TeamViewer Germany GmbH
Type 2 SOC 3
2020

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

January 1, 2020 to September 30, 2020

Table of Contents

SECTION 1

ASSERTION OF TEAMVIEWER GERMANY GMBH MANAGEMENT

ASSERTION OF TEAMVIEWER GERMANY GMBH MANAGEMENT

November 30, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within TeamViewer Germany GmbH's ('TeamViewer' or 'the Company') TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting Services System throughout the period January 1, 2020 to September 30, 2020, to provide reasonable assurance that TeamViewer's service commitments and system requirements relevant to Security and Availability (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "TeamViewer Germany GmbH's Description of Its TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting Services System throughout the period January 1, 2020 to September 30, 2020" 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 period January 1, 2020 to September 30, 2020, to provide reasonable assurance that TeamViewer's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy* (AICPA, *Trust Services Criteria*). TeamViewer's objectives for the system in applying 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 presented in "TeamViewer Germany GmbH's Description of Its TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting Services System throughout the period January 1, 2020 to September 30, 2020".

TeamViewer uses ANEXIA Internetdienstleistungs GmbH ('ANEXIA') to provide hosting and information technology services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TeamViewer, to achieve TeamViewer's service commitments and system requirements based on the applicable trust services criteria. The description presents TeamViewer's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TeamViewer's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve TeamViewer's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of TeamViewer's controls.

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 period January 1, 2020 to September 30, 2020 to provide reasonable assurance that TeamViewer's service commitments and system requirements were achieved based on the applicable trust services criteria.

Karl Markgraf

Karl Markgraf
Chief Operations Officer
TeamViewer Germany GmbH

ppa. Mike Eissele

Mike Eissele
Chief Technology Officer
TeamViewer Germany GmbH

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To TeamViewer Germany GmbH:

Scope

We have examined TeamViewer Germany GmbH's ('TeamViewer' or 'the Company') accompanying description of TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting Services System titled "TeamViewer Germany GmbH's Description of Its TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting Services System throughout the period January 1, 2020 to September 30, 2020" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2020 to September 30, 2020, to provide reasonable assurance that TeamViewer's service commitments and system requirements were achieved based on the trust services criteria relevant to Security 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*).

TeamViewer uses ANEXIA to provide hosting and information technology services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TeamViewer, to achieve TeamViewer's service commitments and system requirements based on the applicable trust services criteria. The description presents TeamViewer's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TeamViewer's controls. The description 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 description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TeamViewer, to achieve TeamViewer's service commitments and system requirements based on the applicable trust services criteria. The description presents TeamViewer's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of TeamViewer's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

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

Inherent Limitations

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

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

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

Opinion

In our opinion, management's assertion that the controls within TeamViewer's TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting Services System were suitably designed and operating effectively throughout the period January 1, 2020 to September 30, 2020, to provide reasonable assurance that TeamViewer's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on TeamViewer’s website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of TeamViewer, user entities of TeamViewer’s TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting services during some or all of the period January 1, 2020 to September 30, 2020, business partners of TeamViewer subject to risks arising from interactions with the TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting services, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
November 30, 2020

SECTION 3

TEAMVIEWER GERMANY GMBH’S DESCRIPTION OF ITS TEAMVIEWER, IOT, PILOT, TENSOR, REMOTE MANAGEMENT AND TEAMVIEWER MEETING SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2020 TO SEPTEMBER 30, 2020

OVERVIEW OF OPERATIONS

Company Background

Launched in 2005, TeamViewer focuses on cloud-based technologies to enable online support and collaboration in real time across the globe.

People have collectively used the technology from TeamViewer in billions of instances where distance and time would have otherwise prevented them from accomplishing their goals. TeamViewer has been installed on over 2 billion devices (each device generates a unique ID), creates 750,000 new IDs every day, has over 35 million devices online at any given time and can provide software and support for more than 30 languages.

