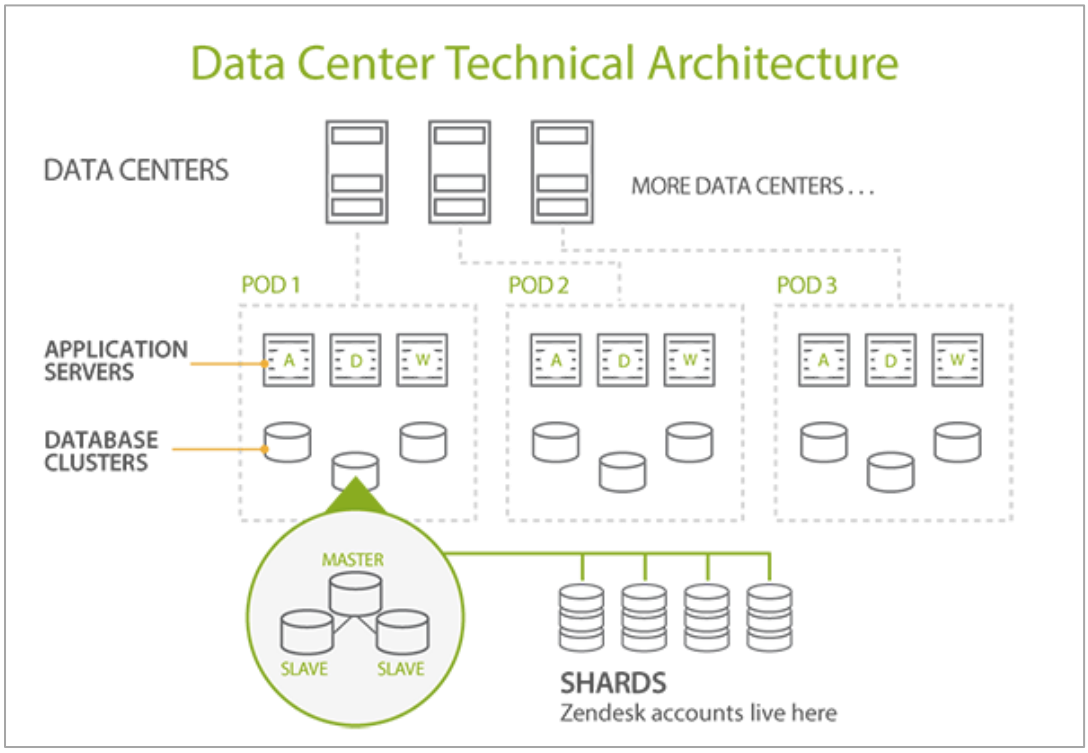
A new Zendesk customer is assigned to a specific Pod in one of the datacenters. Each Pod has the resources necessary to run Zendesk independently of the other Pods. The resources include, but are not limited to, application servers, web servers, database servers, and additional resources to handle other work such as email processing and reporting.

Sharded Database Architecture

Each Pod contains several database clusters, each cluster consists of a master database server and two database servers that continuously replicate the master. If the master unexpectedly encounters a problem, one of the spares immediately takes its place. This automated system of fault tolerance and database failover reduces the risk of downtime.

The building blocks of each database cluster are shards, which are smaller, logical databases. A sharded architecture allows Zendesk to rebalance load across physical database clusters and Pods. Zendesk has hundreds of shards distributed across database clusters worldwide. Each shard supports a certain number of customers. The number of customers within each shard varies depending on the data volumes they generate. If a customer's usage demands more capacity, Zendesk can fully dedicate a single shard or database cluster to the customer.

See below for a graphical representation of the Datacenter architecture.



Corporate Infrastructure

Zendesk's corporate infrastructure is located in its San Francisco, California headquarters and satellite offices in Copenhagen, Denmark; Dublin, Ireland; London, England; Madison, Wisconsin; Manila, Philippines; Melbourne, Australia; Montpellier, France; Palo Alto, California; Tokyo, Japan; Singapore, Singapore; Mexico City, Mexico; New York, New York' Portland, Oregon; Sao Paulo, Brazil; Bangalore, India; Bangkok, Thailand; Jakarta, Indonesia; Seoul, South Korea; Sydney, Australia; Berlin, Germany; and Paris, France. Employees connect remotely to the Zendesk Production Network through a Virtual Private Network (VPN) tunnel and must authenticate into the Zendesk Production systems using a valid, unique SSH key.

