Security Description

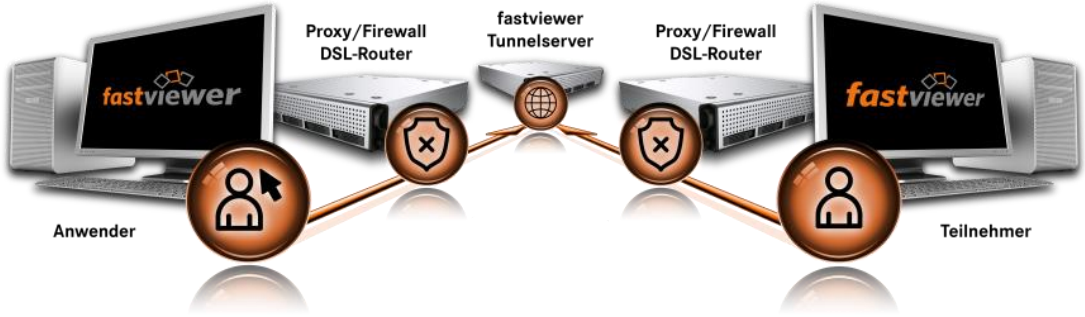
Online-Meetings and Remote Support. Easy & secure.

fastviewer

TABLE OF CONTENTS

GENERAL PROCEDURE	1
ENCRYPTION	4
FASTVIEWER SECURITY	5
EVEN MORE SECURITY	6
SECURITY FEATURES - CUSTOMER PORTAL	8
SECURITY FEATURES - MODULES	9
CERTIFICATES USED (SSL)	12
EXTERNAL CERTIFICATES	13
TECHNICAL & ORGANIZATIONAL MEASURES	14
NOTE: USEAGE WITH OWN SERVER SOLUTION	17

GENERAL PROCEDURE



Welcome to our security description

The security of data connections is becoming increasingly important in our digital world. At FastViewer, we take security very seriously. For this reason, we not only rely on standard protocols but have e.g. created our own encryption within these protocols.
On the following pages you will find an excerpt from our security documents. The document is intended for privacy advocates, security officers and persons interested in the security of data. The aim of the document is to provide a comprehensive insight into the security concept of FastViewer. If you have any further questions, we are at your disposal to answer them.

Protocol

For communication between the FastViewer clients and the FastViewer server only outgoing connections are required. FastViewer does not use its own protocol, but uses the following standard protocols of the respective operating system (in the following order):

- TCP (Port 5000)
- HTTPS Port 443)
- HTTP (Port 80)

All settings of the SSL connection are handled by the operating system of the FastViewer clients or the FastViewer server.
If you operate your own FastViewer server, transport layer security can be determined by the customer himself by configuring the operating system.
When FastViewer is operated within a cloud environment, HTTPS utilizes the TLS 1.2 protocol together with the cipher suite AES256CBC and HMAC-SHA1.

Remarkable:
The protocol is independent of the encryption! Due to the encryption presented below, even data transmitted with HTTP (Port 80) or TCP (Port 5000) is securely encrypted end to end.

FastViewer only needs one port for the transmission of the data. If several ports are available, the highest port is used. The other ports then serve as fallback should the selected port fail. Thus, an interruption-free transmission - even if one port fails – is possible.

GENERAL PROCEDURE

Encryption of data

All user data (screen content, files, chat, VoIP, video and status information) are protected by a 256-bit AES end-to-end encryption. The session key is renegotiated at each session and due to an exchange of key pairs through the RSA procedure is unique to the participants.
This ensures that the data transmitted during a FastViewer session can only be decrypted by the FastViewer participants joining this session. The server is not in possession of the session key and therefore can not decrypt the data.

Remarkable:
Often, a 256-bit AES end-to-end encryption is understood to mean only the HTTPS protocol, in which the transmitted data is only encrypted end to end between the server and the subscriber. With this method, the server can read the transmitted data! FastViewer encrypts the data from the subscriber to the subscriber without the server being able to read the data. This applies to Windows, OSX, iOS and Android operating systems.

Difference Moderator / Client Module

The FastViewer moderator module is used to schedule and start sessions. You can also use the moderator module - provided you have the necessary permissions - to manage the software.
The client module only entitles to attend meetings.

