CONNECTWISE, LLC

Fortify, StratoZen, and Perch Systems

System and Organization Controls (SOC) for Service Organizations Report
for the period July 1, 2021 to December 31, 2021

Report of Independent Service Auditors issued by Aprio LLP

Table of Contents

I. Report of Independent Service Auditor

We have examined ConnectWise, LLC's (the "Company" or "ConnectWise") accompanying assertion titled *ConnectWise, LLC's Assertion* (the "Assertion") indicating that the controls within the Fortify, StratoZen, and Perch Systems (the "System') were effective for the period July 1, 2021 to December 31, 2021 (the "Specified Period"), to provide reasonable assurance that ConnectWise, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The Company uses Amazon Web Services (AWS), a subservice organization, for third-party hosting of servers and equipment in an Platform-as-a-Service environment, including restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. Certain AICPA Applicable Trust Services Criteria specified in the section titled *ConnectWise, LLC's Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's Assertion includes only the controls of the Company and excludes the controls performed by the subservice organization. The Assertion does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Assertion indicates that certain AICPA Applicable Trust Services Criteria specified in the section titled *ConnectWise, LLC's Description of the Boundaries of its System*, under the section *User Entity Controls*, can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's responsibilities

The Company 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 the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *ConnectWise, LLC's Assertion* about the suitability of design and operating effectiveness of controls. When preparing its assertion, the Company is responsible for selecting, and identifying in its assertion, the Applicable Trust Services Criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that the controls within the system were effective throughout the period to provide reasonable assurance that the service organizatin's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the controls were not effective to achieve the Company's service commitments and system requirements based on the Applicable Trust Services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve the Company's service commitments and system requirements based on the Applicable Trust Services Criteria.

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

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

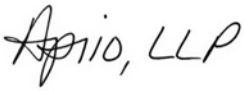
Other matters

We did not perform any procedures regarding the fairness of presentation as it relates to the description criteria of the description in Section III titled *ConnectWise, LLC's Description of the Boundaries of its System*, and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, ConnectWise, LLC's assertion that the controls within the Company's System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria, in all material respects, is fairly stated.

Aprio, LLP



Atlanta, Georgia
April 21, 2022

II. ConnectWise, LLC's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over ConnectWise, LLC's (the "Company" or "ConnectWise") Fortify, StratoZen, and Perch Systems (the "System") for the period of July 1, 2021 to December 31, 2021 (the "Specified Period"), to provide reasonable assurance that the Company's service commitments and system requirements relevant to Security, Availability, Confidentiality, and Privacy were achieved. We have performed an evaluation of the effectiveness of the controls within the System throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy (the "Applicable Trust Services Criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). The Company's objectives for the system in applying the Applicable Trust Services Criteria are embodied in its service commitments and system requirements relevant to the Applicable Trust Services Criteria. The principal service commitments and system requirements related to the Applicable Trust Services Criteria are specified in the section titled *ConnectWise, LLC's Description of the Boundaries of its System*.

The Company uses Amazon Web Services (AWS), a subservice organization, for third-party hosting of servers and equipment in a Platform-as-a-Service environment, including restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. Certain AICPA Applicable Trust Services Criteria specified in the section titled *ConnectWise, LLC's Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by the subservice organization.

Certain AICPA Applicable Trust Services Criteria, specified in Section III, *ConnectWise, LLC's* Description of the Boundaries of its System, under the section User Entity Controls can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by User Entities.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria.

III. ConnectWise, LLC's Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of ConnectWise, LLC's (the "Company" or "ConnectWise") as it relates to its Foritfy, StratoZen, and Perch Systems (the "System") for the period of July 1, 2021 to December 31, 2021 (the "Specified Period"), for the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy (the "Applicable Trust Services Criteria") as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

B. Company Overview and Background

Company Overview

ConnectWise is an IT software company, powering Technology Service Providers (TSP) to achieve their vision of success in their as-a-service business with intelligent software packages, expert services, and vast eco-system of integration. ConnectWise has unmatched flexibility which caters profitable long-term growth to TSPs.

ConnectWise develops and distributes a business management platform. The Company offers a suite of applications that includes an integrated customer relationship management (CRM) solution, help desk and customer service applications, project management, finance and billing systems, and a workflow automation solution. ConnectWise software caters to information technology services, system integration, software development, professional services, and telecommunications sectors. The Company was founded in 1982 and is based in Tampa, Florida.

ConnectWise Office Locations

- Head Office - Tampa:
  4110 George Rd #200,
  Tampa, FL 33634, United States
- Operations – India:
  - Bangalore, India
  - Mumbai, India
  - Pune, India

Overview of the Fortify System

ConnectWise's Fortify products deliver security technology to protect end users, their assets, and data from evolving threats—either on-premise or in the cloud. From endpoint protection and vulnerability assessments to a fully staffed Security Operations Center (SOC) to monitor and stop threats, ConnectWise Fortify keeps partners prepared to protect the client's data from advanced threats.