ii. Software

Software consists of the application programs and IT system software that supports application programs (operating systems, middleware, and utilities). Zendesk's software stack consists of Linux servers running Nginx and MySQL databases. Zendesk has a PXE (pre-boot execution environment) server containing the latest Linux distribution image, and it is updated daily to ensure it includes the latest patches and updates. This is also used to update and manage a standard build image for *new* server deployments. The configuration management tool actively manages the infrastructure configuration across servers. Ruby on Rails and Python are the primary programming languages used for developing Zendesk applications. Daily application and weekly network vulnerability scans detect vulnerabilities within the operating system, network, or application. File Integrity Monitoring (FIM) software is used to detect changes made to the system files. Customer support tools allow Zendesk to provide support and troubleshoot problems within the customer's Zendesk instance.

Zendesk uses the following ancillary software internally to build, support, maintain and monitor the Zendesk infrastructure.

Application/Tool	Monitored Resource
Mobile Application security scanner	Mobile applications
Web application security scanner	Web applications
Application error tracking and analysis	Web applications
Rails security scanner	Web applications
Network security scanner	Production network
Incident notification tool	Production network
Application performance monitoring	Web applications
Security Information and Event Monitoring (SIEM) system	Production servers
Database activity monitoring	Production databases
"Bug Bounty" program	All
Intrusion Detection System	Production environment
Application performance monitoring	Production servers
Issue and project tracking	Production network
Cloud computing and hosting	Production servers and network
Behavioral and Signature based scanning	Endpoints
Systems-Management software	Servers and endpoints
Backup software	Endpoints
File Integrity Monitoring (FIM)	Production servers
Configuration management	Servers
Software development platform	Web applications
VPN	Production network
Mobile VPN	Production network
Directory service	Servers
Deploy service	Servers
Issue and project tracking	All
Disk encryption (Max)	Endpoints
Disk encryption (Windows)	Endpoints
Two-factor authentication	Mobile and web applications
Network management	Production network

iii. People

People consist of the personnel involved in the governance, operation, and use of a system:

- **Engineering** – Responsible for the development, testing, deployment, and maintenance of new code for Zendesk production applications. Engineering consists of multiple global teams with specific assignments including Quality Assurance, Product Development, and Sustaining.
- **Operations** – Responsible for making hardware, network, and server configuration changes within the Zendesk Production Network. Additionally, responsible for granting logical access to the systems within the Zendesk Production Network, performing quarterly reviews of access to those systems, and revoking logical access rights upon user termination. Operations manages the DDOS protections, and is responsible for overall system availability, including system redundancy, system logging and monitoring, backup and recovery, and capacity planning. Operations works closely with Security to patch discovered system vulnerabilities. Operations consists of multiple teams with specific assignments including System Operations, Cloud Operations, Infra Operations, Core Operations, Shared Services Operations, Data Operations, Network Operations, Datacenter Operations, Database Management, and DevOps.
- **Information Technology (IT)** – Responsible for managing corporate computing devices (laptops/endpoints), business applications, supporting toolsets, and employee and contractor identities. IT grants access to SaaS applications and to systems within the corporate network, and manages this access using Single sign-on (SSO), Active Directory (AD), HR management and Virtual Private Networking (VPN) technologies and terminates access when applicable.
- **Security** – Responsible for security governance, security monitoring, vulnerability scanning, network and application layer penetration testing, security awareness, incident response, security architecture, and compliance oversight. Security consists of multiple teams with specific assignments including Product Security, Network Security, and Security Compliance.
- **People Operations (HR)** – Responsible for onboarding new personnel, defining the role/position of new hires, performing background checks, and facilitating the employee termination process.
- **Workplace Experience (Facilities)** – Responsible for managing physical security and granting physical access to Zendesk corporate offices.
- **Customer Support** – Responsible for managing customer interactions via email, chat, social media and over the phone. The team fields and resolves customer inquiries and issues regarding Zendesk plans, training, and other technical issues related to the software. They are also responsible for communicating information to customers regarding new issues and/or developments, changes in processing schedules, system enhancements, new product features and updates, security incidents, and other relevant information.
- **Legal** – Responsible for setting contractual obligations with third parties and technology partners/suppliers, including (i) negotiation and drafting of legal terms and conditions; (ii) ensuring compliance with internal contractual standards; and (iii) review of information security and privacy issues.
- **Product Management** – Responsible for building features and products for customers as well as actively communicating the changes to external and internal stakeholders such as customers and employees, respectively.

iv. Processes

Processes include the automated and manual procedures involved in the operation of the Platform. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to Operations, Security, Engineering, IT, etc., as detailed later in this System Description. These procedures are drafted in alignment with the overall Information Security Policies and are updated and approved as necessary for changes in the business, but no less than annually.

v. Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by a system. Via the Platform, the customer defines and controls the data they load and store in the Zendesk Production Network. This data is loaded into the environment and accessed remotely from customer systems via the Internet. Zendesk classifies this data as Service Data.