Session setup FastViewer Cloud

First, the moderator module via port 80 obtains a redundantly distributed list of all available FastViewer communication servers.Note: When using the own server solution, the communication server list can also be retrieved exclusively via HTTPS or a freely configurable port.
For more deatils, please: Useage with own server solution on page 17.

After receiving the list, the FastViewer moderator module determines the fastest communication server for this session. Incidentally, the FastViewer customer portal can be used to configure whether the communication is to be made via the FastViewer communication servers distributed worldwide or only in Europe or exclusively in Germany. The servers provided for the respective regions ensure a 100% failure safe operation of the FastViewer Cloud.

The moderator module now connects to the selected FastViewer communication server. A 6-digit session number is obtained via the established connection, which is used for the identification of the correct session by the subscriber. This session number is usually transmitted encrypted by the moderator via telephone or email to the session partner.

Continuation of the session setup FastViewer Cloud

The session participant must enter the received session number into the client module (or start the link in the e-mail invitation). The connection is then made to the identified FastViewer server, which hosts the session for the specified session number.

Subsequently, a 256-bit AES key is negotiated between the participants, which is used for this session. The exchange of the key takes place via the RSA procedure.

In order to ensure that neither the FastViewer communication server nor any other item in the connection can be read, further communication takes place exclusively via the 256-bit AES end-to-end encrypted connection.It is NOT possible for the FastViewer communication server to decrypt the data because it is never in possession of the 256-bit AES key!

Once the secure end-to-end connection between the moderator module and the clinet module has been established, the screen is transferred in the required direction. The session partner can stop the control at any time with the panic button, or disconnect the connection immediately with a mouse click. The client module only entitles to attend meetings.

Note:
The session number presented here has nothing to do with the session key. It merely represents the meeting room and ensures that the participants meet in the same room.

Encryption of files

All files that are set via the FastViewer file storage remain temporarily cached 256-bit AES encrypted on the FastViewer server for the duration of the FastViewer session.
This ensures that each participant can only download the files during the active session. In addition to 256-bit AES encryption of the data itself (see „Encryption of data“ on page 2), the files are still cached as fragmented 64-KB packets. Consequently, not only the contents of the files but also their composition is cryptic.

CRC check

A checksum is built into the program code when compiling the EXE files. If the EXE is changed via a tool, the program can not be used due to a checksum error. This effectively prevents unwanted changes to the program code while ensuring the functionality of all defined security features.

Redundancy – load distribution

The moderator module looks for the fastest available communication server, which will be used for the following session. f you are using your own server solution, a list of the available communication servers is stored in both the moderator module and the client module. If several own servers are in use, or the FastViewer cloud servers are used, then the moderator module checks which of the servers has the shortest reaction time to the request. This server provides the session number and serves as the session's communication server. Thus, a uniform utilization of the server is ensured. he load is distributed automatically.

Authentication

To authenticate a user different options are available in FastViewer, which can also be used in combination.

AD - Authentication

The user administration of FastViewer offers the possibility to import AD groups or AD users. Thus, both the access rights and the use of different profiles can be configured centrally in their Active Directory (AD).

AD - Connection

We know how sensitive the data of the AD are, so we only import the SID of the AD information into FastViewer and check it against the operating system at program start. Thereby we use the standards of your operating systems. There is therefore no need to have access to your AD management during the runtime of the program.

Username and password

Also provides a method to log on to FastViewer. This information is stored in the user management of FastViewer and is available - even outside the company's own AD.

AD - Lock

Prevent the use of FastViewer outside of its domain or restrict the use of FastViewer to an AD group or an AD user. The AD lock can be set in the FastViewer portal and requires no additional user management.

Single-Sign on

With just one click in the user management, all previously used FastViewer programs can be subsequently converted to the single sign on method.

Two way authentication

When accessing remote hosts, security plays a particularly important role. For this reason, we have established a 2-way authentication via SMS. Every access to a remote host (after successful login to the system itself) must be additionally confirmed by entering an SMS PIN on the FastViewer application.
Thus, access to their system is not only safe, but can also be done via a four-eye principle.

EVEN MORE SECURITY

Tamper proof recording

A video recording, which starts automatically on request, can be activated for verification purposes at both the customer and supporter ends. The video data is stored in its own format as an audit-proof EXE file. This prevents later manipulation. The recording file can be played independently at any time by means of an integrated player.

Application security

Secure connections on its own are not enough; the transferred content must also be protected or restricted. We have invested a lot of time to create a portal that allows you to customize FastViewer to the requirements of your privacy policy.

