TeamViewer Germany GmbH

Type 2 SOC 3

2024

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

October 1, 2023 to September 30, 2024

Table of Contents

SECTION 1

ASSERTION OF TEAMVIEWER GERMANY GMBH MANAGEMENT

ASSERTION OF TEAMVIEWER GERMANY GMBH MANAGEMENT

November 20, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within TeamViewer Germany, GmbH's ('TeamViewer' or 'the Company') TeamViewer Engage, TeamViewer Classroom, Internet of Things (IoT), Assist AR, Tensor, Remote Management, TeamViewer Meeting Services and TeamViewer Frontline System throughout the period October 1, 2023 to September 30, 2024, to provide reasonable assurance that TeamViewer's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "TeamViewer Germany, GmbH's Description of Its TeamViewer Engage, TeamViewer Classroom, Internet of Things (IoT), Assist AR, Tensor, Remote Management, TeamViewer Meeting Services and TeamViewer Frontline System throughout the period October 1, 2023 to September 30, 2024" 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 October 1, 2023 to September 30, 2024, to provide reasonable assurance that TeamViewer's service commitments and system requirements were achieved based on the trust services criteria. TeamViewer'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 presented in "TeamViewer Germany, GmbH's Description of Its TeamViewer Engage, TeamViewer Classroom, Internet of Things (IoT), Assist AR, Tensor, Remote Management, TeamViewer Meeting Services and TeamViewer Frontline System throughout the period October 1, 2023 to September 30, 2024".

TeamViewer uses ANEXIA Internetdienstleistungs GmbH ('ANEXIA') to provide hosting and information technology solutions services and Microsoft Azure ('Azure') to provide cloud hosting services (collectively, the 'subservice organizations'). 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 organizations.

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 October 1, 2023 to September 30, 2024 to provide reasonable assurance that TeamViewer's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of TeamViewer's controls operated effectively throughout that period.

Mei Dent

ppa. Mei Dent
Chief Product and Technology Officer
TeamViewer Germany, GmbH

Kai Werner

ppa. Kai Werner
Group General Counsel
TeamViewer Germany, GmbH

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To TeamViewer Germany GmbH:

Scope

We have examined TeamViewer's accompanying assertion titled "Assertion of TeamViewer Germany GmbH Management" (assertion) that the controls within TeamViewer's TeamViewer Engage, TeamViewer Classroom, Internet of Things (IoT), Assist AR, Tensor, Remote Management, TeamViewer Meeting Services and TeamViewer Frontline System were effective throughout the period October 1, 2023 to September 30, 2024, to provide reasonable assurance that TeamViewer's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

TeamViewer uses ANEXIA to provide hosting and information technology solutions services and Azure to provide cloud hosting 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 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 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 also provided the accompanying assertion (TeamViewer assertion) about the effectiveness of controls within the system. When preparing its assertion, TeamViewer 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 management's assertion that 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 AICPA. 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 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 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

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

Independence and Ethical Responsibilities

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

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 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 Engage, TeamViewer Classroom, Internet of Things (IoT), Assist AR, Tensor, Remote Management, TeamViewer Meeting Services and TeamViewer Frontline System were suitably designed and operating effectively throughout the period October 1, 2023 to September 30, 2024, 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, if complementary subservice organization controls and complementary user entity controls assumed in the design of TeamViewer's controls operated effectively throughout that period.

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 Engage, TeamViewer Classroom, Internet of Things (IoT), Assist AR, Tensor, Remote Management, TeamViewer Meeting Services and TeamViewer Frontline System during some or all of the period October 1, 2023 to September 30, 2024, business partners of TeamViewer subject to risks arising from interactions with the TeamViewer Engage, TeamViewer Classroom, Internet of Things (IoT), Assist AR, Tensor, Remote Management, TeamViewer Meeting Services and TeamViewer Frontline System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity 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 20, 2024

SECTION 3

TEAMVIEWER GERMANY GMBH'S DESCRIPTION OF ITS TEAMVIEWER ENGAGE, TEAMVIEWER CLASSROOM, INTERNET OF THINGS (IOT), ASSIST AR, TENSOR, REMOTE MANAGEMENT, TEAMVIEWER MEETING SERVICES AND TEAMVIEWER FRONTLINE SYSTEM THROUGHOUT THE PERIOD OCTOBER 1, 2023 TO SEPTEMBER 30, 2024

OVERVIEW OF OPERATIONS

Company Background

Launched in 2005, TeamViewer focuses on cloud-based technologies to enable online support and collaborate 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, has over 35 million devices online at any given time and can provide software and support for greater than 30 languages.

