TeamViewer

TeamViewer encara com seriedade a **proteção** dos seus **dados**.

Como uma empresa alemã, nos dedicamos a atingir os exigidos altos padrões de segurança da Alemanha. Tomamos várias medidas para garantir a segurança dos seus dados, a privacidade no local de trabalho e a proteção contra fraudes. Enquanto a TeamViewer fornece segurança em seu background por meio de criptografia, verificação em duas etapas, e mais, também oferecemos outras funcionalidades úteis para manter a sua segurança durante o trabalho diário.

Segurança TeamViewer

A TeamViewer ID
TeamViewer ID é um número de identificação exclusivo para o seu dispositivo, que é gerado automaticamente e verificado antes de cada sessão.

Os mais altos padrões de segurança
Nosso centro de dados principal cumpre os padrões de segurança industrial ISO 27001.

Proteção contra ataques direcionados
Com o TeamViewer, o tempo entre as tentativas de login que falharam aumentou exponencialmente e apenas é restabelecido quando a senha correta for inserida. Dispositivos de acesso remoto ou parceiros de conexão também são protegidos contra outros ataques.

Senha TeamViewer
TeamViewer gera automaticamente uma nova senha de sessão dinâmica após a reinicialização de cada serviço do TeamViewer. Mas há também uma configuração opcional, que permite que uma senha seja definida dinamicamente após cada sessão. Como padrão, essa senha é alfanumérica e consiste em seis caracteres, o que significa que existem mais de 2,1 bilhões de combinações possíveis.

Secure Remote Protocol (SRP)
O TeamViewer usa o protocolo SRP para autenticação e criptografia de senha. A senha nunca é enviada pela Internet, nem mesmo criptografada e, portanto, é idealmente protegida contra acesso externo. As senhas também recebem criptografia de back-end.

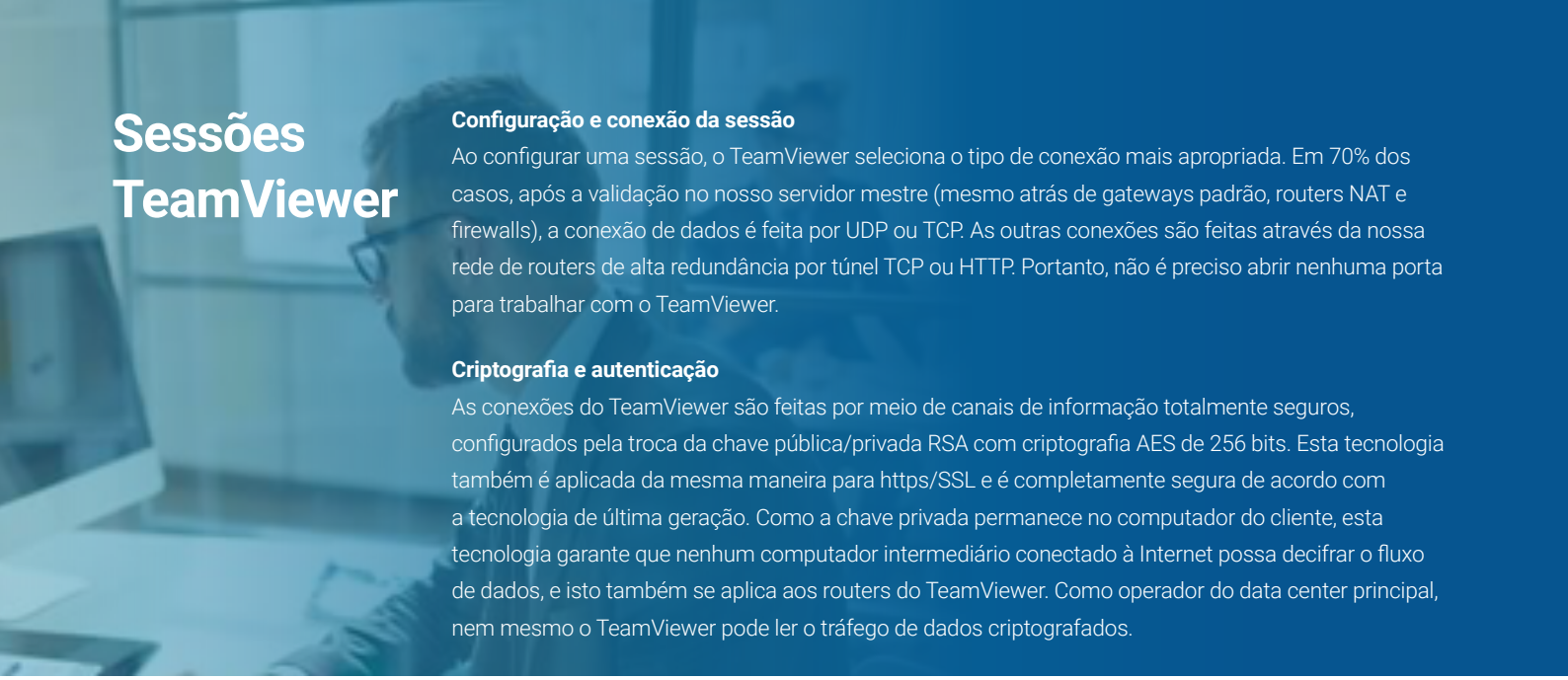
Criptografia
Todas as interações através do TeamViewer, incluindo transferências de arquivos, VPN, chat, etc, são protegidas por criptografia de ponta-a-ponta com uma chave pública/privada RSA de 4096 bits.

