TeamViewer

Security Datasheet

TeamViewer Takes Your Data Protection Seriously

As a German company, we're dedicated to meeting the high requirements of German security standards. We have various measures to ensure the security of your data, workplace privacy, as well as fraud protection. While TeamViewer provides background security through encryption, code signing, two-factor authentication, and more, we also offer other helpful functions to maintain security during your everyday work.

TeamViewer Security

The TeamViewer ID
The TeamViewer ID is unique to your device, which is generated automatically and checked before each session.

The TeamViewer Password
TeamViewer automatically generates a new dynamic session password after each TeamViewer service restart. But there is also an optional setting which allows a password to be set dynamically after each session. This password is alphanumeric as standard, and consists of six characters, which means that there are more than 2.1 billion possible combinations.

Encryption
All interactions through TeamViewer, including file transfers, VPN, chat, etc., are protected by end-to-end encryption with a 4096-bit RSA public/private key.

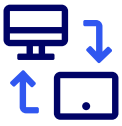
Bring Your Own Certificate*
The “Bring Your Own Certificate” (BYOC) feature of TeamViewer Tensor enables our users to use their own certificates to authenticate the devices involved in a TeamViewer connection.

The Highest Security Standards Worldwide
Our data centers and our Information Security Management System (ISMS) are ISO 27001 certified.

Conditional Access*
With Conditional Access, you can enforce remote access rules in order to prevent unauthorized activity and adjust the security guidelines.

Protection from Brute Force Attacks
With TeamViewer, the time between failed login attempts is increased exponentially and is reset only when the correct password is entered. Remote access devices or connection partners are also protected from other attacks.

Secure Remote Protocol (SRP)
TeamViewer uses the SRP protocol for authentication and password encryption. So the password is never sent over the internet, even encrypted, and is therefore optimally protected from outside access. Passwords also receive backend encryption.

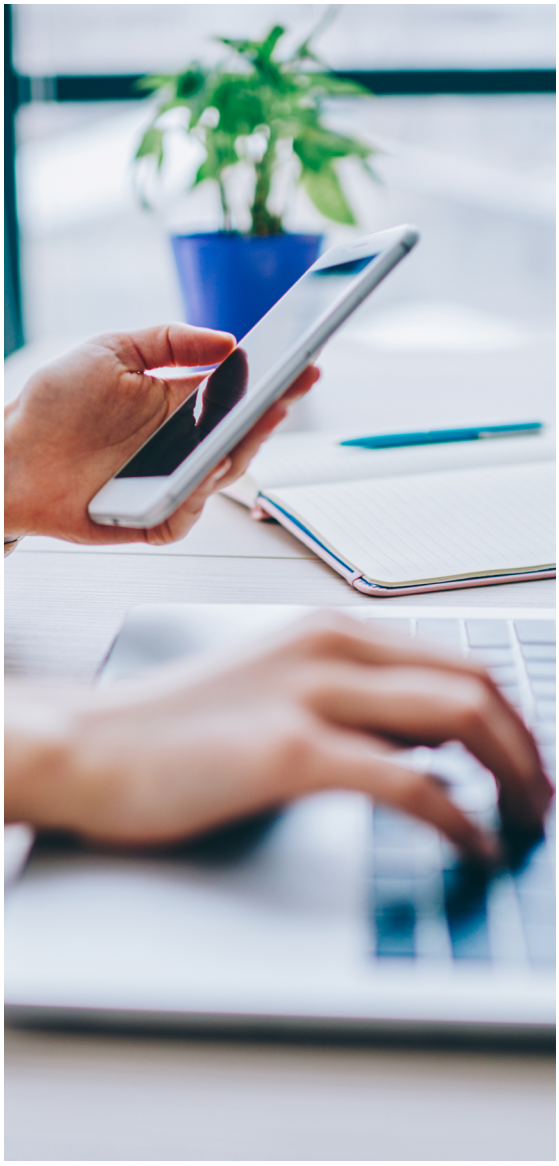


Two-Factor Authentication
In this case, login takes place using a new unique code, which is generated each time by an algorithm and supplied from a mobile device.

*Available with TeamViewer Tensor. Term and conditions apply.

HIPAA, HITECH, and SOC2 certified
TeamViewer received HIPAA, HITECH, and SOC2 certification from A-LIGN, a U.S. nationwide security and compliance provider. While HIPAA and HITECH are crucial for health care organizations to ensure the confidentiality and security of sensitive data and protected health information (PHI), SOC2 is an essential reporting framework for service provider organizations to establish a means to report on nonfinancial internal controls, so that their clients get a better understanding ofthe enforcement of the five Trusted Service Principles (TSP).

TeamViewer Sessions



Session Setup and Connection
When setting up a session, TeamViewer selects the optimal type of connection. In 70 percent of cases, after the handshake through our master server (even behind standard gateways, NAT routers, and firewalls), data connection is by UDP or TCP. The other connections are made through our highredundancy router network by TCP or HTTP tunnelling. So you don't have to open any ports in order to work with TeamViewer.

Encryption and Authentication
TeamViewer connections are made through fully secured data channels, which are set up by RSA public/private key exchange with 256-bit AES encryption. This technology is also applied in the same way for https/SSL and is completely secure according to the current state of the art. Since the private key never leaves the client computer, this technology ensures that no intermediate computers connected on the internet can decrypt the data stream, and this applies also to TeamViewer routers. As operator of the main data center, not even TeamViewer can read the encrypted data traffic.

Compliance and data protection

Trusted devices
Trusted Devices ensures that authentication is requested the first time a new device attempts to log in to an existing TeamViewer account.

Data Integrity
Data Integrity provides protection from cyber criminals: The system checks continuously for any unusual behavior on a user account and, if this is detected, generates an automatic password reset.

Allow list/block list
This function provides special protection if TeamViewer is installed on computers which are being maintained while unsupervised. The allow list is used to decide which clients are allowed access. The block list is used to decide which TeamViewer IDs and accounts are blocked.

ISO/IEC 27001
Our data centers and our Information Security Management System (ISMS) are certified to ISO/IEC 27001 standard. This represents the international standard for security management and controls.

ISO 9001:2015
TeamViewer is also ISO 9001:2015 certified for Quality Management Systems (QMS).

General data protection regulation (GDPR)
On May 25, 2018, the European General Data Protection Regulation (GDPR) came into effect, reflecting the importance of data protection in our increasingly digital world. TeamViewer is a global organization, and for us, it is important that the personal information of our customers and our own people is handled in accordance with GDPR. To learn more about TeamViewer's commitment to data privacy and the GDPR, visit our Knowledge Base.

About TeamViewer

TeamViewer is a leading global technology company that provides a connectivity platform to remotely access, control, manage, monitor, and repair devices of any kind – from laptops and mobile phones to industrial machines and robots. Although TeamViewer is free of charge for private use, it has around 630,000 subscribers and enables companies of all sizes and from all industries to digitalize their business-critical processes through seamless connectivity. Against the backdrop of global megatrends like device proliferation, automation and new work, TeamViewer proactively shapes digital transformation and continuously innovates in the fields of Augmented Reality, Internet of Things and Artificial Intelligence.

Since the company's foundation in 2005, TeamViewer's software has been installed on more than 2.5 billion devices around the world. The company is headquartered in Goppingen, Germany, and employs more than 1,400 people globally.

Stay Connected

www.teamviewer.com