With TeamViewer Tensor (a cloud-based enterprise connectivity platform enabling large-scale IT management framework deployments), TeamViewer Assist AR (augmented reality enhanced remote support), TeamViewer Embedded (Remote Operations, Assistance and Alarming for All “Things”), TeamViewer Remote Management (Protect and monitor remote devices and keep track of IT assets), TeamViewer Frontline (AR Productivity Solutions), TeamViewer Engage (Digital Customer Engagement), 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 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 an enterprise, providing the industry’s leading connectivity and real-time support tools in a convenient, ready-to-deploy 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 available to integrate with corporate cloud identity platform. TeamViewer Tensor works with any identity provider that uses SAML 2.0 for single sign-on for cloud-based identity and access control.
- **Conditional Access** is a framework allowing to control which devices, users, and user groups using TeamViewer Tensor have access to which data sources, services, and applications in the organization. With Conditional Access, Enterprise IT and security managers can maintain company-wide oversight of TeamViewer access and usage from a single location.
- **Device-Agnostic Connectivity** - Perfect for enterprises who support BYOD (bring your own device) or CYOD (choose your own device) flexibility, TeamViewer Tensor provides an added layer of network connectivity with unprecedented simplicity and accessibility, 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 can audit every connection made to and from PCs to the TeamViewer Tensor platform.
- **Silent Rollout** - TeamViewer Tensor can be installed and updated silently on corporate devices by network admins with appropriate security access. It provides interruption-free device and functional support, while keeping devices in the network running with the latest software updates.
- **Your Embedded Device, TeamViewer’s Global Network** - TeamViewer Tensor Embedded connector allows the client to connect to devices or sensors from anywhere without accessing any special network. TeamViewer’s framework allows enterprises to build their own embedded connectors and feed data and sensors into TeamViewer’s embedded network.
- **Augmented Reality Remote Guidance** - Integrating TeamViewer Assist AR provides an enhanced set of augmented reality tools that enable onsite employees or clients to share their smartphone’s camera view. The camera acts as the eyes, allowing the problem to be seen and assistance to be provided to the person onsite.

TeamViewer Assist AR is an augmented reality-enhanced remote support tool. Augmented reality enables fixing issues beyond the screen, regardless of distance. With this solution, it is possible to see through the connection partner's smartphone camera, making it easy to observe any kind of equipment, machinery, infrastructure issues, and more. Guidance is provided by setting 3D markers onto real-world objects. Product features of TeamViewer Assist AR include the following:

- Remote Camera Sharing and Real-Time Video Streaming - Enable on-site employees or clients to share their smartphone's camera view. The camera acts as the eyes, allowing the problem to be seen and assistance to be provided to the person onsite.
- HD VoIP - Speak to the service technician or client on the other side of the screen, giving them detailed instructions on how to fix the issue at hand.
- Highlighting on 3D objects and Adding Text - Help the on-site employee or customer fix the issue by drawing and highlighting on the screen onto real-world objects, as well as adding text descriptions.
- Freeze image - Pause the 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 iOS or Android device to connect and support anyone with a smartphone or smart glasses.

TeamViewer Embedded enables instant and secure connection, monitoring, and operation of machines and devices from anywhere. Full visibility into embedded devices is provided with real-time status alerts and early insights, allowing for quick reactions to mitigate risks and proactively solve issues before they impact business operations. Product features of TeamViewer Embedded include the following:

- One-click Monitoring and Control - Monitor and control devices on the edge or via the cloud with one solution.
- Remote Screen Grabbing - Remotely capture what is being displayed on an operation panel of any endpoint.
- Remote Control for Edge Device - Get secure, seamless access to control embedded edge devices remotely, secured by end-to-end encryption without complicated system configuration.
- Fast, Flexible Integration - Easily integrates into common third-party platforms with APIs and SDKs, compatible with most widely used protocols to customize the embedded solution.

TeamViewer Remote Management provides users with the ability to monitor its devices from a centralized, remote location. This 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 the user with an overview of the critical aspects of their systems from one place. By defining groups of devices and creating individual check policies, TeamViewer Monitoring can be adjusted to meet specific needs.
- Asset Management - TeamViewer Asset Management provides users with a solution to view and generate reports on 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 Detection and Response - Keeps 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. Don't worry about updates anymore - TeamViewer Endpoint Protection maintains itself and is always up to date to ensure maximum safety.
- Backup - TeamViewer Backup is a backup solution to endpoint data protection that can deploy and activate TeamViewer Backup remotely within seconds. Customer data will be stored in the cloud using the highest security standards.

TeamViewer Frontline is a solution to digitalize and streamline processes for frontline employees in desk-free workspaces with AR-guided solutions - seamlessly integrated with wearables and mobile devices - increasing productivity, efficiency, and quality along the entire value chain. Product features of TeamViewer Frontline includes the following:

- Security - Protect and control intellectual property rights of workflow apps
- Independence - No external resources like additional software or hardware needed
- Agility - Create and edit AR workflow applications instantly
- Scalability - Companies can easily transfer requisites from one site to the next
- Flexibility - Forward task changes immediately to frontline workforce
- Usability - Easy to use with no programming know-how required

TeamViewer Engage is a next-gen digital customer engagement platform for online sales, digital customer service, and video consultations that empowers companies to elevate their customer experience for lifelong brand loyalty.

