

How to Establish an Enterprise Grade Security Posture for Remote Connectivity

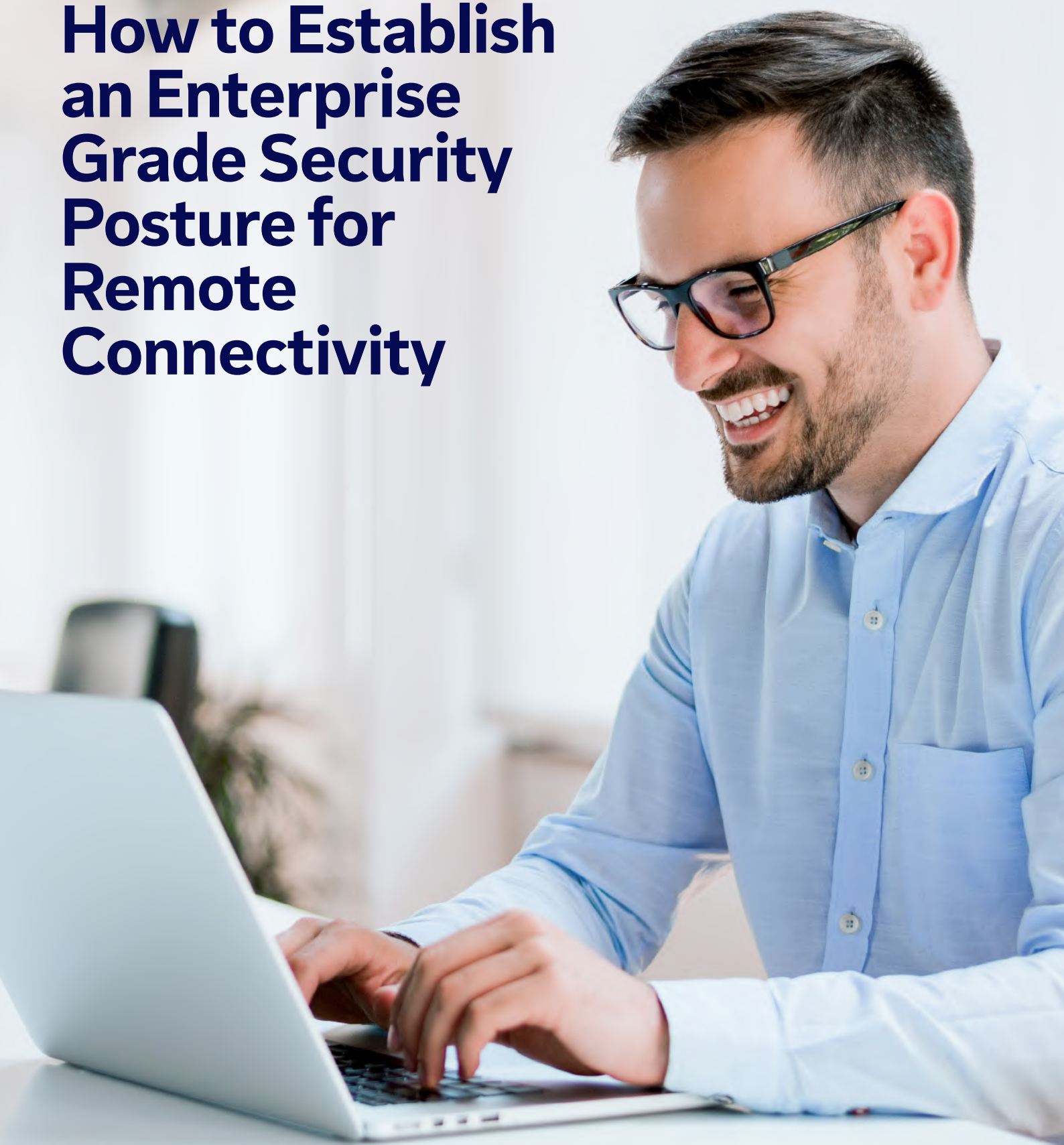


Table of Content



A Framework for Secure Remote Connectivity	04
Why Secure Enterprise-wide Remote Connectivity matters	06
Layer 1: The Commitments for Security Posture	06
Layer 2: Setting Expectations	07
Layer 3: Defining the Actors	08
Built-in Security Features	11
Security Standards and Certifications	12
Continuous Security Improvements	14
The Strategies: Interweaving the Risks and Configuration Around Security	15
Layer 4: Understanding the Security Risks in Enterprise Applications	16
Layer 5: The Key Security Configuration Objects	18
The Processes	21
Layer 6: The Golden Security Rules	21
Additional Resources	27