Fortify Assess reports give users a complete security analysis to share with clients, exposing their environmental risks, and providing peer comparison with other companies. Assess reports provide:

- Dark Web assessment
- Endpoint and User risk analysis
- Peer comparison that evaluates client security readiness against other organizations

Key features include:

- *ConnectWise Fortify SaaS:* ConnectWise Fortify SaaS recognizes abnormal user behavior within Cloud-based apps like Microsoft 365, Azure to stop threats before they compromise customers' users and data.
- *ConnectWise Fortify Assessment:* ConnectWise Fortify Assessment pinpoints security vulnerabilities to mitigate risk and enhance endpoint health.
- *ConnectWise Fortify Protection:* ConnectWise Fortify Protection scans client networks and operating environments for a holistic view of looming security risks and vulnerabilities. ConnectWise Fortify Protection provides the control of the information that helps shape customers' security strategy to keep users and business reputations safe.
- *ConnectWise Fortify Endpoint:* ConnectWise Fortify Endpoint provides protection over endpoints, including laptops, desktops, mobile devices, servers, and even virtual environments, which are all open to cyberattacks. ConnectWise Fortify Endpoint includes a fully staffed, 24/7 SOC to detect, mitigate, and remediate threats.
- *ConnectWise Fortify Network:* ConnectWise Fortify Network provides flexible and scalable security functionality for network device analysis, endpoint log management, and alerts to satisfy compliance requirements. Data privacy laws and other regulatory requirements for compliance with GDPR, CCPA, HIPAA, and more are constantly evolving.

Overview of the StratoZen system

The StratoZen Platform provides solutions to the most common Cybersecurity challenges for Managed Service Provider (MSP) partners and large enterprise clients. StratoZen's Platform components are all modular and fully customized to integrate seamlessly with MSPs existing tools, operations, and teams. For service providers and enterprises, the StratoZen Platform provides modern security information and event management (SIEM), SOC-as-a-Service (Security Operations Center), and Proactive Defense solutions that bridge the gap between traditional in-house cybersecurity and legacy outsourced managed security service provider (MSSP) options. The StratoZen Platform delivers unique value to its Partners by focusing on high accuracy, unmatched flexibility, and custom integration with existing IT operations.

Organizations that outsource IT management can access StratoZen's solutions through its extensive network of service provider partners, while enterprises with in-house teams can leverage the StratoZen Platform to dramatically reduce the cost and complexity of their SIEM and security operations.

StratoZen as a Service provides the following services to partners:

- *SIEM-as-a-Service Features* - StratoZen's SIEM-as-a-Service offers a completely turnkey SIEM solution, configured, and managed by StratoZen experts. It is a comprehensive solution that is fully customizable to meet Partners'/Customers' needs.
- *Enhanced SOC-as-a-Service (ESOC)* - StratoZen's Daily Cybersecurity Review (DCR) provides cost-efficient SOC monitoring and response support that meets regulatory requirements such as PCI, FFIEC, and HIPAA. Enhanced SOC builds on the DCR service to deliver complete, 24/7 incident investigation. ESOC includes manual investigation of all high-severity incidents by highly trained StratoZen SOC analysts, 24/7. Analysts research the incident with additional scrutiny to add additional context and cross-correlate against StratoZen's global network of monitored partner and client environments. It allows clients to provide their own custom response guidance and incident response procedures.

- *(Co)Managed SIEM* - StratoZen offers custom tailored SIEM services to address the needs of clients and helps ensure that their SIEM solutions provides the highest level of value and security. (Co)Managed SIEM, a dedicated instance for the clients that can be deployed anywhere. With (Co)Managed SIEM, StratoZen takes over the management, monitoring, and maintenance of clients' SIEM remotely with administrator access with client's team.
- *Proactive Defense for Networks* - StratoZen's Proactive Defense for Networks service leverages the global threat intelligence network and SWAT Feed to continuously update blacklists on clients' firewalls and other network devices and automatically blocks inbound and outbound traffic to known bad IPs, active attackers, and many other malicious sources.

Overview of the Perch system

Perch is a Co-managed threat detection and response tool. Perch connects managed service providers (MSPs) with threat intelligence sharing communities and sources and automates intel consumption. Perch identifies potential threat activity on MSP's network and views everything through a user-friendly online interface.

The Perch Security Operations Center investigates any alerts on MSP's network, escalates real incidents to the MSP's attention, and helps them eliminate the threat. Perch provides the following services to partners through its product:

- *Multi-tenancy* - Perch is built with multi-tenancy at its core. This feature provides leverage to MSPs to manage alerts for as many lines-of-business or clients they opt for.
- *Threat Hunting* - This feature provides an advantage to MSPs by including Perch's tier-1 alert support, reducing noise, and alerting them of only real threats. In the case of an in-house threat analyst at MSPs, they can participate through Perchybana: investigate Perch alerts; analyze network traffic and logs. They can also drill down into alert details and view the same alert data as Perch's SOC Team.
- *Log-Ingestion* - MSPs/Partners can ingest logs from syslog and Windows Event Logs and retain them to meet compliance requirements. Perch also generates alerts to highlight notable log events based on log data and enhance reporting and visualizations; and it gives Perch's SOC extra insight into MSPs/Partner's endpoints and network traffic data.
- *Threat Management* - Perch's interface lets MSPs/Partners enter and manage their own threat indicators. MSPs/Partners can even build their own threat intelligence repository with Perch.
- *Reports* - This feature provides MSPs/Partners an ability to add custom dashboards and pre-built reports through Perchybana dashboards. Pre-built reports include PCI DSS v3.2.1 Compliance, HIPAA Compliance, Networking, Windows Logs, Monitored Assets, and Office 365.

