CONNECTWISE, LLC

ConnectWise ITBoost System

SOC 3® System and System and Organization Controls (SOC) for Service Organizations

Report throughout the period of May 1, 2020 through October 31, 2020
**Table of Contents**

I. **Report of Independent Service Auditor** ................................................................. 1

II. **ConnectWise LLC’s Assertion** .............................................................................. 3

III. **Management of ConnectWise’ Description of its ITBoost System** ...................... 4

   A. **Scope and Purpose of the Report** ................................................................. 4
   B. **Company Overview and Background** .......................................................... 4
   C. **Principal Service Commitments and System Requirements** ......................... 5
   D. **Components of the System Used to Provide the Services** ........................... 5
   E. **Policies and Procedures** .............................................................................. 5
   F. **User Entity Controls** ................................................................................... 8
   G. **Subservice Organizations** ......................................................................... 8
I. Report of Independent Service Auditor

To: Management of ConnectWise, LLC

Scope
We have examined ConnectWise LLC’s (the “Company”) accompanying assertion titled ConnectWise LLC’s Assertion (the “Assertion”) that the controls within ConnectWise LLC’s ITBoost System were effective throughout the period May 1, 2020 to October 31, 2020 (the “Specified Period”), to provide reasonable assurance that ConnectWise’ service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security, Confidentiality, and Availability (“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).

ConnectWise uses Amazon Web Services as a subservice provider for hosting of the production infrastructure system and associated physical security and infrastructure support. The Assertion indicates that certain AICPA Applicable Trust Services Criteria specified in the section titled Management of ConnectWise’ Description of its ITBoost 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. Our examination did not extend to the controls of 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 Management of ConnectWise’ Description of its ITBoost 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
ConnectWise 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. ConnectWise 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 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.
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.

Opinion

In our opinion, ConnectWise’ assertion that the controls within the ITBoost 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.

Atlanta, Georgia
February 24, 2021
II. ConnectWise LLC’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over ConnectWise LLC’s (the “Company”) ITBoost System (the “System”) throughout the period May 1, 2020 to October 31, 2020 (the “Specified Period”), to provide reasonable assurance that the Company’s service commitments and system requirements relevant to Security, Confidentiality, and Availability were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

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 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 Section III titled Management of ConnectWise’ Description of its ITBoost System.

ConnectWise uses Amazon Web Services as a subservice provider for hosting of the production infrastructure system and associated physical security and infrastructure support. Certain AICPA Applicable Trust Services Criteria specified in the section titled Management of ConnectWise’ Description of its ITBoost 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, Management of ConnectWise’ Description of its ITBoost 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. Management of ConnectWise’ Description of its ITBoost System

A. Scope and Purpose of the Report

This report describes the control structure of ConnectWise (the “Company”) as it relates to its ConnectWise ITBoost System (the “System”) for the period of May 1, 2020 to October 31, 2020 (the “Specified Period”) for the Security, Confidentiality, and Availability Trust Services Categories (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

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.

Overview of the ITBoost system

ITBoost is an IT documentation system managed by ConnectWise. It has a versatile dashboard that hosts the most advanced documentation solution in the industry and displays the numbers you need to see from your external platforms.

Founded in 2018 and acquired by ConnectWise in 2019, ITBoost is a Software as a Service (SaaS) system that includes controls designed to meet the applicable Trust Services Criteria. Management is responsible for the identification of risks associated with the system of controls, and for the design and operation of controls intended to provide reasonable assurance that the applicable Trust Services Criteria would be met.

ITBoost System Overview

- **Documentation**: Whether you prefer to work off customizable templates or build your knowledge base from the ground up, everything you need to customize your documentation experience with ITBoost is at your fingertips.
- **Comprehensive Dashboard**: ITBoost links your critical information together across companies, contacts, and assets, enabling organizations to deliver seamless customer experiences from a single pane-of-glass view.
- **Customized Templates**: ITBoost eases the documentation process with the use of customized templates.
- **VOIP Integrations**: With Ring Central and Jive VOIP integrations, on-screen prompts deliver all the information your techs need to provide a seamless and consistent customer support experience.
C. Principal Service Commitments and System Requirements

ITBoost designs its processes and procedures to meet the objectives for its service. ConnectWise is in compliance with the necessary and applicable laws and regulations and only collects data that is required to provide services to customers.

