CONNECTWISE

CONNECTWISE, LLC

ScreenConnect and Automate Systems

SOC 3

System and Organization Controls (SOC) for Service Organizations Report
for the period of January 1, 2023 to December 31, 2023

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations

Aprio®
Passionate for what's next®

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's Assertion* (the "Assertion") indicating that the controls within the ScreenConnect and Automate Systems (the "System") were effective for the period of January 1, 2023 to December 31, 2023 (the "Specified Period"), to provide reasonable assurance that ConnectWise'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 200, *2018 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) for the Specified Period.

The Company uses the subservice organizations noted in the Subservice Organizations table in Section III of this report. Certain AICPA Applicable Trust Services Criteria specified in the section titled *ConnectWise'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 organizations. The Assertion 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.

The Assertion indicates that certain AICPA Applicable Trust Services Criteria specified in the section titled *ConnectWise'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'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 organization'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.

We are required to be independent and to meet our ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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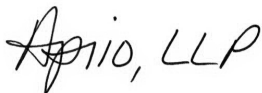
Other matters
We did not perform any procedures regarding the fairness of presentation as it relates to the description criteria of the description in Section III titled *ConnectWise's Description of the Boundaries of its System*, and, accordingly, do not express an opinion thereon.

Opinion
In our opinion, ConnectWise'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

Aprio, LLP

Atlanta, Georgia
March 5, 2024

II.   ConnectWise's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over ConnectWise, LLC's (the "Company" or "ConnectWise") ScreenConnect and Automate Systems (the "System") for the period of January 1, 2023 to December 31, 2023 (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 200, *2018 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's Description of the Boundaries of its System*.

The Company uses the subservice organizations noted in the Subservice Organizations table in Section III of this report. Certain AICPA Applicable Trust Services Criteria specified in the section titled *ConnectWise'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 organizations.

Certain AICPA Applicable Trust Services Criteria, specified in Section III, *ConnectWise'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's Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of ConnectWise, LLC (the "Company" or "ConnectWise") as it relates to its ScreenConnect and Automate Systems (the "System") for the period of January 1, 2023 to December 31, 2023 (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 200, *2018 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:
  400 N Tampa St #2600,
  FL 33602, United States
- Operations – India:
  - Bangalore, India
  - Mumbai, India
  - Pune, India

Overview of the ScreenConnect System

ScreenConnect is a remote desktop support software application that is hosted by ConnectWise primarily in its standalone bare metal Equinix servers. The application is set up in a multi-instance Software-as-a-Service (SaaS) architecture that allows for a high degree of customization and security management by the primary user including the ability to limit access to the instance by network address. ScreenConnect has an open architecture structure that can be utilized by users to implement custom plugins, scripting, or various integrations.

A typical use model would start with a host initiating a session through the central web application. A participant would then join a session by clicking on an email link or via the guest page of the application. An unattended client can be created and deployed to a targeted machine without the need for human intervention. Most commonly expected features for a product in this arena are present. Examples include reboot and reconnect, drag and drop file transfer, screen recording, safe mode support, multiple monitors, command line access, wake-on-LAN, Voice over Internet Protocol (VoIP), chat, and a custom toolbox for quick deployment of support tools. In addition to features that facilitate communication, ScreenConnect also offers complete control over branding and customization of the product design, logo, color scheme, icons, text strings, and localization.

ScreenConnect's SaaS provides the following services to partners:

- *Ad Hoc support* – The agent provides a code or link to connect. This process is a non-persistent connection. Once the session is over, the link or access is no longer available. There is no agent installed. There is an executable, but it is not an installation. The executable runs at the user level to establish the user connection.

- *Screen sharing* – This method of connecting is simply, sharing the screen of the user needing support. A link is provided to the user with a code and a package file is downloaded or executed. This process is not a peer-to-peer connection. This connection goes through a server over a secure connection.

- *Agent based support session* – This method of connection is agent based. An administrator typically sets this up. This approach is generally used by internal IT. With the agent installed, the IT support group has the ability to connect to the user's machine and control it for support.

Overview of the Automate System

Automate SaaS is a remote management and monitoring tool that allows partners to manage asset inventories, patching, scripting, software deployments, and monitoring at multiple locations in real-time. Once installed, the central web application can be made visible inside and outside of the local area network (LAN). ConnectWise Automate has an open architecture structure that can be utilized by users to implement custom plugins, scripting, or various integrations.

Automate provides visibility by allowing partners to dynamically audit hardware and software across major Windows, Linux, and Apple platforms. In addition, Automate allows partners to deploy patches, scripts, and software updates automatically, keeping systems current as changes occur. The monitoring function of Automate provides partners with the ability to proactively monitor and support users and devices with an integrated search tool. Automation of recurring tasks with Automate allows IT personnel to spend time on higher priorities.

Automate SaaS provides the following services to partners:

- *Network Discovery* – Allows partners to scan their networks to audit both hardware and software assets.

- *Automation* – Allows partners to automate recurring tasks, such as patch deployment, scripting, and software updates.

- *Monitoring* – Allows partners to proactively support users by pre-emptively addressing issues before they become outages.

C. System Overview

1. Infrastructure and Software

ScreenConnect is a cloud-based multi-instance SaaS application that is hosted in AWS, Azure, and Equinix. ScreenConnect is also hosted in OVHcloud (free instances, limited number of non-free instances). Partner solutions are housed in their own instances, making this a multi-instance solution as opposed to multi-tenant which is common in cloud architecture. The following table describes the in-scope components supporting the ScreenConnect SaaS system:

System/Application	Description	Infrastructure
ScreenConnect	Remote-control software	Host servers use Windows Server 2019 and Server 2022. Each server can have up to 800 instances. Each instance has an SQLite database, a proprietary webserver as relay service session manager.