Establishing Enterprise-wide Security Posture

Today, enterprises rely heavily on remote connectivity to manage a majority of their IT operations. In addition, the rise of distributed workforce and adoption of work-from-home policies have led to a significant dependence on remote access and control capabilities. As a consequence, the scope of security has increased manifold.

In the past, security requirements were discrete since IT infrastructure was managed from close proximity within company firewalls and accessed by a

handful of operators and users from a single location. However, with the move towards digital transformation providing borderless access to employees, partners, and vendors, security can no longer be treated as an afterthought.

The work environment in these connected enterprises is constantly evolving. They are a complex ecosystem comprising of humans, technology stacks and workflows. Most of the ecosystem is managed remotely through various IT systems and network equipment.



Today's work environment is constantly evolving and changing

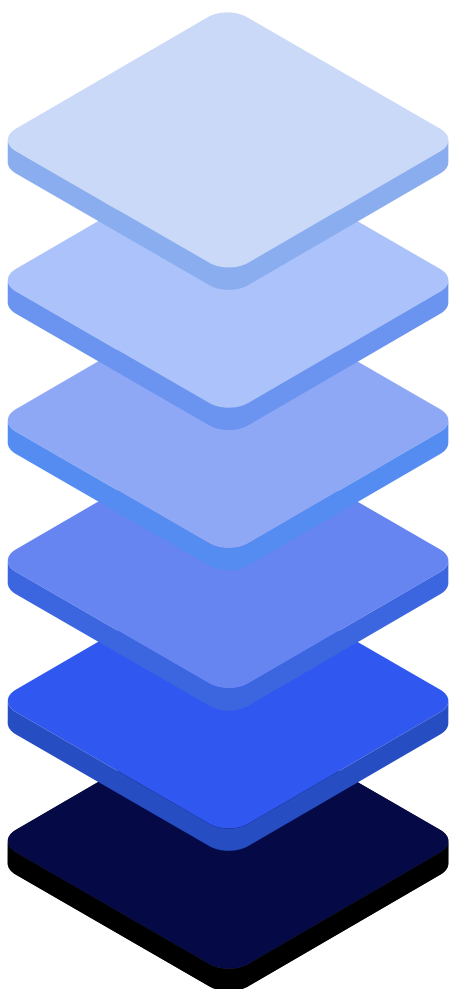
As organizations look to take advantage of remote connectivity platforms to manage these complex infrastructures, they often encounter security issues due to misconfiguration, and other forms of human errors.

Hence building a resilient security posture that can minimize network and cyber security breaches is of critical importance. Organizations in the initial stages of deploying remote connectivity and remote infrastructure management platform need to start with an approach that helps them maintain this security posture.



A Framework for Secure Remote Connectivity

At TeamViewer, we understand the importance of driving business success through remote connectivity and establishing a framework for robust security posture. This framework is split into six layers:



6

Rules

The golden rules for ensuring a secure remote connectivity experience

5

Configurations

Configuration parameters that involve security in general

4

Risks

Potential risks that need to be safeguarded against

3

Actors

The actors involved in or affected by security breaches

2

Expectations

Setting expectations for a more secure remote connectivity experience

1

Commitments

Establishing an organization-wide security posture

Security
framework at
TeamViewer



Establishing a robust security posture starts with a firm **commitment**



Why **Secure** Enterprise-wide Remote Connectivity matters

IT applications have evolved from the traditional mainframe/desktop-based, standalone systems. These systems had a natural barrier to security threats due to a limited number of attack vectors that were prevalent. However, the attack surface has expanded significantly with workloads moving to the cloud. This has happened primarily to support a globally distributed workforce and an expectation of having an always-available, enterprise network that enables a business to stay competitive and agile in today's environment.

With a constantly growing number of applications, a heterogeneous landscape of devices and employees working remotely from different locations, security is an increasing concern. It is necessary to address these concerns with stakeholders to lay the groundwork for security posture.