C. System Overview

1. Infrastructure and Software

ConnectWise Fortify enables users to focus on their customers while leveraging ConnetWise's technology and expertise to respond to cybersecurity attacks before, during, and after an event. The following describes the in-scope components supporting the Fortify System:

System/Application	Description	Infrastructure
Fortify	Security suite with multiple different applications to identify vulnerabilities and to assess and report the security posture of one or more sites for a partner.	Platform leveraging the ConnectWise platform and AWS stack, also leveraging Kafka, Cassandra, and Containerized layers.

StratoZen is a cloud-based Software as a Service (SaaS) application that is hosted solely in AWS. Partners connect to StratoZen's application using their web browser. The following describes the in-scope components supporting the StratoZen's SaaS system:

System/Application	Description	Infrastructure
StratoZen	Cybersecurity Solutions	Data from SIEM Comes to Elastic first, is transformed, and is then output to MySQL in AWS.

Perch is an application that is hosted in AWS. Partners connect to Perch's application using their web browser. The following describes the in-scope components supporting the Perch's system:

System/Application	Description	Infrastructure
Perch	Co-managed threat detection and response platform	Platform hosted on Linux with Elasticsearch Postgres database in AWS, SQS, Logstash, and Kafka for some queue processes running on python3.

The ConnectWise internal network is protected from public internet traffic via stateful inspection firewalls managed by the IT Team. These firewalls are configured to deny all traffic and only allow specific services to a specific destination. Access to administer the firewalls is restricted to personnel in the Cloud Infrastructure group and is commensurate with their job responsibilities. Custom rules are added that govern the allowed inbound traffic to ConnectWise resources. All other inbound traffic is denied. Rules can be modified as needed and new rules are automatically enforced for all existing and future resources.

Encrypted communications are utilized to protect remote internet sessions to the ConnectWise applications and internal network. Encryption is used to help ensure the privacy and integrity of the data being passed over the public network.

Network Security

ConnectWise manages the network security services for their cloud environment. The production infrastructure resides within AWS in multiple availability zones. Partners only have access to their instance. Remote access to the production network is granted via encrypted VPN client. A demilitarized zone (DMZ) is implemented in the cloud-hosted environment to limit inbound traffic from the internet to externally facing production servers while restricting direct access to back-end services. Internal or external web application testing is performed annually to detect new and unknown vulnerabilities. Remediation of all critical/high vulnerabilities is tracked within a ticketing system, and a policy is in place for timely remediation of any critical/high noted vulnerabilities.

Security commitments to user entities are documented and communicated in Terms and Conditions and other partner agreements, as well as in the description of the service offerings provided online. Security commitments are standardized and include, but are not limited to, the following:

- Use of encryption technologies to protect partner data stored and in transit; and
- Role-based access controls to limit user access to sensitive data.

Security groups are used to provide security at the protocol and port level and are configured to explicitly filter traffic coming into and out of the cloud-hosted environment. A DMZ is implemented in the cloud-hosted environment to limit inbound traffic from the internet to externally facing production servers while restricting direct access to back-end services. The credential and user web interfaces are secured using encryption techniques (HTTPS). ConnectWise's management establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements.

Such requirements are communicated through ConnectWise's system policies and procedures, system design documentation, and contracts with partners. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.

Anti-virus is utilized for servers and is centrally managed and configured for real-time protection and to log and report on metrics such as online status and malicious software detection.

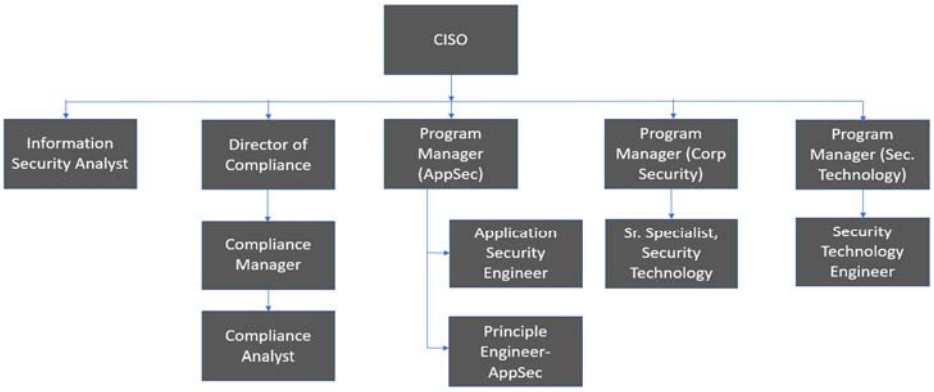
System Availability

ConnectWise maintains production system availability using virtual server technology, network-based storage, and redundant systems and connections. Availability zones are available across 12 datacenters for partners depending on contractual agreements.