FastViewer Cloud Server

All FastViewer Cloud servers are located in high-security data centers. With the help of your personal customer portal, you can decide for yourself whether you only want to communicate via the German servers, servers in the European Union (EU) or the worldwide FastViewer servers.

If all of this is not sufficient, you can also operate your own FastViewer server in a data center of your choice, your DMZ or in your intranet. All sessions are then handled by your own server, independent of the FastViewer communication servers.

Installation-free usage

FastViewer is one for the moderator, as well as for the customer an installation-free application. After a FastViewer session, the program modules are finished without leaving a trace.

EVEN MORE SECURITY

Especially with unattended support security must be right. For this reason, we have established a sophisticated rights system for our remote solution that works closely with the user administration. Starting with an automated installation including group assignments, to limited access for user groups, we offer everything you need for an unattended remote support solution.

Further information can be found in the user manual of the FastViewer user administration.

One-time remote maintenance?

For remote hosts, the state can be freely defined after a FastViewer session. The computer can be ready immediately for the next session, or after a manual process, ready for the next support session.

Panic button

With a fixed button, remote control and screen sharing can be interrupted immediately. Thus, a user can end a remote control at any time.

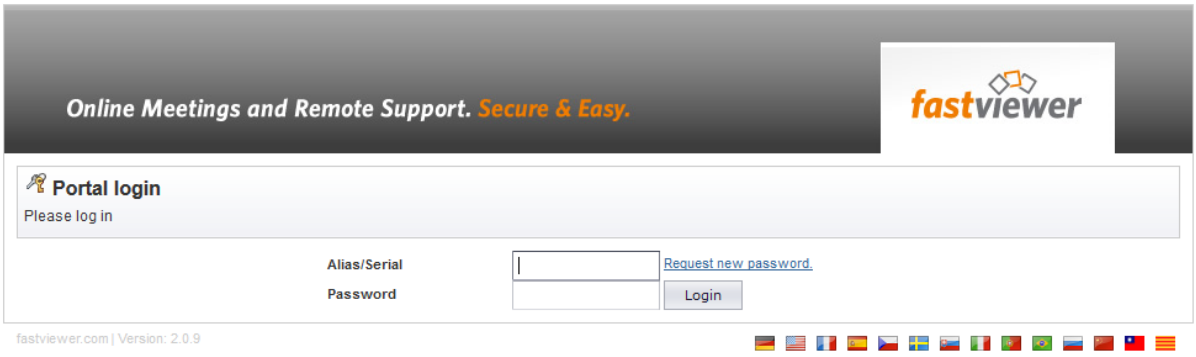
Remote maintenance interrupted?

With FastViewer, you can decide for yourself which state the remote-controlled computer should go to, if a remote control aborts unexpectedly. This ensures that no computer remains unprotected (e.g., open session).

Full control

When releasing the screen transfer, the user always decides which content he wants to release.

SECURITY FEATURES - CUSTOMER PORTAL

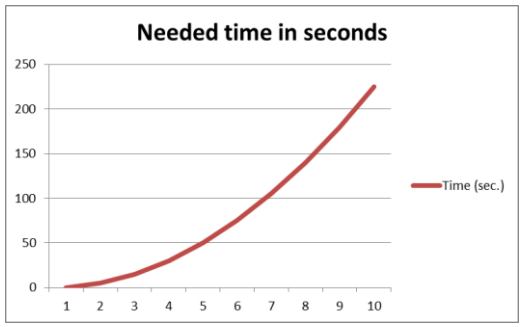


The FastViewer customer portal serves as the configuration platform of the FastViewer solution. Here you can make adjustments to the security, the functionality or the appearance of the software. Access to the FastViewer customer portal is protected by a 10-digit license number and an individual password. Only authorized license holders can access the customer portal and thus the FastViewer modules. Communication with the customer portal is always via HTTPS (port 443).