Layer 1: The Commitments for Security Posture

Establishing a robust security posture starts with a firm commitment. This commitment must be driven as a top-down corporate responsibility with initiatives such as:



Building awareness among employees and staff through regular updates on security news and trends.



Continuously training and educating the external partners and vendors to build and maintain a secure ecosystem.



Establishing thought leadership in the cyber and network security community by contributing to regular briefings, community forums, and working together with government bodies.

Did You Know

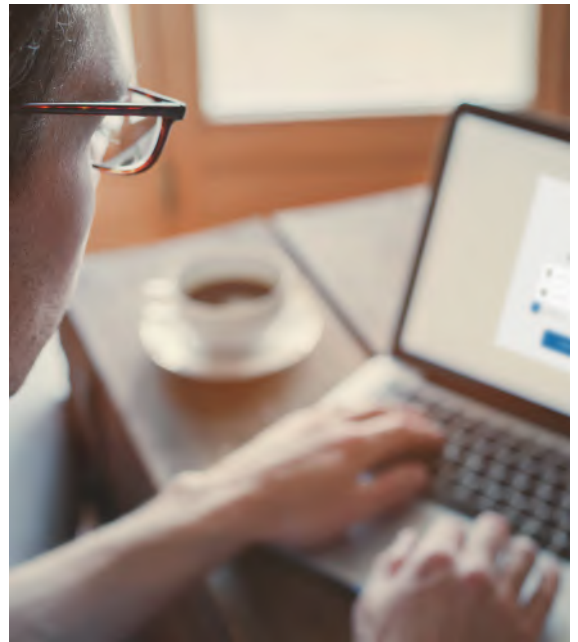
- TeamViewer is an audited member of the Forum of Incident Response and Security Teams (FIRST), a leading association for incident responders.
- TeamViewer cooperates with the leading crowd sourced security platform YesWeHack to engage with a large community of security researchers.
- TeamViewer has been rated as Top 1% in the tech industry by BitSight Security Rating, an independent 3rd party company for measuring cybersecurity risk and security management effectiveness.

Layer 2: Setting Expectations

Before arriving at an ideal security posture, it is crucial to set the right expectations in context to security.

Different people perceive security in different ways. However, it is not hard to imagine that most public disclosures of corporate IT security breaches happen in the form of privacy or access issues.

Whether it is an incident of stealing credit card data or manipulating a computer or device to send malicious packets. All security measures fall under one of the two categories, privacy and access control. These measures form the bedrock for any security posture.



- People, Systems, Data
- Access Control
- Privacy

Fundamental
Security Measures

Organizations strive to encourage a favourable work-life balance. Individuals working in such organizations want easy and secure access to digital workspaces.

In organizations, privacy safeguards employee data, sensitive business data, and classified information related to business transactions and trade secrets. Similarly, access pertains to only authorized personnel for the configuration and management of equipment, premises, and systems.

Layer 3: Defining the Actors

Setting security expectations is only possible by defining the actors that are involved. For example, a privacy breach involving credit card details affects all the persons whose data is exposed. In this case, the credit card holder is an actor. From an organizational standpoint, these actors are directly or indirectly involved in a security-related incident, either as a beneficiary or a victim.



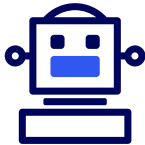
Human

A user that is assigned to various broader categories such as an employee, partner, or vendor interacting with other humans and machines. They are further categorized into more granular groups and roles based on departments and corporate functions.



Machine

Represents the computers, servers, networking devices, and other hardware/software assets that are used by various stakeholders with an organization to conduct their daily business, operational, and service workflows.



Bot

A programmable hardware/software with minimal intelligence to mimic a subset of behavior representing either a human user or a machine. It serves as a proxy for humans to automate tasks.



The foundation for a reliable remote connectivity security posture starts with the internal assessment of these three layers. This assessment serves as the clear articulation of security expectations with respect to each actor.



70 % of organizations

cannot secure data across multiple cloud and on-premises environments.

92 % of organizations

cannot securely enable and extend new cloud-native capabilities to internal and external partners.

33 % increase

in the number of incidents caused by vulnerability exploitations from 2020 to 2021.