Automate is a cloud-based multi-instance SaaS application that is hosted in AWS. Each partner's solution is housed in their own instance, making this a multi-instance solution as opposed to multi-tenant which is common in cloud architecture. The following table describes the in-scope components supporting the Automate system:

System/Application	Description	Infrastructure
Automate	Remote Management and Monitoring Application	Windows Server 2016, 2019, 2022 Internet Information Services (IIS), and MySQL database.

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 data centers in multiple availability zones. Partners only have access to their instance. Remote access to the production network is granted via an 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 interface 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 logs and reports on metrics such as online status and malicious software detection.

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, availability, confidentiality, and privacy 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;

- Making commercially reasonable efforts to destroy or encrypt any information that is not filtered automatically; and

- Make commercially reasonable efforts to collect, use, retain, disclose, and dispose of personal information to achieve the Company's service commitments and system requirements.

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

Security, Availability, Confidentiality, and Privacy Trust Services Categories	
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) products 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.

Security, Availability, Confidentiality, and Privacy Trust Services Categories	
Non-Applicable Trust Services Criteria	**ConnectWise's Rationale**
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.
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.

Security, Availability, Confidentiality, and Privacy Trust Services Categories		
Non-Applicable Trust Services Criteria		**ConnectWise's Rationale**
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.
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 Partner information.

Security, Availability, Confidentiality, and Privacy Trust Services Categories	
Non-Applicable Trust Services Criteria	**ConnectWise's Rationale**
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 subservice organizations 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 organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

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 organizations, 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	The Company uses Amazon AWS Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the 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 Company also uses the AWS Simple Storage Service (S3) as a Platform-as-a-Service, more specifically a Database-as-a-Service. Amazon S3 provides object	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	storage through a web service interface. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure security such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the physical servers supporting the Infrastructure-as-a-Service Platform; • Controls over the configuration settings within the EC2 instance to ensure that data is encrypted and stored as per the configuration settings selected with AWS; • Controls over incident monitoring, response, and follow up; • Controls over managing the Platform-as-a-Service components for AWS S3 such as physical servers and operating systems including applying critical patching for this infrastructure; • Controls over AWS S3 including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; • Controls over AWS S3 redundancy, including controls over data replication; and • Controls over the change management processes for the AWS Infrastructure-as-a-Service Platform and the Platform-as-a-Service Platform (AWS S3) components as applicable. 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 vendors' compliance with frameworks such as the General Data Protection Regulation (GDPR), SOC 2 Type II, and ISO 27001 to assess their security benchmarks in terms of security commitment.	CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3* C 1.1* C 1.2* P 4.2* P 4.3* P 6.6
Equinix, Inc.	The Company uses Equinix, Inc. for its third-party colocation data center services for the hosting of servers and equipment, including the 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 data center hosts Worker Servers running Free License Control instances. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls around the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; and	CC 6.4 A 1.2* A 1.3* P 4.2* P 4.3* P 6.6

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over physical access to the Data Centers hosting the in-scope production 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 vendors' compliance with frameworks such as the General Data Protection Regulation (GDPR), SOC 2 Type II, and ISO 27001 to assess their security benchmarks in terms of security commitment.	
Microsoft Azure	The Company uses Microsoft Azure's Platform-as-a-Service for its third-party hosting of servers and equipment, including the 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 Company also uses the Azure SQL Database and/or SQL Managed Instance service, which is a Platform-as-a-Service or more specifically a Database-as-a-Service. The Company uses Microsoft Azure for creating Azure Workflow logic, SQL databases for storing account information, and VM clusters for upgrading instances in Azure. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing the security of infrastructure and software including Azure SQL Database and/or SQL Managed Instance service such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the software and infrastructure supporting the platform including Azure SQL Database and/or SQL Managed Instance service; • Controls over incident monitoring, response, and follow up; • Controls over the prevention, detection, and follow up upon the introduction of malicious software; • Controls over Azure Storage redundancy, including controls over data replication; • Controls over the encryption of transmitted and stored data within the platform including Azure SQL Database and/or SQL Managed Instance service; and • Controls over managing patching for the software and infrastructure supporting the platform, including Azure SQL Database and/or SQL Managed Instance service. 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	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3* C 1.1* C 1.2* P 4.2* P 4.3* P 6.6

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	critical vendors' compliance with frameworks such as the General Data Protection Regulation (GDPR), SOC 2 Type II, and ISO 27001 to assess their security benchmarks in terms of security commitment.	
OVHcloud	The Company uses OVHcloud for its third-party colocation data center services for the hosting of servers and equipment, including the 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 data center hosts Worker Servers running Free License Control instances. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls around the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; and • Controls over physical access to the Data Centers hosting the in-scope production 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 vendors' compliance with frameworks such as the General Data Protection Regulation (GDPR), SOC 2 Type II, and ISO 27001 to assess their security benchmarks in terms of security commitment.	CC 6.4 A 1.2* A 1.3* P 4.2* P 4.3* P 6.6

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'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 ensuring that appropriate individuals have the requisite training on ConnectWise software.	CC 2.3
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 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 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*
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* C 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 ScreenConnect and Automate systems.	CC 6.1*
User entities are responsible for responding to alert notifications.	CC 7.1
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
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 Entity Control	Associated Criteria
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 determining whether ConnectWise's security infrastructure is appropriate for its needs and for notifying ConnectWise personnel of any requested modifications.	CC 8.1

* 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.