With scalable cloud or on-premises deployment options, single sign-on (SSO) integration, and built-in security, TeamViewer Engage is enterprise-ready to meet requirements. Manage TeamViewer Engage users with existing SSO or role-based access control system and ensure proper auditability of customer engagements. Product features of TeamViewer Engage includes the following:

- Co-Browsing - Co-Browsing streamlines communication between customer and agent through advanced, hassle-free screen sharing technology. Use TeamViewer Engage to Co-Browse with customers on any device, across browsers - without downloads or installation.
- Chatbots - Create automated chat dialog flows based on prebuilt conditional rules to pre-qualify leads, answer common questions, and more. If problems are too complex for automated Chatbot guidance, an agent will be alerted and can seamlessly take over through Live Chat.
- Live Chat - Integrate TeamViewer's Live Chat solution on websites to convert visitors into customers and provide instant support. Empower agents with helpful tools to increase their efficiency, such as automated chatbot flows and predefined answers to frequently asked questions.
- Video Chat - Offer customers an even more personalized experience with Video Chat. Conduct customer consultations, sales calls, remote home inspections, tech support, and more. Integrate Video Chat into customer websites, online customer portal, or mobile app for one-click access to digital customer service.
- eSignature - Available with Document Co-Browsing, this is a legally binding electronic signature tool enabling users to get contracts, proposals, forms, or any digital document signed legally by eSignature in seconds, from any device - without investing in separate software.
- Appointment Scheduling - Easily prepare and manage sales and consultation appointments with TeamViewer Engage. Sync appointments with users' favorite calendar app, send e-mail appointment invitations, and use the Appointment Booker to let customers reserve calendar time.

Any existing products that are not explicitly mentioned are still in scope of this report even if they are End of Life or in the phase out portion of the product lifecycle.

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 the TeamViewer Engage, TeamViewer Classroom, Internet of Things (IoT), Assist AR, Tensor, Remote Management, TeamViewer Meeting Services and TeamViewer Frontline 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
Operating System	Cent OS / Rocky Linux	TeamViewer Master environment

Software

Primary software used to provide TeamViewer Engage, TeamViewer Classroom, Internet of Things (IoT), Assist AR, Tensor, Remote Management, TeamViewer Meeting Services and TeamViewer Frontline System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Intune	SaaS Azure	Network Inventory, Asset Management, Software Deployment, to manage Windows and Mac OS devices

Primary Software		
Software	**Operating System**	**Purpose**
(Atlassian) Jira & Confluence	SaaS	Project management and documentation tools for agile teams
E-mail	SaaS (Microsoft Office 365 suite)	E-Mail
CRM	Microsoft Dynamics SaaS	Customer relations tool
Microsoft Office 365	Azure	SaaS (Microsoft Office 365 suite) includes E-mail, SharePoint, and Teams communication system
Veeam backup & replication	Windows Server	Backup & Replication software
Github	SaaS and 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
FreshDesk	SaaS	FreshDesk is used as a ticketing tool for tracking customer support requests
WordPress	SaaS	Website content management
Adobe Experience Manager	SaaS	Website content management
Tableau	SaaS	Business reporting and analytics

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 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, IDS alerts, or automated patching systems
- Incident reports documented via the ticketing systems

TeamViewer does not store, access, or transmit ePHI data and payment card 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. 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 employee.

As an innovative and knowledge-based company, TeamViewer is particularly reliant on the confidential handling of information. The information cumulated in the company and the accumulated knowledge are significant capital of TeamViewer and has led TeamViewer to implement the security-based controls discussed below.

Physical Security

TeamViewer Group has offices located around the globe. The entrances to the buildings / office areas are restricted to users possessing an access card. Key fobs/Keycards are granted to working employees with business hours access.

Exterior ingress doors are restricted to users possessing an access card/ID that has been assigned access to use the door. The access card/ID system uses zones to control access. Each exterior door and doors to restricted areas within the facilities are assigned to door zones. Access to zones is restricted through the use of access control lists. Employees and vendors granted access cards are assigned to roles based on their job responsibilities.

Visitors check in by contacting their party's action via software and / or phone stationed in the reception area. The visitor's name, employer, and purpose for visit are recorded in a visitor log and his or her visit must be approved by a TeamViewer employee who is authorized to sign non-employees into the facility. The visitor is issued a temporary ID badge to be worn throughout his or her visit. This temporary badge does not permit users access through any secured doors within the facility.