With TeamViewer Tensor™ (a cloud-based enterprise connectivity platform enabling large-scale Information Technology (IT) management framework deployments quickly and easily), TeamViewer Pilot (augmented reality enhanced remote support), TeamViewer Internet of Things (IoT) (Remote Operations, Assistance and Alarming for All "Things"), TeamViewer Remote Management (Protect and monitor remote devices and keep track of IT assets) and TeamViewer Meeting (a meeting functionality which provides a platform for users to communicate through audio/video calling), TeamViewer has expanded its portfolio with technologies that enable IT professionals to more quickly manage, collaborate, and enable their infrastructure and users across the globe.

Description of Services Provided

TeamViewer Tensor™ is a cloud-based enterprise connectivity platform enabling large-scale IT management framework deployments quickly and easily. Built upon the world's largest remote connection infrastructure already covering 200 countries and connecting more than 2 billion devices, TeamViewer Tensor™ scales linearly to the needs of the enterprise, providing connectivity and real-time support tools in a convenient, ready-to-deploy Software as A Service (SaaS) environment. Product features of TeamViewer Tensor™ include the following:

- Single Sign-On Security - The full power of the world's largest connectivity network is now available to integrate with corporate cloud identity platforms. TeamViewer Tensor™ works with any identity provider that uses Security Assertion Markup Language (SAML) 2.0 for single sign-on for cloud-based identity and access control
- Device-Agnostic Connectivity - Perfect for enterprises who support Bring Your Own Device (BYOD) or Chose Your Own Device (CYOD) flexibility. TeamViewer Tensor™ provides an added layer of network connectivity with unprecedented simplicity and accessibility to any team, while staying within corporate security guidelines
- Comprehensive Logging - The advent of the connected workplace has given birth to new kinds of threats and TeamViewer Tensor™ brings a new level of auditability to the enterprise. Now every connection made to and from Personal Computers (PCs) to the TeamViewer Tensor™ platform can be audited
- Silent Rollout - TeamViewer Tensor™ can be installed and updated silently on all corporate devices by network admins with appropriate security access. Enterprises are able to provide interruption-free device and functional support, while keeping all devices in the network humming with the latest software updates
- Your IoT Device, Our Global Network - TeamViewer Tensor™ IoT connector allows for connections to devices or sensors from anywhere without accessing any special network. TeamViewer's framework allows enterprises to build IoT connectors and feed their own data and sensors into the IoT network
- Augmented Reality Remote Guidance - Integrating TeamViewer Pilot™ provides an enhanced set of augmented reality tools that enable onsite employees or clients to share their problem through their smartphone's camera view and receive help to address the problem.

TeamViewer Pilot is an augmented reality enhanced remote support. Augmented reality enables fixing of issues beyond the screen - no matter how far away. With TeamViewer's augmented reality solution TeamViewer Pilot, a smartphone can be utilized to see through the connected partner's smartphone camera. At a glance, any kind of equipment, machinery, infrastructure issue, and more can be observed. Guidance can be provided by setting Three Dimension (3D) markers onto real-world objects. Product features of TeamViewer Pilot include the following:

- Remote Camera Sharing and Real-Time Video Streaming - Enable on-site employees or clients to share their smartphone's camera view
- High Definition (HD) Voice Over Internet Protocol (VoIP) - Speak to a service technician or client on the other side of the screen, providing detailed instructions on how to fix the issue at hand
- Highlighting on 3D objects and Adding Text - Help on-site employees or customers fix an issue by drawing and highlighting on the screen onto real-world objects, as well as adding text descriptions
- Freeze image - Pause a video stream to get a clear still image to highlight and discuss technical details, as well as work hands-free
- Mobile to mobile - Use an iPhone Operating System (iOS) or Android device to connect and support anyone with a smartphone or smart glasses

TeamViewer IoT enables instant connection, monitoring, and operation of machines and devices securely - from anywhere. Full visibility into all IoT devices with real-time status alerts and early insights are available, to facilitate a quick reaction to mitigate risks and proactively solve issues, before they impact the business. Product features of TeamViewer IoT include the following:

- Real-time Data Visualization on Edge and in the Cloud - Get a complete overview of all company IoT data in one single dashboard in the cloud or on the edge
- One-click Monitoring and Control - Monitor and control devices on the edge or via the cloud with one solution
- Multi-Condition Rules and Data-Based Alerts - Set multi-condition rules at specific thresholds for IoT devices and get alerts with real-time status updates
- Remote Screen Grabbing - Remotely capture what is being displayed on an operation panel of any endpoint, and work as if right in front of it
- Remote Control for Edge Device - Get secure, seamless access to control IoT edge devices remotely, secured by end-to-end encryption without complicated system configuration
- Fast, Flexible Integration - Easily integrates into common third-party platforms with Application Programing Interfaces (APIs) and Software Development Kits (SDKs), compatible with most widely used protocols to customize the IoT solution

TeamViewer Remote Management provides users with the ability to monitor devices from a centralized, remote location. The application allows users to set up checks such as online status, disk health and memory usage, and receive notifications when a certain threshold is exceeded. TeamViewer Remote Management provides users with a solution to view and generate reports on remote devices' hardware and installed software. TeamViewer Remote Management protects users' computers against threats such as viruses, Trojans, rootkits and spyware. Product features of TeamViewer Remote Management include the following:

- Monitor - Set up checks like online status, disk health and memory usage, and get notified when a certain threshold is exceeded. TeamViewer Monitoring provides an overview of the critical aspects of the managed systems from one place. By defining groups of devices and creating individual check policies, TeamViewer Monitoring can be adjusted to the customer's specific needs
- Asset Management - TeamViewer Asset Management provides a solution to view and generate reports on all of the customer's devices' hardware, installed software and more with only a few clicks. See what version a software is, and when it was installed or modified. Detect inappropriate software and eliminate risks

- Endpoint Protection - Keep computers clean and safe. TeamViewer Endpoint Protection protects computers against threats such as viruses, ransomware, Trojans, rootkits and spyware. 24/7 - no matter if on- or offline. Determine time, scope and thoroughness of each check-policy and apply them to different computers or groups. TeamViewer Endpoint Protection maintains itself and is always up to date to ensure maximum safety
- Backup - TeamViewer Backup is simple, hassle-free, and reliable solution to endpoint data protection. Deploy and activate TeamViewer Backup remotely within seconds

The TeamViewer Meeting installs on desktops or mobile phones for quick access to all of the customer's (TeamViewer Meeting and TeamViewer) contacts, enabling logged and indexed team messaging, face-to-face HD VoIP video and audio calling, instant or scheduled huge group meetings (up to 300 people), screen sharing, and session recording for later use - all the essential meeting tools needed to communicate better with teams and clients. Product features of TeamViewer Meeting Collaboration Companion includes the following:

- Instant Meetings - Focus on the meeting, not figuring out how to start and join a meeting. Instant meetings always one click away
- 1-Click Voice Calls - Start a VoIP call with TeamViewer Meeting, and reach audiences on their desktop or mobile app, with one click
- Host Huge Huddles - Host all-hands meetings with up to 300 people to huddle for big announcements
- Meet with Anyone™ - One click to join a TeamViewer Meeting session directly from any browser or mobile device, no software required
- Indexed Messaging - Stop tracking multiple e-mail chains and collaborate quickly with advanced chat messaging, indexed to save brilliant ideas
- TeamViewer™ Security - Built with TeamViewer security, TeamViewer Meeting is ISO27001 certified, with 256Bit end-to-end encryption, protecting sessions

Principal Service Commitments and System Requirements

TeamViewer designs its processes and procedures related to their products to meet its objectives for its remote access, collaboration and managing services. Those objectives are based on the service commitments that TeamViewer makes to user entities, the laws and regulations that govern the provision of remote access, collaboration and managing services, and the financial, operational, and compliance requirements that TeamViewer has established for the services. The remote access, collaboration and managing services of TeamViewer are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which TeamViewer operates.