ITBoost has established policies and procedures and defined adequate security controls required to safeguard information collected. ITBoost leverages user access management principles that are designed to permit system users to access only the information they need based on their role in the system while restricting them from accessing information that is not needed for their role.

Data Security

The system of information security controls was 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 Data Handling Policy present in the IS Policy. As per the Data Classification Policy, the following classifications are maintained: Sensitive Information, Confidential Information, Internal, and Public Information. Each type of information has their own exposure level.

D. Components of the System Used to Provide the Services

ITBoost is a cloud-based SaaS application that is hosted solely in AWS. Partners connect to ITBoost using a web browser.

E. Policies and Procedures

ConnectWise management has developed and communicated policies and procedures to all corporate employees and contractors 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.

- Acceptable Use: The purpose of this policy is to set expectations that users are required to adhere to regarding the proper use and protection of all information systems.
- Third Party Vendor – Data Protection: The purpose of this policy is to ensure vendors maintain adequate risk management programs to protect customer information.
- Acceptable Encryption: The purpose of this policy is to require strong encryption controls to protect the company’s information in transit and at rest to ensure confidentiality and integrity.
- Acquisition Assessment: The purpose of this policy is to establish information security responsibilities in the event of a corporate acquisition and define the minimum-security requirements of an information security acquisition assessment.
- Anti-Virus: The purpose of this policy is to safeguard all devices owned by the Company from malicious code.
- Data Backup: The purpose of this policy is to ensure the availability of data and ensure business continuity in the event of an accidental deletion or corruption of data.
- Data Retention and Records: The purpose of this policy is to ensure that all information is retained and disposed of in accordance with business, legal, and regulatory requirements.
- Security Credentials Management: The purpose of this policy is to ensure the confidentiality and integrity of databases where credential information is stored.
- Destruction of Electronic Media: The purpose of this policy is to establish a standard for the proper disposal of media containing electronic data and prevent unauthorized disclosure of the information.
- Information Security Risk Assessment: The purpose of this policy is to perform periodic information security risk assessments to ensure risks are identified, mitigated, and communicated in a timely manner.
• **Information Sensitivity:** The purpose of this policy is to define the classification of the Company’s information and provide guidelines for the management of information to ensure it is protected from 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 the creation of strong passwords, the protection of those passwords, and the frequency of password changes.

• **Patch Management:** The purpose of this policy is to define patch management practices including acquiring, testing, and installing patches of software for existing applications.

• **Physical Security for Information Resources:** The purpose of this policy is to control physical access to information resources. This policy sets forth the rules for establishing, controlling, and monitoring physical access to information resources.

• **Remote Access:** The purpose of this policy is to ensure adequate security measures while accessing information from remote locations or mobile devices.

• **Network Security:** The purpose of this policy is to ensure that access to ConnectWise’s networks are managed and controlled to protect information and information systems.

• **Secure Application Development:** The purpose of this policy is to ensure business applications are written with secure coding standards to protect the confidentiality and integrity of information.

• **Server Security:** The purpose of this policy is to establish standards for the base configuration of internal servers that are owned and/or operated by ConnectWise.

• **Change Management:** The purpose of this policy is to manage changes made to information assets, including network infrastructure and applications, by ensuring that changes to the IT environment are made in a controlled manner.

• **Access Control:** The purpose of this policy is to ensure the confidentiality and integrity of information and to grant and revoke information access in a timely manner in accordance with business requirements.

• **Incident Response:** The purpose of this policy is to define steps to quickly recover from any type of security incident and minimize the business impact, while maintaining business continuity.

• **Information Security Continuity:** The purpose of this policy is to ensure the continuity and security of operations in the event of a disaster.

• **Information Security Compliance Policy:** The purpose of this policy is to ensure compliance with relevant laws and regulations.

• **Asset Management:** The purpose of this policy is to maintain documented asset management guidance and to achieve and maintain appropriate protection of company assets.

• **Vulnerability Management:** The purpose of this policy is to maintain a documented vulnerability management program, which guides authorized personnel in the performance of information security vulnerability assessments to identify vulnerable areas. Critical vulnerabilities are required to be remediated within 30 days of identification and high vulnerabilities are required to be remediated within 60 days of identification. Additionally, penetration tests are required to be performed bi-annually to identify vulnerabilities present in the organization.