Upon an employee's termination of employment, the HR team generates a ticket for deletion in the ticket system on the last day of employment. This ticket is routed to the access administrators for deletion. In addition, terminated employees turn over their access cards/IDs during their exit interview. These cards are then sent via interoffice mail to IT Administration for recording and destruction. On a monthly basis, the IT Administrator runs a report detailing access cards with deleted access that have not been recorded as returned. The director investigates missing cards and documents the resolution in the event management system.

On a quarterly basis, zone owners review access to their zones. Access listings are generated by security and distributed to the zone owners via the event management system. Zone owners review the listings and indicate the required changes in the event management record. The record is routed back to the access administrators for processing. The director of physical security identifies any records not returned within two weeks and follows up with the zone owner.

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.

Password less Authentication

To further strengthen TeamViewer's corporate security measures, TeamViewer has put password-less and phishing-resistant authentication as a mandatory authentication strength. TeamViewer's accounts must access systems without the need for traditional passwords. This eliminates the risk of password-related security breaches especially through phishing and streamlines the login process.

Conditional Access

TeamViewer has enforced its zero-trust strategy to a 100% zero trust, meaning exclusions have been fully remediated. Only centrally managed and compliant devices together with the predefined authentication strength and a valid certificate can access company resources. Additionally, risk-based detections enforce strong conditional access when accessing company resources.

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

Employees and approved vendor personnel sign on to the TeamViewer network using an Active Directory user ID and a password-less authentication method. 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. Initial 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 the user to reauthenticate after a period of inactivity.

Employees accessing the system from outside the TeamViewer network are required to use a VPN tunnel-two-factor authentication system. Employees are issued VPN certificates upon employment and access is disabled during their exit interview. Vendor personnel are not permitted to access the system from outside the TeamViewer network.

Customer employees' access two factor authentication services through the Internet using the SSL functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Initial 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 employees' 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 the team leads, to see if access or rights can be revoked. While evaluating the access, the team lead considers job description, duties requiring segregation, and risks associated with access.

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 access roles from IDs belonging to the employee of the ticket.

On a quarterly basis, managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system.

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, they review employees with access to privileged roles and requests modifications through the event management system.

TeamViewer does not store, access, or transmit ePHI data and payment card data.

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 and on-site backup tape media are physically secured in locked cabinets and/or caged environments within the third-party data centers. The backup infrastructure resides 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 and endpoints.

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 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 patches have been installed and if applicable that reboots have been completed.

Change Control

TeamViewer maintains documented Secure Software Development Life Cycle (SSDLC) 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 User Acceptance Testing (UAT) 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.

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 & Demand-management”, a member of the IT Security team and the requester of the change. This ensures that 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 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, 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 TeamViewer on a daily basis in accordance with TeamViewer policy. Vulnerability scans 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 from the internet through the use of leading VPN technology. In addition, the user needs a valid certificate on his endpoint. Employees are authenticated using a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes TeamViewer's TeamViewer Engage, TeamViewer Classroom, Internet of Things (IoT), Assist AR, Tensor, Remote Management, TeamViewer Meeting Services and TeamViewer Frontline System performed in Clearwater (United States of America, Florida), Vienna (United States of America, Virginia), Atlanta (United States of America, Florida), Adelaide (Australia, South Australia), Yerevan (Armenia), Linz (Austria), Bremen (Germany, Bremen) and Göppingen (Germany, Baden-Württemberg).

This report does not include the hosting and information technology solutions services provided by ANEXIA or the cloud hosting services provided by Azure at multiple facilities.

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 the12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common/Security, Availability and Confidentiality criteria were applicable to the TeamViewer Engage, TeamViewer Classroom, Internet of Things (IoT), Assist AR, Tensor, Remote Management, TeamViewer Meeting Services and TeamViewer Frontline System.

Subservice Organizations

This report does not include the hosting and Information Technology solutions services provided by ANEXIA and cloud hosting services provided by Azure at multiple facilities.

Subservice Description of Services

Subservice organization	Service Description
ANEXIA	ANEXIA is hosting router servers and the customer environment.
Azure	TeamViewer host the Management Console (login.teamviewer.com) and the CRM in Azure.

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.
		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.
		Control self-assessments that include backup restoration tests are performed on at least an annual basis.
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.

Subservice Organization - ANEXIA		
Category	**Criteria**	**Control**
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Backups of critical system components are monitored for successful replication across multiple Availability Zones.
		Control self-assessments that include backup restoration tests are performed on at least an annual basis.
		When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.
		The ability to restore backups is restricted to authorized personnel.

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

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.
Availability	A1.2	Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.
		Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Customer data is automatically replicated within Azure to minimize isolated faults.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities.
		Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		Production data is encrypted on backup media.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.

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:

- Reviewing and reconciling output reports
- Holding periodic 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 criteria 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 criteria 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 system(s) 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.