Asserting the Underlying Assumptions for Security Posture

There are many technologies that help manage enterprise-wide IT initiatives which span across many departments and functions. Similarly, every technology that helps save time, effort and boosts productivity can also be abused or hacked by third party threat actors. Email was and still is one of the most widely used technologies for hacking into businesses. Similar to email, there are countless ways hackers can and will continue their efforts to exploit vulnerabilities and disrupt daily business operations. These are done usually to harm, extort money and also cause loss of reputation in the public domain.



Remote connectivity is no exception. However, businesses need to understand that adopting remote connectivity can far outweigh the risks. Benefits such as reducing technician fatigue, improving employee productivity and speed up processes in the office. Businesses need to choose that the platforms, solutions that are secure from the get go.

Organizations are increasingly realizing how remote connectivity enables them to easily manage interactions and communication across personnel, systems, processes and workflows.

Built-in Security Features

Built-in security features ensure a secure remote connectivity session. This guarantee extends to privacy and access. Every session is encrypted and therefore ensures that only the intended actors can share and access content.

Additionally, any remote connection involving two or more actors must have a mechanism. This helps authenticate the connection with safeguards in place that control the permissions to access devices of employees that are working remotely or on the move.

The built-in security features also include specific provisions for managing sensitive information. These include various cryptographic and ciphering techniques

for generating random, unpredictable security keys and protocols which serve the exchange of sensitive security information (e.g. multiple forms of key exchange protocols).

The built-in security features also include specific provisions for managing sensitive information.

Did You Know

TeamViewer supports built-in and additional security features such as:

- Password randomization after each session
- Device authentication (Trusted devices)
- One-time password (OTP)
- Multi-factor authentication (MFA) for connection
- Smart card re-direct
- Conditional access
- Single Sign-On (SSO)

Security Standards and Certifications

Security standards and certifications lay the groundwork for security compliance and expectations of any platform.

In the case of remote connectivity platforms, here are some of the critical standards and certifications:



Encryption Standards

define a mechanism to encrypt information. AES (Advanced Encryption Standard) and RSA (Rivest, Samir, Adleman) are the two popular standards for encrypting data and information exchanged in a remote connectivity session.



Security Frameworks

define policies on an organizational level involving legal, physical and technical controls to regulate all the information systems and access to the data generated by them. ISO 27001 and GDPR are the most well-known examples of security and privacy frameworks.



Code Signing

is a method of digital attestation where a file or a software executable is prevented from alteration or corruption, thereby asserting its originality and integrity.

Security is an ever-evolving
challenge



Did You Know

TeamViewer is backed by:

- End-to-end 4096 bit RSA key encryption and 256 bit AES encrypted session
- GDPR, HIPAA / HITECH, TISAX, SOC 2, SOC 3, ISO 27000 compliances
- Best-in-class security posture rating by BitSight - an independent 3rd party cybersecurity ratings company
- IAPP gold membership
- Digital Risk Protection

Continuous Security Improvements

Security is an ever-evolving challenge. Historically, all significant technological innovations that enabled businesses to streamline, accelerate their workflows and processes were also used against them through malicious activities leveraging technologies such as email, instant messaging and so on. Newer innovations such as AI, and emerging technologies are also being leveraged in the same way to hack systems or steal data.

As a result, every remote connectivity platform must be guarded against emerging security threats and updated regularly. However, predicting these threats is not easy. Therefore, keeping oneself informed about the latest happenings in the cyber security and network security space is essential.



Vulnerability Disclosures

Being transparent about possible security vulnerabilities is the best way to impede the pace of exploitation of a security hole. This way, enterprises using a specific platform are well informed, whether for remote connectivity or otherwise.



Bug Bounty Program

Bug bounty is another way in which companies reward individuals through recognition and compensation for reporting bugs relating to vulnerabilities.



Security Thought Leadership

Companies must engage in technology thought leadership engagements to lend their voice to the current state-of-the-art on security. There are several channels through which it is possible. Various media outlets, communities, and collectives interested in the security space and allied fields are the best source of collaboration for driving such initiatives.