If the license holder has forgotten his individual password, this can be retrieved via the start page of the portal. The dispatch takes place exclusively to the e-mail address deposited in the portal, which was selected by the license holder when the license was issued.
Secure connections on its own are not enough; the transferred content must also be protected or restricted. We invested a lot of time to create a portal that allows you to customize FastViewer to your privacy policy:

Protection against brute-force

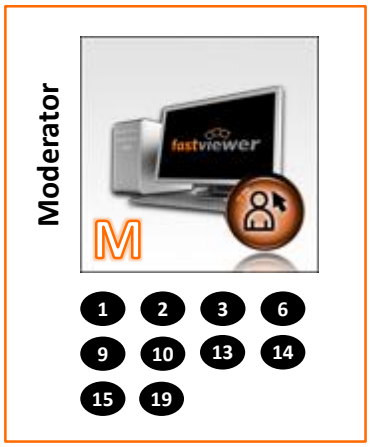
Access to the portal settings of FastViewer is password protected. To avert brute-force attacks, a delay is used, which increases with each erroneous logon. It takes about 5 minutes for 10 attempts.



Black- & Whitelist

The Black- & Whitelist can determine which applications may be transferred or which applications should be explicitly excluded from the transmission.

SECURITY FEATURES - MODULES



1 Video recording

The modertaor and client modules independently allow you to record the active session. The video is saved in its own format including its own FastViewer player. For each opposite side is always visible when a video recording takes place.

2 Logging

During a session, information about the session being performed is stored in an online log. These include the FastViewer user name, the session number used, number of participants, FastViewer version number, Windows login name, host names, IP addresses, free text items, and timestamps. Optionally and via the customer portal adjustable, the transferred application can additionally be logged. The logs can be evaluated and exported via the customer portal or by using a separate server solution via a separate tool.

3 User Management

The moderator module can be protected by the user administration against unauthorized access. With the LDAP import function, AD groups and users can easily get permission to use FastViewer. Thus, both the access rights and the use of different profiles can be configured centrally in their AD.

We know how sensitive the AD data are, so we just import the SID of the AD information into FastViewer and check it against the program at startupOperating system. We use the standards of their operating systems.

There is therefore no need to access your AD management and make adjustments during runtime of the program.

4 Pause function

The active session can be paused at any time by the presenter. The image transfer is frozen.

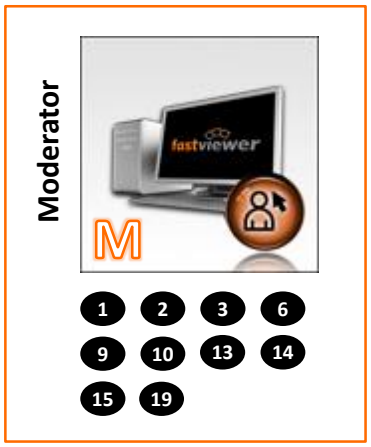
5 Protection functions

The user always has control over the remote maintenance. The control rights can be removed from the supporter by pressing the panic button. The user has the option of canceling file access or the entire session at any time.

6 Active Directory user lock

This feature allows a domain key imported from an existing Active Directory (Domain SID or Domain Group SID) to be used by FastViewer. Users outside the domain / group can not start the modules. Alternatively, FastViewer user management can be used to assign access rights at the user or group level.

SECURITY FEATURES - MODULES



7 Black- & Whitelist

A Black- or Whitelist can be configured in the customer portal to make applications selectively available or to block access. This setting cannot be changed during the active session.

8 Application filter

Before the remote desktop is transmitted, the presenter has the opportunity to select the specific applications to be transmitted. You can also follow the same procedure for the desktop and task bar or newly launched applications. You can, of course, also share the entire desktop.

9 Configuration of the features

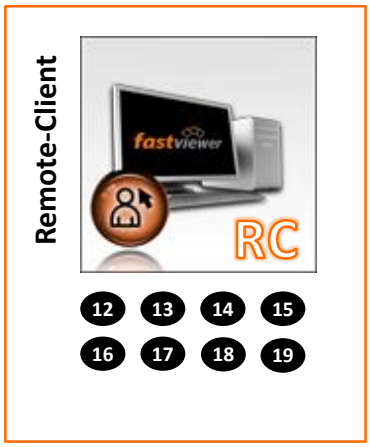
All features can be configured via the customer portal. This makes it possible to customize the interaction between all security features. For example, file transfer and file storage can be prevented. Client control can also be prevented.

10 Ending a session

The customer is able to end the session at any time. This is done by clicking on the Close button in the FastViewer sidebar. In addition, the customer has the option to stop the remote control by pressing the "F11 key" on his or her keyboard. The customer can thus actively prevent changes to his or her system and terminate access.

11 File transfer

If the remote system is accessed by file transfer during an active session, multiple security barriers go into effect. The supported customer must approve the file transfer. If the approval is not granted, the file system cannot be accessed. A shared file transfer or file system access can, of course, also be canceled at any time.