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 commitments are standardized and include, but are not limited to, the following:

Security principles are within the fundamental designs of the products 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.

Use of encryption technologies to protect customer data both at rest and in transit.

TeamViewer establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in TeamViewer'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 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. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the TeamViewers products.

Components of the System

Infrastructure

Primary infrastructure used to provide TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Firewalls	FortiGate (Customer Production) Palo Alto (Corporate IT and offices)	Filters traffic into and out of the private network supporting the corporate services.
Server	Dell R640, R6525	TeamViewer Master environment
Network	Juniper MX240, QFX5100-96s	TeamViewer Master environment

Software

Primary software used to provide TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Matrix 42 Empirum	Windows, MacOS, Linux	Network Inventory, Asset Management, Software Deployment
(Atlassian) Jira & Confluence	Windows Server	Project management and documentation tools for agile teams
Microsoft Customer Relationship Management (CRM)	Windows Server	Customer relations tool
Veeam backup & replication	Windows Server	Backup & Replication software
GitHub	Windows Server	GitHub is an open source tool used as the code repository.
Freshservice	SaaS	Freshservice is used as a ticketing tool for tracking service and purchase requests, incidents and infrastructure changes.

Primary Software		
Software	**Operating System**	**Purpose**
Freshdesk	SaaS	Freshdesk is used as a ticketing tool for tracking customer support requests.

People

TeamViewer staff provide support for services in each of the following functional areas:

- Executive Board - provides oversight to the TeamViewer organization
- Product Management - dealing in planning, forecasting, production and marketing of TeamViewer software
- Business Development - responsible for creating long term value for TeamViewer's customers, markets and relationships
- Finance Department - responsible for all accounting, financing, purchasing and treasury activities within TeamViewer
- Procurement - oversees the action of obtaining possessions for the benefit of TeamViewer
- Development Team - cross functional team located within Europe responsible for application and database production maintaining product lifecycle
- Quality assurance team - verifies that the software complies with the functional specification through functional testing procedures
- IT - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues
- Marketing - performs planning, research, communication and strategies for delivering product information to customer base and understanding customer's needs
- Corporate IT Security - responsible for overseeing the security of the corporate infrastructure, suppling IT Security policies and governing the overall security posture
- Product Security - responsible for the security of the products (includes codes, functions and provisioning), the security for the production environment

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured which is utilized by TeamViewer in delivering its data system. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, Intrusion Detection System (IDS) alerts, or automated patching systems
- Incident reports documented via the ticketing systems

TeamViewer does not store, access, or transmit Electronic Protected Health Information (ePHI) data.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the TeamViewer policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any TeamViewer team member.

Physical Security

TeamViewer does not own, lease or operate physical IT infrastructure for either its offices or production environment. TeamViewer production environment is a strictly cloud-based infrastructure residing in ANEXIA data centers.

Logical Access

TeamViewer uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In situations in which incompatible responsibilities cannot be segregated, TeamViewer implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing reviews of access by role.

Employees sign on to the TeamViewer network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the TeamViewer network are required to use a Virtual Private Network (VPN) tunnel and two-factor authentication system. Employees are issued VPN certificates upon employment and access is disabled during their exit interview.

Customer's employees access two-factor authentication services through the Internet using the Secure Socket Layer (SSL) functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with TeamViewer's configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Customer employees may sign on to their systems using virtual server administration accounts. These administration accounts use a two-factor digital certificate-based authentication system.

Upon hire, employees are assigned to a position in the HR management system. Ten days prior to the employee's start date, the HR team creates an onboarding ticket which includes the employee's user IDs and the access rights which need to be granted. The ticket is used by the IT Service Desk to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The ticket system has a template for employees that changes position and the associated rights which needs to be changed within the access rules.