Did You Know

TeamViewer is an authorized CVE Numbering Authority (CNA) joining the ranks of just nine German CNAs such as Siemens, SAP, and Bosch as well as 178 vendors globally. TeamViewer underscores its industry-leading cybersecurity focus and posture in addition to embracing responsible disclosure in order to make our products and services better.

As part of that, we offer clear guidance for ethical hackers by providing a VDP (Vulnerability Disclosure Policy) to challenge ourselves to discover bugs and security exploits.

Learn more:

vdp.teamviewer.com/p/Send-a-report

Strengthening Your Security Posture

Having established a baseline for an enterprise-wide security posture, it's important to also pay attention to the overlaying elements of security enablement. These are related to customizable security configurations at the application level.

The Strategies: Interweaving the Risks and Configuration Around Security

Configurations provide additional layers of safeguards to secure any communication between two or more actors. Scenarios

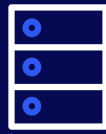
such as a support agent connecting to a remote worker, or a technician logging in to a remote device to provide support or fix issues remotely. It is important to understand the potential security risks that these configurations can have in an enterprise setting in the event of a misconfiguration.

Layer 4: Understanding the Security Risks in Enterprise Applications

Based on current trends in cyber and network security, there are four types of security risks for enterprise applications:



Intrusive Risks



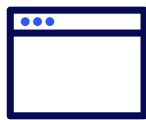
Incidental Risks



Inherent Risks



Interdependent Risks



Inherent Security Risks

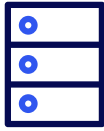
The inherent security risks can sometimes emerge owing to lack of adherence to fundamental security policies in an organization. Some common examples are the lack of encryption or authentication methods resulting in privacy risks during data transfer or providing a secure support experience to a remote worker.



Interdependent Security Risks

Interdependent security risks result from exposing sensitive information that undermines the very notion of security. For example, if a user's login credentials to their workstations are exposed, then the workstations are vulnerable to security breaches.

The login credentials are part of a sensitive set of information that is only shared between certain actors, in this case, the user and the workstation. Passwords, certificates and cryptographic keys, are all different forms of such sensitive information that must be exchanged between two or more actors to establish a secured connection between them. This interdependency is a fundamental tenet for enabling security.