Secure Advisor (Remote Access)

FastViewer Secure Advisor requires particularly intensive protection. Since the remote client only needs an outgoing connection, FastViewer will not open incoming ports. Thus, no hacker attacks are possible. The Windows login provides additional protection to ensure local security.

12 Outgoing connection

The Remote-Client is invisible to outside attacks due to its exclusively outgoing connection.

13 Access restriction

Access is enabled only through the input of a user name and the associated password.

14 As secure as a debit card

FastViewer works like a debit card with a PIN. Login requires possession of the appropriate FastViewer EXE file for the client and knowledge of the right login data.

15 Windows protection

Additional protection is provided by the upstream Windows application of the client (subject to the respective Windows security settings).

16 Service settings

The user must activate the service to grant access (configurable).

17 Access timeout

When accessing a Remote-Client, this timeout determines the time available for the participant to interact.
The FastViewer customer portal can be used to configure whether access to the Remote-Client should be granted or denied after this time. Furthermore the length of the timeout can also be adjusted.

18 Two way authentication

When accessing Remote-Clients, security plays a particularly important role. That's why we have established a 2-way-authentication via SMS, which can be activated for additional security.

Every access to a Remote-Client (after successful login to the system itself) must be additionally confirmed by entering an SMS PIN on the FastViewer application. Thus, access to their system is not only safe, but can also be done via a four-eye principle.

19 Other authentication mechanisms

The use of smart card authentication makes it possible to authenticate subscribers directly and securely. For this purpose, the respective user identifies and authenticates by means of his smartcard and subsequently receives access and authorization to start the Moderator / Client Module.

This authentication mechanism is highly dependent on the particular customer IT infrastructure and smart card solution used by the customer and is generally implemented as a customer-specific solution. Should additional or other access control measures be necessary, please contact us to discuss a solution according to your requirements.

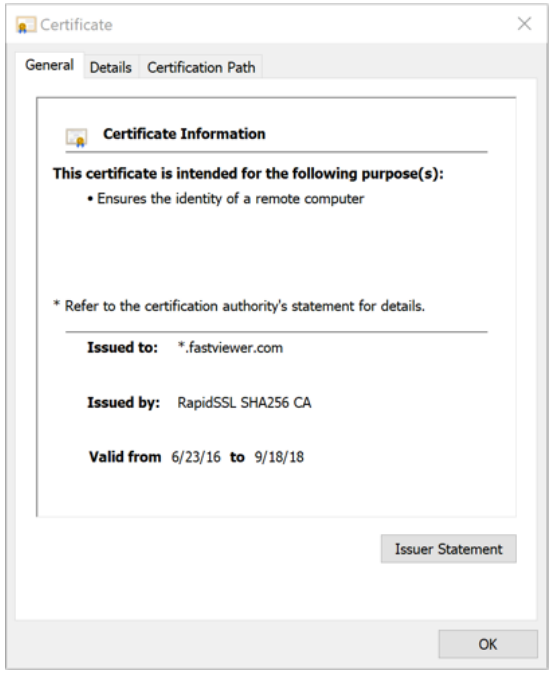
CERTIFICATES USED (SSL)

Server certificate requests

By default, FastViewer communication occurs over TCP 5000 or over HTTPS 443 or HTTP 80 as alternatives. Customers who use their own server solution of FastViewer can decide which ports to use for the commu- nication. Operating FastViewer exclu- sively over HTTPS provides enhanced security, since this makes it possible to verify the "authenticity" of the tunnel server(s) by the standard SSL encry- ption method. The communication server requires an IP address and an SSL certificate to operate using HTTPS. Viewers can check which protocol is connecting them to the tunnel server in the FastViewer connection. It is possible to allow only valid HTTPS connections on a proxy server or fire- wall, which means that a connection will only be established if valid SSL certificates are recorded on the tunnel server. The SSL certificate can be easily checked by calling it from Internet Explorer.
e.g.: https://tunnel200.fastviewer.com -> Right mouse button: Properties -> Certificates

Authentication

An SSL server certificate guarantees the encrypted transmission of data as well as the identity of the respective communication server. It serves to ensure that the participants can be certain about the trustworthiness of the communication server.



HTTPS

HTTPS is used for encrypting and authenticating communication between web servers and browsers on the World Wide Web.