On an annual basis, access rights are reviewed by team leads, to see if access rights can be revoked. While evaluating access, team leads consider job description, duties requiring separation, and risks associated with access rights.

The HR team creates tickets if an employee gets terminated. These tickets are processed by the IT Service Desk to delete employee access. The IT Service Desk uses the tickets to suspend user IDs and delete all access roles from IDs belonging to the employee of the ticket.

Managers review the lists and indicate the required changes in the event management record. The record is routed back to the security help desk for processing. The IT Service Desk manager identifies any records not returned within two weeks and follows up with the manager. As part of this process, the Information Security Officer (ISO) reviews employees with access to privileged roles and requests modifications through the event management system.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Backup infrastructure is physically secured in locked cabinets and/or caged environments within the third-party data centers. The backup infrastructure resides on private networks logically secured from other networks.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

TeamViewer monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements.

TeamViewer evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power and cooling
- Disk storage
- Tape storage
- Network bandwidth

TeamViewer has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and TeamViewer system owners review proposed operating system patches to determine whether the patches are applied.

Customers and TeamViewer systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. TeamViewer staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

TeamViewer maintains documented Software Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes.

Quality assurance testing and results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

All infrastructure changes to the environment are reviewed and approved by the Change advisory board (CAB). The CAB consists at least of the director of “IT Infrastructure”, the director of “Application and Demand-management”, a member of the IT Security team and the requester of the change. This ensures that all changes are reviewed, and quality of implementation is maintained.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network Address Translation (NAT) functionality is utilized to manage internal Internet Protocol (IP) addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by TeamViewer. The third-party vendor’s approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network.

Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible.

Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a TeamViewer on a weekly basis in accordance with TeamViewer policy. Vulnerability scanning are also performed by a Third-Party Vendor upon request on a per client basis in accordance with TeamViewer policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by TeamViewer. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows.

Tools requiring installation in the TeamViewer system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes TeamViewer’s TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting Services System performed in the Clearwater, Florida, United States of America; Adelaide, South Australia, Australia; Yerevan, Armenia; and Göppingen, Baden-Württemberg, Germany facilities.

This report does not include the hosting and information technology solutions services provided by ANEXIA in the Klagenfurt, Austria facility.
.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common and Availability criteria were applicable to the TeamViewer, IoT, Pilot, Tensor, Remote Management and TeamViewer Meeting Services System.

Subservice Organizations

This report does not include the hosting and information technology solutions services provided by ANEXIA in the Klagenfurt, Austria facility.

Subservice Description of Services

TeamViewer does not own, lease or operate physical IT infrastructure for either its offices or production environment. TeamViewer production environment is a strictly cloud-based infrastructure residing in the ANEXIA data center. TeamViewer is relying on ANEXIA to perform their internal management and control of their secure environment.

Complementary Subservice Organization Controls

TeamViewer’s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to TeamViewer’s services to be solely achieved by TeamViewer control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of TeamViewer.

The following subservice organization controls should be implemented by ANEXIA to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - ANEXIA		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4; CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.

Subservice Organization - ANEXIA		
Category	**Criteria**	**Control**
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
		All data centers are equipped with fire detection alarms and protection equipment.
		Data center server floors and network rooms are connected to an UPS system and emergency generator power is available in the event of a loss of power.
		Information is protected from damage resulting from water leakage by providing shutoff valves that are accessible, working properly and known to key personnel.

TeamViewer management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, TeamViewer performs monitoring of the subservice organization controls, including the following procedures:

- Holding discussions with vendors and subservice organizations
- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

TeamViewer’s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Principles related to TeamViewer’s services to be solely achieved by TeamViewer control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of TeamViewer.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Principles described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities’ locations, user entities’ auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to TeamViewer.

2. User entities are responsible for notifying TeamViewer of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of TeamViewer services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize TeamViewer services.
6. User entities are responsible for providing TeamViewer with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying TeamViewer of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.