Acesso condicional*
Com o Acesso Condicional, é possível aplicar regras de acesso remoto para impedir atividades não autorizadas e ajustar as diretrizes de segurança.

Verificação em duas etapas
Neste caso, o login ocorre usando um novo código único, que é gerado a cada vez por um algoritmo e fornecido por um dispositivo móvel.

**Disponível com o TeamViewer Tensor. Aplicam-se termos e condições.*

AICPA SOC · A-LIGN HIPAA · südcert ISO 9001 · digicert · ISO ISO/IEC 27001



Sessões TeamViewer

Configuração e conexão da sessão

Ao configurar uma sessão, o TeamViewer seleciona o tipo de conexão mais apropriada. Em 70% dos casos, após a validação no nosso servidor mestre (mesmo atrás de gateways padrão, routers NAT e firewalls), a conexão de dados é feita por UDP ou TCP. As outras conexões são feitas através da nossa rede de routers de alta redundância por túnel TCP ou HTTP. Portanto, não é preciso abrir nenhuma porta para trabalhar com o TeamViewer.

Criptografia e autenticação

As conexões do TeamViewer são feitas por meio de canais de informação totalmente seguros, configurados pela troca da chave pública/privada RSA com criptografia AES de 256 bits. Esta tecnologia também é aplicada da mesma maneira para https/SSL e é completamente segura de acordo com a tecnologia de última geração. Como a chave privada permanece no computador do cliente, esta tecnologia garante que nenhum computador intermediário conectado à Internet possa decifrar o fluxo de dados, e isto também se aplica aos routers do TeamViewer. Como operador do data center principal, nem mesmo o TeamViewer pode ler o tráfego de dados criptografados.

Conformidade & proteção de dados

Dispositivos confiáveis

Dispositivos Confiáveis garantem que a autenticação seja solicitada na primeira vez em que um novo dispositivo tentar efetuar login numa conta existente do TeamViewer.

Integridade de dados

A Integridade de Dados fornece proteção contra criminosos cibernéticos: o sistema verifica continuamente se existe algum comportamento incomum em uma conta de usuário e, se isso for detectado, gera uma redefinição automática da senha.

Permitidos/bloqueados

Esta função fornece proteção especial se o TeamViewer estiver instalado em computadores que estão passando por manutenção enquanto não são supervisionados. A lista de permitidos é usada para decidir quais clientes têm permissão de acesso. A lista de bloqueados é usada para decidir quais IDs e contas do TeamViewer estão bloqueadas.

ISO/IEC 27001

O nosso principal data center está certificado conforme a norma ISO/IEC 27001. Esta norma representa o padrão internacional para gestão e controle de segurança.

ISO 9001:2015

O TeamViewer também possui a certificação ISO 9001:2015 para Sistemas de Gestão de Qualidade (QMS).

General Data Protection Regulation (GDPR)

Em 25 de maio de 2018, a lei europeia General Data Protection Regulation (Regulação Geral sobre a Proteção de Dados) (GDPR) entrou em vigor, refletindo a importância da proteção de dados no nosso mundo cada vez mais digital. A TeamViewer é uma organização internacional e, para nós, é importante que as informações pessoais dos nossos clientes e dos nossos colaboradores sejam tratadas de acordo com o GDPR. Para saber mais sobre o compromisso de privacidade de dados da TeamViewer e a preparação do GDPR, visite a nossa base de conhecimento.

Certificações HIPAA, HITECH e SOC2

A TeamViewer recebeu as certificações HIPAA, HITECH e SOC2 da A-LIGN, um provedor americano de segurança e conformidade. Enquanto o HIPAA e o HITECH são cruciais para as organizações de saúde garantirem a confidencialidade e a segurança de dados sensíveis e a proteção do sigilo médico (PHI), o SOC2 é uma estrutura de relatório essencial para as organizações de provisão de serviços estabelecerem um meio para relatar controles internos não financeiros, para que seus clientes entendam melhor a aplicação dos cinco Princípios de Serviços Confiáveis (Trusted Service Principles - TSP).

TeamViewer

TeamViewer US
5741 Rio Vista Dr
Clearwater, FL 33760
EUA
Telefone: 0-800-761-1931

Conecte-se conosco em nossas redes sociais!