2. People

ConnectWise has a staff of approximately 2,700 employees organized as executives, senior operations staff, and Company administrative support staff, such as legal, compliance, accounting, finance, human resources. Key roles in the Company are:

- Chief Executive Officer (CEO) – The CEO of ConnectWise serves as the leader behind the growth and creation of the ConnectWise platform and community. The CEO is focused on expanding ConnectWise through their suite of solutions.
- Executive Vice President (EVP) and Chief Legal Officer (CLO) – The EVP and CLO are responsible for all legal matters relating to business operations.
- Chief Product Officer (CPO) – The CPO oversees product management and development of the ConnectWise platform portfolio. The CPO is responsible for strategic product direction. It includes product vision, product innovation, product design, product development, project management, and product marketing of ConnectWise products.
- Chief Talent Officer (CTO) – The CTO has the responsibility of finding and developing ConnectWise personnel and helping individuals grow to meet their career goals. The CTO is also responsible for identifying and executing best practices in human resources and talent management as well as serving as in-house expert and strategic advisor on all human resources and talent-related issues.
- Chief Information Security Officer (CISO) – The Information Security Officer is responsible for ConnectWise's overall security strategy, including identifying and implementing security practices, policies, and solutions, and recommending best practices for infrastructure and application security. The Information Security Director will also act as a thought leader within the Company, keeping colleagues and the executive leadership team educated on all matters related to security.



Information Security Organization Chart

3. Data

The system of information security controls were designed to protect specific client contact information, server location, and access credentials. ConnectWise products and services operate with a defined hierarchy of access control requirements.

- Partners can only see their own information.
- Clients can only see their own information.

Data is handled in accordance with the Information Classification & Handling Policy which is included in the Information Security Policy. As per the Information Classification & Handling Policy, the following classifications are maintained: Restricted, Confidential Information, Internal, and Public Information. Each type of information has its own exposure level.

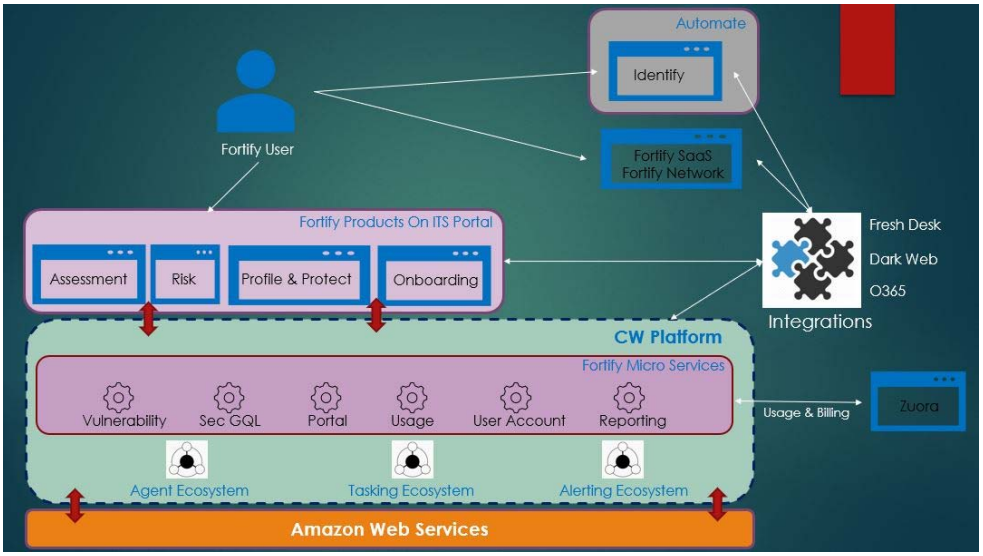
The nature and purpose of processing customer's personal data is to:

1. Provide the service.
2. Provide technical administration and customer support.
3. Respond to inquiries.
4. Send important notices, such as communications about purchases and changes to terms, conditions, and policies.
5. Payments for purchases made.
6. Deliver Process products and services purchased or requested.
7. Manage use of the service.
8. Enforce Connect Wise's Terms of Service

Data collected by the Fortify application is maintained in MySQL located in AWS. Partner data is stored in a dedicated instance of MySQL. Data is stored in encrypted volumes, and transmission to and from the application is encrypted using TLS 1.2. Formal data retention and destruction standards have been developed to provide guidelines for the retention of data for required periods of time.