Syntax

HTTPS is syntactically identical to the scheme for HTTP; the additional encryption of data is done via SSL/TLS: a protected identification and authen- tication of the communicating parties is initially performed using the SSL hand- shake protocol. A shared symmetrical session key is then exchanged using asymmetrical encryption or the Diffie- Hellman key exchange. This method is ultimately used to encrypt the user data.

EXTERNAL CERTIFICATES

FIDUCIA

When it comes to money, nothing but the best security standard is good enough. Our solution successfully completed security technology testing by Fiducia IT. The safety of the installation of a third-party-application was verified on the "agree Windows 7 Bank Workstation" in the Fiducia & GAD environment. As a provider, Fiducia IT supports file exchanges for more than 1.120 agricultural credit cooperative banks and private banks.

OPDV

The OPDV guidelines of the Sparkassen Finanzgruppe define the highest security standards for IT. The OPDV test highlight how correct, functional, economic and secure the software is. The tests specifically looked at safety against manipulation. The OPDV approval shows once again that FastViewer stands for the highest security!

BISG

The German Federal Association of IT Experts and Consultants (BISG) has awarded FastViewer its prestigious seal of quality and describes the product's performance as "very good." In particular, the testers praised the product's lean architecture, installation- free use, outstanding handling and excellent stability.

The testers also praised the fact that the user interface is transparently designed for users and thus avoids a steep learning curve. All in all, it is rated as an excellent product. FastViewer offers all options for connection types as well, including, for example, an HTTP client for tunnel connections (even behind firewalls), secure direct connections (encrypted) and direct connections.

Since Fast- Viewer never acts as a server, it also meets modern security guidelines without sacrificing balanced performance. The German Federal Association made the following concluding comments:

"In summary, FastViewer is a product that is impressive in its flexibility and user-friendliness".

TECHNICAL & ORGANIZATIONAL MEASURES

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

a) Entry control
Unauthorized access to data processing systems must be prevented.
(Examples: access control system, ID card readers, magnetic and chip cards, keys including key assignment, plant and door security (electric door openers, etc.), alarm systems, gatekeepers or video monitoring)

Entrance control is ensured by a documented and supervised handover of keys. The server room of FastViewer can only be accessed by persons authorized to enter the server room. The lock on the door to this room prevents unauthorized access by external or third parties.

b) Access control
Unauthorized system use has to be prevented.
(Examples: secure passwords, automatic locking mechanisms, two-factor authentication, encryption of data carriers, creation of a user master record per user)

Access to the premises of the data processing equipment is protected, and all equipment and IT systems are provided with constantly changing passwords.
All computer systems are set up by the IT staff in a manner that allows only authorized users the opportunity to work with them. Consequently, a personal login with a user ID and password is mandatory. The password must then be changed by the respective user with a password consisting of lowercase and uppercase letters as well as digits. The assignment of user IDs for working on IT systems generally occurs on a personal basis. Working under the credentials of another person is not permitted. The user is prohibited from passing on user IDs and passwords to third parties. The respective passwords are changed regularly every 30 days.
If a user does not change his or her password, the system will force the user to do so.

c) User control
No unauthorized reading, copying, modification or removal of data within systems.
(Examples: authorization concepts, need-based access rights, access logging and evaluation, modification and deletion)

Personal data can only be changed on the basis of the authorizations granted according to the "need to know" principle. For this a documented authorization concept is established. Employees cannot edit or copy personal data stored in the system or manipulate this data in any other unauthorized manner. Employees are divided into groups that have different access authorizations for the data records. This is guaranteed by a Windows server structure in conjunction with the "Active Directory".

d) Separation control
Separate processing of data collected for different purposes.
(Examples: multi-client capability / purpose limitation, sandboxing, separation of functions, separation of live / production / test)

Our system guarantees that data collected for different purposes can also be processed separately.

e) Pseudonymization (Art. 32 para. 1 lit. a GDPR, Art. 25 para. 1 GDPR)
The processing of personal data shall take place in such a way that the data can no longer be assigned to a specific person without the need for additional information, provided that such additional information is kept separate and subject to appropriate technical and organizational measures.

All backups (Veeam) are provided with 256-bit AES encryption.