• **Audit Log:** Audit log policy outlines the relevant auditing and logging procedures for computer systems, networks and devices stores or transport critical data.

**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 use, access provisioning, password management, change management, incident response, network security, database security, asset management, information security risk assessments, 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.

1. **Incident Response**
   Documented escalation procedures for reporting incidents are provided to internal and external users to guide users in identifying and reporting failures, incidents, concerns, and other complaints. IT personnel utilize an automated ticketing system to document system incidents, response, and resolution. The ticketing system provides the means to document, track, notify, and escalate incidents that are reported. Incidents are classified based on urgency and include an initial description of the incident which can be linked to an impacted asset (e.g., a server). Incident tickets also include a history of the steps followed to resolve the particular issue.

2. **Communication Systems**
   Management is involved with day-to-day operations and provide personnel with an understanding of their individual roles and responsibilities. This includes providing the necessary training to ensure that personnel understand how their daily activities and roles relate to the overall support of services. Management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed.

3. **Risk Assessment**
   A Risk Assessment Policy is maintained by management that defines the responsibilities and processes for evaluating risks to the organization and determining safeguards to mitigate or reduce those identified risks to an acceptable level.

   ITBoost’s recognition of risks that could affect the organization’s ability to provide reliable services for its user entities is generally implicit, rather than explicit. Management’s involvement in the daily operations allows them to learn about risks through direct personal involvement with personnel and outside parties.

   Identified risks are documented and ranked in the risk register. The risk register is updated at least annually and includes rankings based on a combination of impact and likelihood, identified mitigation activities, and mitigation owners.

4. **Access Requests and Access Revocation**
   An access request form is completed for personnel as a component of the hiring procedures prior to granting system access. The form is authorized by the appropriate supervisor or manager and documents the equipment provided and types of system access required. The completed form is provided to the corporate IT team to provision the requested level of access. Employees are limited to system resources that they require to perform their job responsibilities.

   A similar form is completed as a component of the termination process to collect equipment assigned to the employee and to revoke system access. The completed form is distributed to corporate IT so that system access can be revoked.
F. User Entity Controls

ITBoost’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. ConnectWise’s control policies and procedures were designed with the assumption that certain controls as defined below, would be in place and in operation at the sub-service organization and user entities. Sub-service organization controls and user entity internal controls must be evaluated, taking into consideration ConnectWise controls and their own internal controls. ConnectWise’s management does not make any representations regarding responsibility related to, or provide any assurance in regard to any such internal control or regulatory requirements for which the client must assess or comply.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine if the identified complementary user entity control responsibilities as defined in the following, have been implemented and are operating effectively:

- User entities are responsible for informing ITBoost of any regulatory issues that may affect the services provided by ITBoost to the user entity.
- User entities are responsible for understanding and complying with their contractual obligations to ITBoost.
- User entities are responsible for determining whether ITBoost’s security infrastructure is appropriate for its needs and notifying ITBoost personnel of any requested modifications.
- User entities are responsible for notifying ITBoost personnel, in a timely manner, when changes are made to technical, billing, or administrative contact information.
- User entities are responsible for ensuring that appropriate individuals have the requisite training on ITBoost software.
- User entities are responsible for ensuring the confidentiality of any user IDs and passwords assigned to them for use with ITBoost’s systems.
- User entities are responsible for ensuring that user IDs and passwords are only assigned to authorized individuals and that the roles assigned to the user accounts are appropriate.
- User entities are responsible for the administration of user access for ITBoost applications.
- 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.
- User entities are responsible for immediately notifying ITBoost personnel of any actual or suspected information security breaches, including compromised user accounts.
- User entities are responsible for responding to alert notifications.

G. Subservice Organizations

ConnectWise uses Amazon Web Services 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 following control functions performed by AWS are critical to achieving the Company’s service commitments and system requirements based on the applicable trust services criteria:

- Physical security of the datacenters hosting the in-scope applications,
- Environmental controls, around the backup processes at the datacenters hosting the in-scope applications to support the disaster recovery processes, and
- Processes to ensure the secure destruction of decommissioned equipment.

ConnectWise has deployed the following controls to help monitor the subservice organization:

- On an annual basis, management evaluates the performance of the third-party organization to help ensure the compliance with commitments and agreed-upon service level agreements.