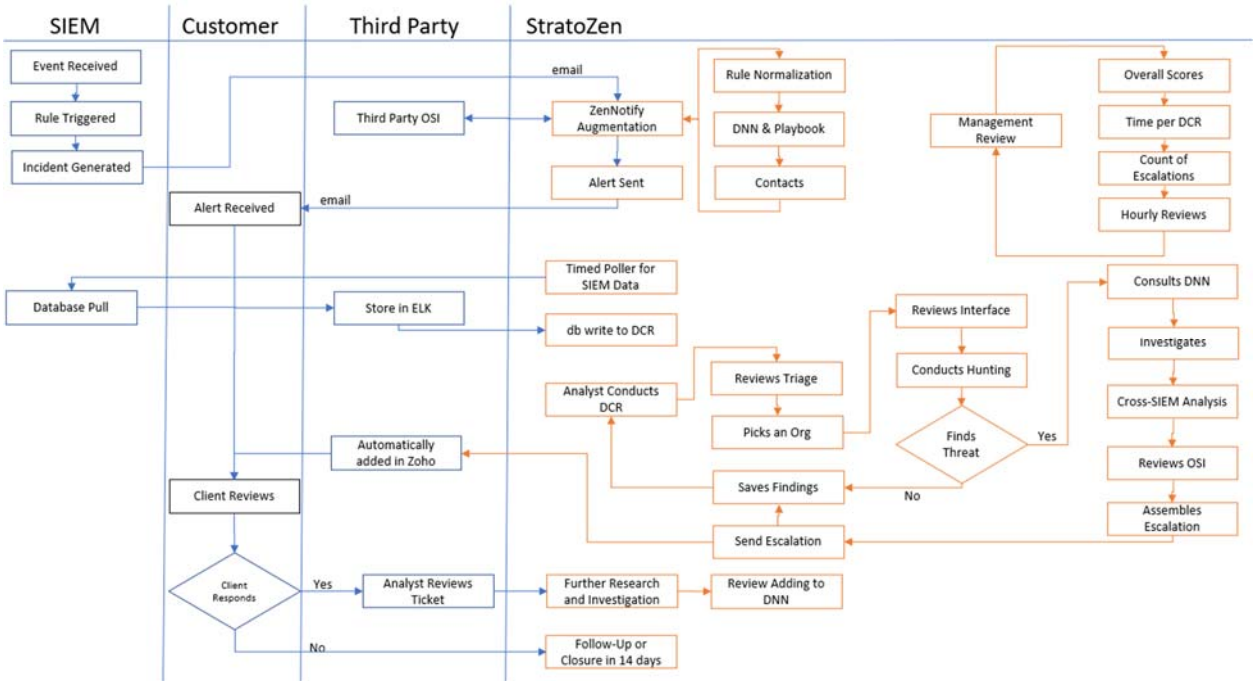
The Company disposes of partner data upon request from the partner to delete the data. An Information Classification and Handling Policy is maintained by management that requires internal controls be implemented to prevent loss, modification, or misuse of confidential information.

Below diagram shows how the information flows in overall process:



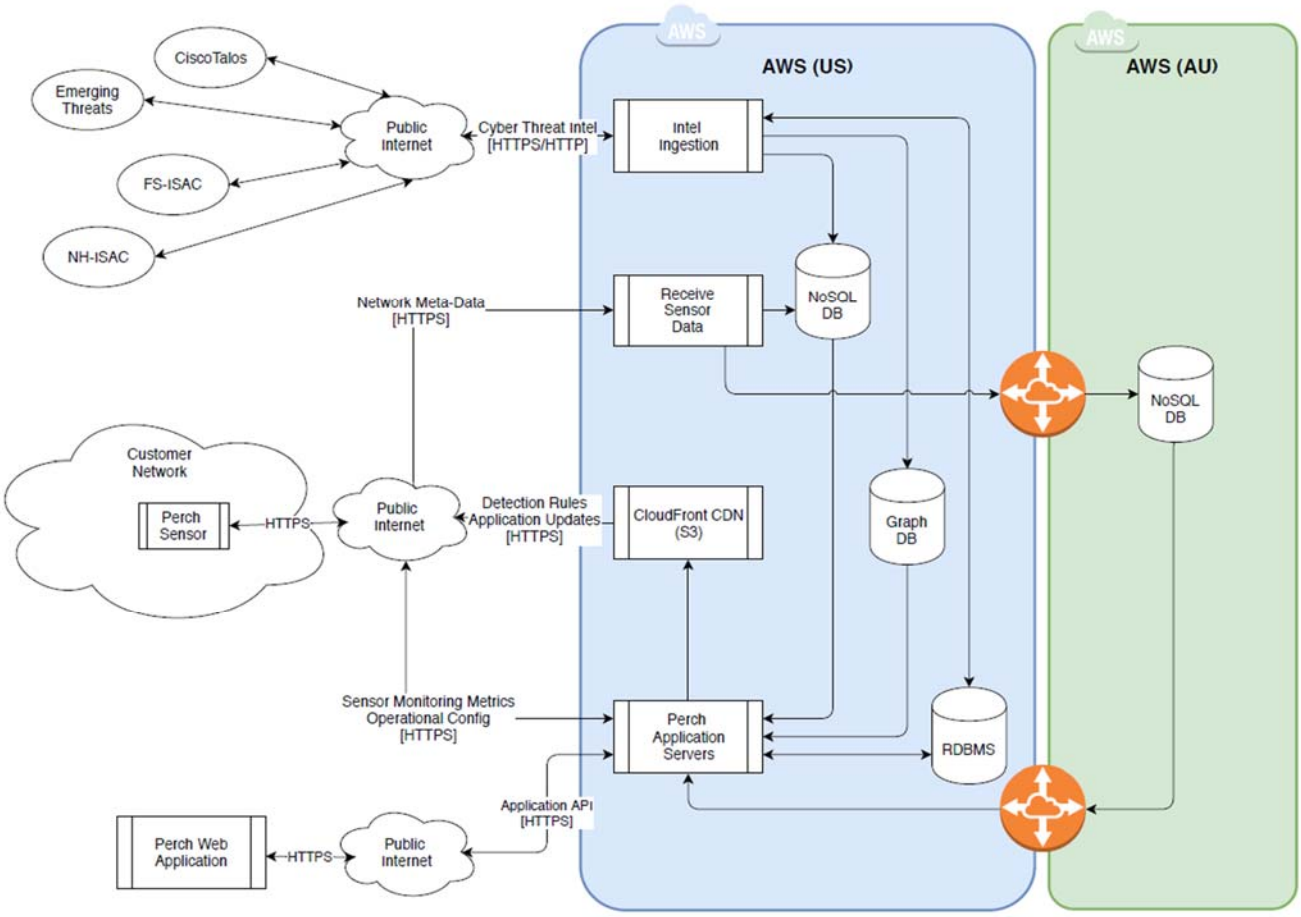
Fortify Data Flow Diagram

Data collected by the StratoZen application is maintained in MySQL located in AWS. Partner data is stored in a dedicated instance of MySQL. Data is stored in encrypted volumes, and transmission to and from the application is encrypted using TLS 1.2.



StratoZen Data Flow Diagram

Data collected by the Perch application is maintained in Postgres located in AWS. Partner data is stored in a dedicated instance of Postgres. Data is stored in encrypted volumes, and transmission to and from the application is encrypted using TLS 1.2.



Perch Data Flow Diagram

4. Policies and Procedures

Policies

ConnectWise management has developed and communicated policies and procedures to all corporate employees and contractors in order to secure systems and facilities and reduce the risk of data loss, compromise, or breach. Changes to these policies and procedures are performed annually and are authorized by senior management. The following policies are in place:

- Acceptable Usage - The purpose of this policy is to set expectations to adhere to the proper use and protection of all information systems.
- Clear Desk - The purpose for this policy is to establish the minimum requirements for maintaining a “clean desk” to prevent any intentional or unintentional information leakage.
- Acceptable Encryption - The purpose of this policy is to implement strong encryption controls to protect the Company’s Information during transit and rest to help ensure confidentiality and integrity.
- Acquisition - The purpose of this policy is to establish InfoSec responsibilities in case of corporate acquisition and define the minimum-security requirements of an InfoSec acquisition assessment.

- Anti-Virus - The purpose of this policy is to safeguard all devices owned by the Company from any malicious code.
- Data Backup - The purpose of this policy is to help ensure the availability of data and business continuity in case of an accidental deletion or corruption of data.
- Data Retention and Records - The purpose of this policy is to help ensure that all the information is retained and disposed as per business requirement & legal and regulatory requirements.
- Database Security - The purpose of this policy is to help ensure confidentiality and integrity of databases where credential information is stored.
- Media Disposal - The purpose of this policy is to establish a standard for the proper disposal of media containing electronic data and to prevent any unauthorized disclosure of the information.
- Information Security Risk Assessment - The purpose of this policy is to perform periodic information security risk assessments ("RAs") to help ensure risks are identified, mitigated, and communicated in a timely manner.
- Information Classification and Handling - The purpose of this policy is to define the classification of the Company's information and provide guidelines for the management of this information to help ensure it is protected from the unauthorized and unintentional access, use and disclosure in accordance with its level of sensitivity.
- Password - The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.
- Patch Management - This policy explains patch management procedure including acquiring, testing, and installing multiple patches of software or existing application.
- Physical Security for Information Resources - This policy is to control the physical access to ConnectWise's Information Resources. This policy sets forth the rules for establishing, controlling, and monitoring the physical access to Information Resources.
- Remote Access - The purpose of this policy is to help ensure adequate security measures while accessing the information from remote locations or from mobile device.
- Network Security - The purpose of this policy is to help ensure that access to ConnectWise networks is managed and controlled to protect information and Information System.
- Secure Application Development - The purpose of this policy is to help ensure ConnectWise's business applications are written with secure coding standard to protect confidentiality and integrity of Information.
- Server Security - The purpose of this policy is to establish standards for the base configuration of the internal servers that are owned and/or operated by ConnectWise.
- Change Management - The purpose of this policy is the basis of Senior Management support for the implementation of change processes to manage ConnectWise's information assets, including the network infrastructure and applications by assuring that changes to the IT environment are made in a controlled manner.
- Access Control - The purpose of this policy is to help ensure confidentiality and integrity of information and to timely grant and revoke of information access as per business requirements.
- Incident Response - The purpose of this policy is to define steps to recover quickly from any kind of security incidents to help ensure minimal business impact and help ensure business continuity.
- Information Security Continuity - The purpose of this policy is to help ensure continuity and security of operation in case of disaster.
- Vendor Security Risk Management - The purpose of this policy is to help ensure vendor has adequate risk management program in place to protect ConnectWise's customer's information.