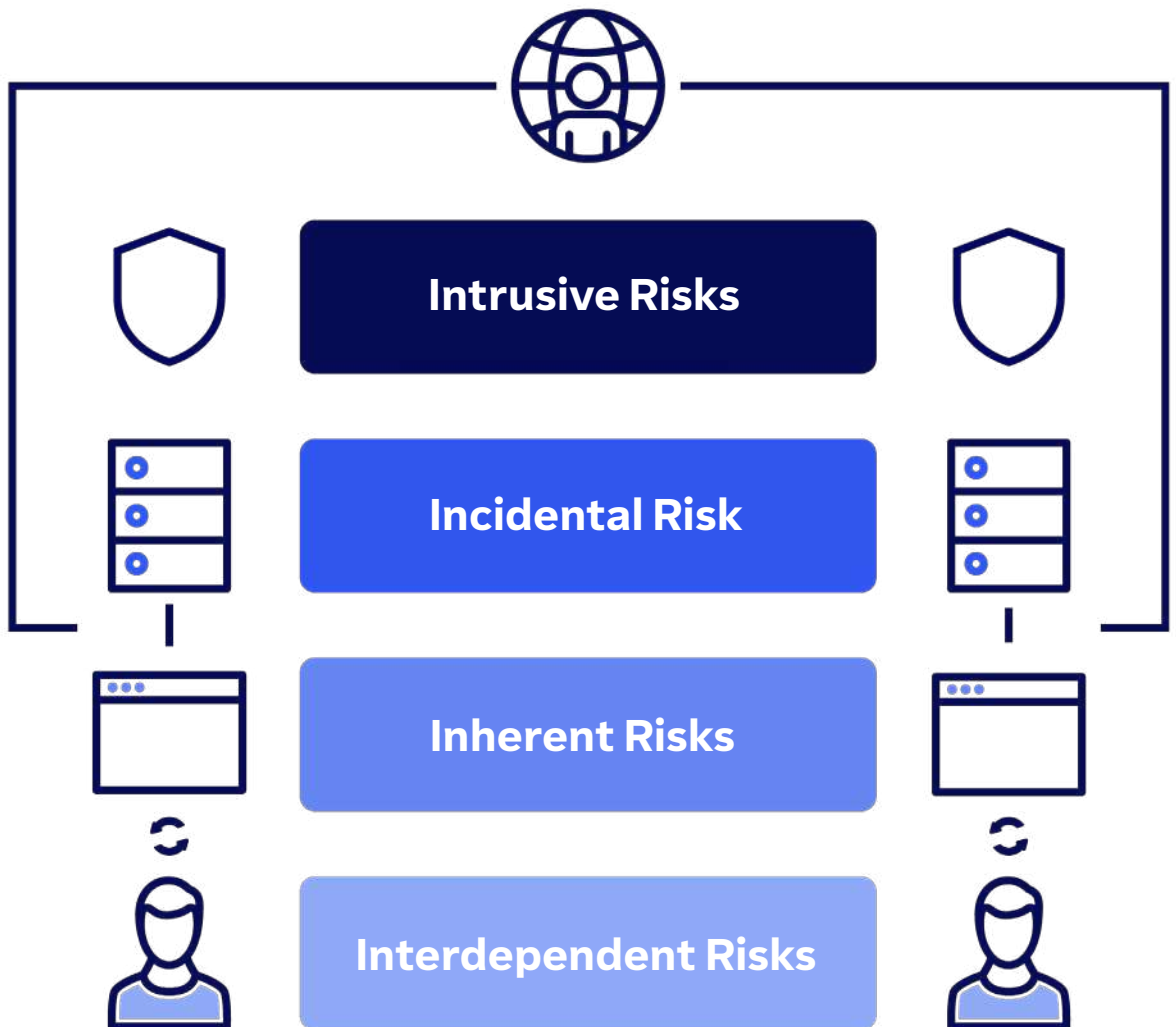
Incidental Security Risks

Incidental security risks are related to intermediaries involved in a secured communication. For example, a firewall that filters traffic to allow only certain types of packets to a specific application. A misconfigured firewall allows unauthorized traffic, resulting in a security lapse. Similarly, there are different intermediaries, such as VPN gateways, authentication servers, and storage vaults, that are involved in managing secured communication between actors. If any of these intermediaries are compromised, security can be jeopardized.



Intrusive Security Risks

Security is also a function of access provisions. The more the number of access mechanisms provided, the more the chances of intrusion through multiple attack surfaces. In some ways, this risk is very similar to interdependent or incidental security risks, wherein a password is exposed, or a device is misconfigured, resulting in the emergence of an attack surface.



The Four Security Risks in Enterprise Networks

Layer 5: The Key Security Configuration Objects

The goal of strengthening the security posture is to mitigate these four risks.

There are a few important security parameters to achieve that. They need to be configured as part of the overlaying security enablement within the remote connectivity platform.

Identity

It establishes a unique signature that can unambiguously pinpoint an actor.

In many cases of secured communication, the actual identity is always kept under the wraps, while an associated temporary identity is used.

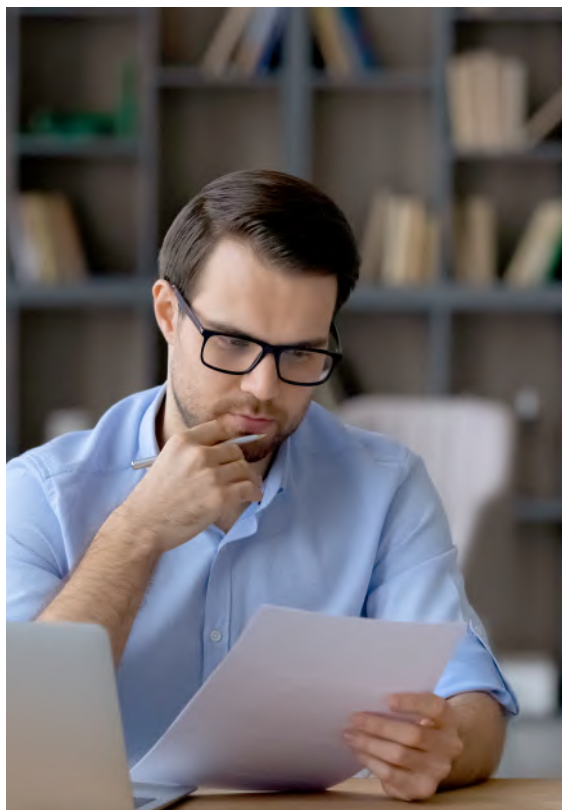
TeamViewer offers flexible options to create user identities based on Active Directory or via TeamViewer Company profile.