Zendesk also stores user credentials, which are used to authenticate to the Platform. Credential data, consisting of unique usernames and passwords, is stored in hashed format using bcrypt or scrypt, a cross-platform hashing utility. User password information is "salted" (mixed with random data) and hashed using bcrypt or scrypt. The hash and salt identifier, and not the password itself, is what is stored in the database. Password hashing is managed in the application, and to verify that the password is correct, Zendesk compares the result of the one-way hash. This means that user passwords are never written to the database in a human readable format. User passwords and other authentication credentials are also filtered out from logs, prior to writing the logs to disk.

System Boundaries

The scope of this report includes the systems and services operated by Zendesk, including Support, Guide, and Chat that support the development, deployment, control, and configuration of the Zendesk Production Network. These systems and services are externally available to customers as the Platform and are limited to the following:

- Zendesk Production Network located in Sacramento, California (RagingWire); Ashburn, Virginia (RagingWire); Dublin, Ireland (Equinix); and Frankfurt, Germany (Equinix). This includes Pods 3 through 11.
- Zendesk Production Network hosted in various Amazon Web Services (AWS) locations namely, AP Northeast, AP Southeast, US West, US East, EU Central, and EU West. This includes Pods 12 through 15.

Scope Exclusions

The scope of this report does not include the following:

- Explore, Talk, Message, Connect + Outbound, Inbox, and the specific infrastructure hosting it; however, supporting processes and procedures are inherently covered – such as background checks, employee onboarding procedures, security awareness training, endpoint management, etc.
- Professional Services provided by Zendesk – such as onboarding new customers during product implementation and migrating data from old systems.
- Any additional apps or tools, such as Zendesk Apps Marketplace & Integration and Embeddables that are installed on top of the customer's Zendesk instance and opt-in product features.

Subservice Organizations

Due diligence procedures are in place upon engagement and at least annually for third-party service providers that have access to the Zendesk Production Network or to Service Data, according to the *Information Management Standard*. Zendesk utilizes the following subservice organizations:

- **RagingWire** – The servers and networking equipment that support the Zendesk Production Network in Sacramento, California and Ashburn, Virginia are physically located in a third-party datacenter that is owned and operated by RagingWire. Zendesk relies upon RagingWire for physical access controls, protection of equipment from environmental hazards, and power. Zendesk specifies to RagingWire a list of Zendesk personnel who are authorized to physically access the facility and approves access for other personnel who are not RagingWire employees.
- **Equinix** – The servers and networking equipment that support the Zendesk Production Network in Dublin, Ireland and Frankfurt, Germany are physically located in a third-party datacenter that is owned and operated by Equinix. Zendesk relies upon Equinix for physical access controls, protection of equipment from environmental hazards, and power. Zendesk specifies to Equinix a list of Zendesk personnel who are authorized to physically access the facility and approves access for other personnel who are not Equinix employees.
- **Amazon Web Services (AWS)** – The Platform-as-a-Service (PaaS) environments that support Zendesk's Production Network in AP Northeast, AP Southeast, US West, US East, EU Central, and EU West are physically located in datacenters owned and operated by AWS. AWS manages and is responsible for its own internal processes as related to the logical security of the infrastructure used by Zendesk. Zendesk also relies upon AWS for physical access controls, protection of equipment from environmental hazards, and power. In addition, Zendesk offers customers functionality that allows additional files to be attached to tickets. Ticket attachments are stored directly in AWS S3 (Amazon Simple Storage Services), and are, therefore, never stored within Zendesk's RagingWire or Equinix datacenters. AWS S3 is also used to archive database backups and some logs. Ticket attachments, database backups, and logs are transferred to AWS S3 via Transport Layer Security (TLS), and are encrypted at rest via AWS's Server-Side Encryption (AES-256). The Zendesk Operations team manages access to S3 buckets where ticket attachments, database backups, and logs are stored. The AWS EC2 is used to run and support certain elements of its application infrastructure such as proxy mediators. It is also used internally to process Service Data, for example, analyzing customer logs. Access to the services running in this infrastructure is limited through the use of Access Controls Lists (ACLs) on the security groups associated with the EC2 instances.