- Information Security Compliance - The purpose of this policy is to maintain a documented Information security Compliance policy. This document shall guide about compliance requirements and steps to get compliant with relevant laws, regulations.
- Asset Management - The purpose of this policy is to maintain a documented asset management guideline and to achieve, maintain appropriate protection of all ConnectWise assets.
- Vulnerability Management - The purpose of this policy is to maintain a documented Vulnerability Management program, which will guide authorized ConnectWise personnel to perform information security vulnerability assessment in order to determine vulnerable areas. The critical and high vulnerabilities identified have an SLA in place for timely remediation the vulnerabilities. The InfoSec team performs penetration testing bi-annually to identify vulnerabilities present in the organization.
- Audit Log & Monitoring - Audit log policy outlines the relevant auditing and logging procedures for computer systems, networks, and devices stores or transport critical data.
- Privilege Identity Access Management - The purpose of this policy is to help ensure protection of privilege accounts to prevent from any misuse and unauthorized access.
- Security Awareness - The purpose of this policy is to create Information Security Awareness for all Company's employees as awareness is major part of Information Security. This policy defines the steps to spread provide security awareness in the organization.
- Email Security - The purpose of this policy is to minimize any risk that may arise from the use of email, compromised email account, and reduce threat related to unauthorized access of email.
- Minimum System level Security - The purpose of this policy is to maintain minimum security measures on all the information systems owned by ConnectWise before they are deployed onto the Company network.
- Cloud Security - The purpose of this policy is to maintain confidentiality, Integrity, and availability of the information when stored, transmitted or processed by a third-party cloud provider.
- Talent Management - The purpose of this policy is to help ensure that the employees and contractors understand their responsibility and are suitable for the roles for which they are considered.
- New Technology adoption - The purpose of this policy is to maintain guidelines while adopting new technology so to make adoption process smooth and less vulnerable for sophisticated attacks.

Procedures

Standard operating procedures (SOPs) are documented for automated and manual procedures involved in the operation of the SaaS platform. Along with SOPs, management has identified and put into effect actions needed to affect those standards. Control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently.

Documented information security policies and procedures are in place to guide IT and operations personnel in information security administration processes, including, but not limited to acceptable usage, access provisioning, password management, change management, incident response, network security, database security, Asset Management, Information Security Risk Assessment, Vendor Security Risk Management, and data retention and classification. The policies are made available via the intranet and personnel are required to acknowledge their acceptance. A security awareness program is administered annually, and completion is compulsory.

The Company has implemented a formal written Information Security Policy which addresses the security, availability, confidentiality, and privacy of the system and covers the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet.

D. Principal Service Commitments and System Requirements

ConnectWise takes security very seriously looking at security as a dynamic threat and continues to work to optimize security for its partners and community. ConnectWise regularly conducts penetration tests that are performed by both internal and external ethical hackers and runs vulnerability assessments on their systems and products on a consistent basis. ConnectWise products are subject to multiple layers of security from design through testing and into operations. Products designs are aligned with security leading-practices and undergo security testing prior to release and regularly in production. In addition, ConnectWise's developers complete security training on an annual basis at a minimum.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security, Availability, Confidentiality, and Privacy commitments are standardized and include, but are not limited to, the following:

- The use of security and confidentiality principles that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role;
- The use of encryption technologies to protect customer data in transit over untrusted networks;
- The use of reasonable precautions to protect the security and confidentiality of the information that is collected;
- Making commercially reasonable efforts to automatically filter certain personal information collected from the System such as password and account numbers; and
- Making commercially reasonable efforts to destroy or encrypt any information that is not filtered automatically.

ConnectWise establishes operational requirements that support the achievement of Security, Availability, Confidentiality, and Privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ConnectWise's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data is protected.

E. Non-Applicable Trust Services Criteria

Common Criteria/Security and Privacy Trust Services Criteria		
Non-Applicable Trust Services Criteria		**ConnectWise's Rationale**
CC 6.4	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.	This criterion is not applicable as ConnectWise leverages only third-party Platform as-a-Service (PaaS) provided by Amazon Web Services (AWS) for providing customer-related services; therefore, physical access is not applicable as the Company does not maintain any hard copy data or store any customer information in a physical location that the Company controls.
P 1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	This criterion is not applicable to ConnectWise because the Company does not directly interact with the Client's and Partner's data subjects who are utilizing the solution. Clients and Partners are the data owner and data controller of all information stored within the solution.

Common Criteria/Security and Privacy Trust Services Criteria		
Non-Applicable Trust Services Criteria		**ConnectWise's Rationale**
P 2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	This criterion is not applicable to ConnectWise because the Company does not directly interact with the Client's and Partner's data subjects who are utilizing the solution. Clients and Partners are the data owner and data controller of all information stored within the solution.
P 3.1	Personal information is collected consistent with the entity's objectives related to privacy.	This criterion is not applicable to ConnectWise because the Company does not directly interact with the Client's and Partner's data subjects who are utilizing the solution. Clients and Partners are the data owner and data controller of all information stored within the solution.
P 3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.	This criterion is not applicable to ConnectWise because the Company does not directly interact with the Client's and Partner's data subjects who are utilizing the solution. Clients and Partners are the data owner and data controller of all information stored within the solution.
P 5.1	The entity grants identified, and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	This criterion is not applicable to ConnectWise because the Company does not directly interact with the Client's and Partner's data subjects who are utilizing the solution. Clients and Partners are the data owner and data controller of all information stored within the solution.
P 5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	This criterion is not applicable to ConnectWise because the Company does not directly interact with the Client's and Partner's data subjects who are utilizing the solution. Clients and Partners are the data owner and data controller of all information stored within the solution.