TECHNICAL & ORGANIZATIONAL MEASURES

2. Integrity (Art. 32 para. 1 lit. b GDPR)

a) Transfer control
During electronic transmission or transport, no unauthorized reading, copying, alteration or removal may be possible.
(Examples: encryption, virtual private networks, electronic signatures, transport security)

Personal data from the IT system is protected against unauthorized copying to data media. Basically, with FastViewer, no data is played on data media and used outside the company. If an employee works in the field over a VPN connection, access is protected by a firewall and appropriate antivirus, spyware removal and antihacker software. Protection is provided from both the server and the user computers by installing the corresponding software.

b) Input control / memory control / data media control
Determine if and by whom personal information has been entered, altered or removed from data processing systems.
(Examples: logging, document management)

The input control is ensured by the internal system-side logging. It is possible to track which user has made what change and when, etc., at any time.

3. Availability and resilience / recoverability (Art. 32 para. 1 lit. b GDPR)

Protection against accidental or willful destruction or loss.
(Examples: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), disk mirroring, e.g. RAID, separate storage, firewalls, reporting channels and emergency plans; quick recoverability, Art. 32 para. 1 lit. c GDPR)

Scalable server systems based on Microsoft Hyper-V are used, which can be adapted to the load. The servers are backed up fully on a daily basis. All servers have mirrored hard drives in RAID systems and are equipped with redundant components.
The equipment used can be remotely serviced and administered at any time via the FastViewer software solution. The communication servers used for this purpose are located in highly secure data centers. For the connections themselves, one of the highest quality encryption methods is used to ensure an appropriate security standard (256 bit AES).

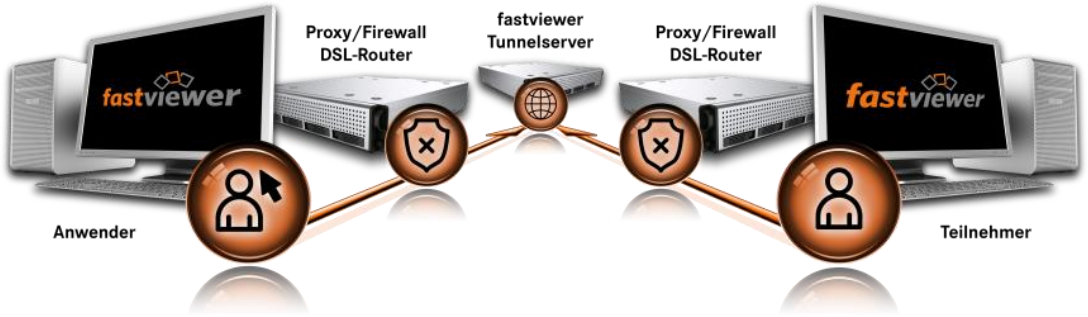
All critical systems are subject to permanent monitoring through the monitoring software of the manufacturer Paessler. If critical values regarding the availability or performance of the networks or used devices are reached, the supervising administrators are notified immediately by email/SMS. The targeted monitoring of system components and processes helps prevent system bottlenecks, congestion and failures. Due to the comprehensive functionality of the monitoring systems by Paessler, it is possible to monitor and document the overall status of the network as well as the individual devices 24 hours a day. The monitoring report is regularly evaluated by an authorized administrator.

4. Procedures for periodic review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR, Art. 25 para. 1 GDPR)

Order control
No order processing in the sense and meaninf of Art. 28 GDPR without corresponding controller instructions
(Examples: clear contract design, formalized order management, strict selection of service providers and subcontractors, follow-up-checks, etc.)

There are written contracts between the Principal and Agents.
The Principal issues directives to the Agent in writing. The Agent has sufficient in-house instructions on the basis of the commission and the related directives of the Principal.

Adequate measures to ensure data protection by any potential subagent can also be reviewed by the Principal. A data protection management system will be established, respecting the principles of the PDCA cycle and written deposition.



Note: Useage with own server solution

The HTTP protocol is used to query the available servers at module startup. If you use your own FastViewer server solution, this call can be made using HTTPS instead of HTTP and the port number can be freely selected. (e.g., HTTPS 321). When configuring HTTPS, FastViewer recommends using TLS 1.2 for maximum security.
Thus, it is possible to restrict the protocols used and thus the requirement of the ports to be opened and to guarantee their own security standards.

A description of the individual configuration steps can be found in the manual of the FastViewer server solution (chapter 6.5 Setup steps for the exclusive use of https), which is located in your personal portal under "Documents":
https://portal.FastViewer.com/