Common Criteria/Security and Privacy Trust Services Criteria		
Non-Applicable Trust Services Criteria		**ConnectWise's Rationale**
P 6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	This criterion is not applicable to ConnectWise because the Company does not directly interact with the Client's and Partner's data subjects who are utilizing the solution. Clients and Partners are the data owner and data controller of all information stored within the solution. ConnectWise does not perform any authorized disclosures of Client or Partner information.
P 6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	This criterion is not applicable to ConnectWise because the Company does not directly interact with the Client's and Partner's data subjects who are utilizing the solution. Clients and Partners are the data owner and data controller of all information stored within the solution.
P 6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	This criterion is not applicable to ConnectWise because the Company does not directly interact with the Client's and Partner's data subjects who are utilizing the solution. Clients and Partners are the data owner and data controller of all information stored within the solution.
P 7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	This criterion is not applicable to ConnectWise because the Company does not directly interact with the Client's and Partner's data subjects who are utilizing the solution. Clients and Partners are the data owner and data controller of all information stored within the solution.

F. Subservice Organizations

The Company utilizes a subservice organization to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party subservice organization described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at this subservice organization.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organization, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Amazon Web Services (AWS)	The Company uses AWS for third-party hosting of servers and equipment in an Platform-as-a-Service environment, including restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls around the underlying infrastructure and Data Centers supporting the Security Services System's production environments; including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure such as physical servers and physical access to backups and facilities; • Controls around the S3 data storage, including controls around physical access to the backup servers and facilities, high availability replication, physical access to storage systems, operating system installation and patches, database software installation and patches, and system configuration; • Controls around the change management processes for the AWS Platform-as-a-Service environment. In addition, the Company has identified the following control activity to help monitor the subservice organization: • Vendor risk assessments are performed for all critical vendors annually. As a part of this assessment, the InfoSec team verifies critical vendor's compliance with frameworks such as GDPR, SOC 2 Type II, and ISO 27001 to assess their security benchmark in terms of security commitment.	CC 5.2* CC 6.4 CC 6.8* CC 7.5* CC 8.1* CC 9.1* A1.1* A1.2* A1.3* C1.1*

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at this subservice organization that support the service organization's service commitments and system requirements are in place and are operating effectively.*

G. User Entity Controls

ConnectWise, LLC's controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary user entity controls identified within the table below, where applicable. As applicable, suggested control considerations and/or complementary user entity controls and their associated criteria have been included within the table below.

Management has highlighted criterion in which complementary user entity controls were assumed in the design of the Company's system with an asterisk. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes each user organization should consider in developing their internal controls or planning their audits that are relevant to the Company's controls detailed in this report, however, such control considerations are not required to achieve design or operating effectiveness for the Company's service commitments and system requirements based on the applicable trust services criteria. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user entity. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities which provide a basis for the assertions underlying the control environments for the Company's user entities.

User Entity Control	Associated Criteria
User entities are responsible for informing ConnectWise of any regulatory issues that may affect the services provided by ConnectWise to the user entity.	CC 2.3
User entities are responsible for understanding and complying with their contractual obligations to ConnectWise.	CC 2.3
User entities are responsible for notifying ConnectWise personnel, in a timely manner, when changes are made to technical, billing, or administrative contact information.	CC 6.1
User entities are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize ConnectWise's services.	CC 7.5 A 1.3
User entities are responsible for ensuring that user IDs and passwords are assigned only to authorized individuals and that the roles assigned to the user accounts are appropriate through the use of administrative accounts provided by ConnectWise.	CC 6.1* CC 6.2* CC 6.3*
Fortify: User entities are responsible for ensuring the confidentiality of any user IDs and passwords assigned to them for use with ConnectWise's systems.	CC 6.1* CC 6.2* CC 6.3* CC 1.1*
StratoZen and Perch: User entities are responsible for ensuring the confidentiality of any user IDs and passwords assigned to them for use with ConnectWise's systems.	CC 1.1
User entities are responsible for the administration of user access for the ConnectWise applications.	CC 6.1* CC 6.2* CC 6.3*
User entities are responsible for configuring password parameters for the Fortify, StratoZen, and Perch Systems.	CC 6.1
User entities are responsible for immediately notifying ConnectWise personnel of any actual or suspected information security breaches, including compromised user accounts.	CC 7.2 CC 7.3 CC 7.4 CC 7.5
User entities are responsible for ensuring that appropriate individuals have the requisite training on ConnectWise software.	CC 2.2
User entities are responsible for responding to alert notifications.	CC 7.1

User Entity Control	Associated Criteria
User entities are responsible for determining whether ConnectWise's security infrastructure is appropriate for its needs and for notifying ConnectWise personnel of any requested modifications.	CC 8.1
User entities are responsible for implementing a security infrastructure and practices to prevent unauthorized access to their internal network and to limit threats from connections to external networks.	CC 6.1 CC 6.2 CC 6.3 CC 6.6
User entities are responsible for applying changes to the production environment or for granting access to ConnectWise employees to apply changes to production.	CC 7.1 CC 8.1
User entities are responsible for ensuring that the software is configured and functioning per their requirements and notifying ConnectWise personnel in a timely manner of any issues.	CC 7.1 CC 7.2

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary user entity controls that support the service organization's service commitments and system requirements are in place and are operating effectively.*


Aprio