Credential

This is a way to verify the connection before it is established between two actors.

This can be used for authenticating each other, or for codifying the information exchanged between them, in order to obfuscate the message.

Apart from password and 2FA, TeamViewer also supports single sign-on (SSO) for users and unattended access to remote devices while ensuring full protection against intrusive security risks.



Policy

It defines a set of core principles for vetting an access request based on certain parameters of the request. For example, a firewall policy relies on the IP address and port number of a request packet to frame policies for accepting or rejecting the packet. Similar policies are devised for access management to machines and systems, based on who is accessing them, from where, and when.

Apart from the general access control policies based on users, and groups, TeamViewer also supports flexible policy options to configure conditional access based on specific time slots and host profiles to counter many forms of interdependent security risks.

Connectivity

It encompasses a virtual connectivity context that establishes a secured end-to-end session. For example, all websites using HTTPS use an end-to-end SSL layer to secure all HTTP traffic between the web server and the browser. Similarly, a VPN connection uses an IP over IP encapsulation to define the connectivity context.

TeamViewer is a network agnostic, end-to-end secure system that offers a more reliant connection than VPN for remote access use cases. It ensures the same levels of inherent security mitigation as a VPN network.

Deployment

It governs the deployment related parameters that are relevant for ensuring continued security protection for applications.

Mechanisms for key exchange, software updates, patch management and monitoring for suspicious events fall under the purview of deployment.



TeamViewer is a network agnostic, end-to-end secure system that offers a more reliant connectivity than VPN for remote access use cases.

Supercharging your Security Posture





The overlay security configuration offers many options to tackle the security risks. However, it may seem a daunting task to arrive at the ideal security setting. Security enforcement should not compromise user experience and cause difficulties or friction in a business' day-to-day operations.

The Processes

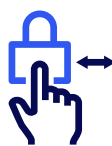
Irrespective of the many complex combinations of configuration versus risk possibilities, there are a few important rules to establish security awareness processes.

Layer 6: The Golden Security Rules

These rules provide guidance on how to arrive at the best possible security posture supporting any enterprise remote connectivity. It is recommended that these rules be incorporated into any system immediately after the installation and setting up of user accounts.



Multi-Factor Authentication



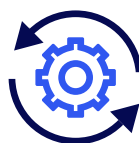
Ease of Access



Allow List



Strong Password



Updates



Backup

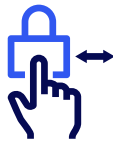


Multi-Factor Authentication

Multi-factor authentication (MFA) offers additional authentication layers to counter intrusive security breaches that result from the exposure of credentials. A single-factor authentication relies on pre-existing credentials of a user. If these credentials are compromised, an immediate recovery is not possible. A second factor brings in an additional temporary credential, that is generated ad hoc. It is shared on a separate communication channel, like email, SMS or phone that enable the actor to perform additional steps as a safeguard.

Two-factor authentication (2FA) is the most recommended setting for MFA. However, based on the criticality, additional factors must be configured to activate temporary credentials such as temporary passwords, codes, or secret questions.

TeamViewer supports one-time password (OTP), as well as smart card redirect mechanism as a secured way of authentication for companies that operate in highly regulated sectors such as banking and financial services.



Ease of Access

Security is a burden, especially in situations where additional processes are necessary to access the same system repeatedly. This is a case of a human actor interacting with a machine on an everyday basis.

For example, an operator uses a device to perform daily routines such as accessing that device after it automatically locked due to company policies.

Easy access provides an intelligent mechanism to pair actors in such a way that they can interact without suffering from complicated security processes. For performing routine tasks, this approach offers a few advantages, such as unattended access, and automation.

TeamViewer has various built-in mechanisms for easy access, such as SSO for users, and unattended access for trusted devices.



Allow List

An allow list defines the policies for allowing only certain actors to access a system. This is part of the access policies for the system. It is recommended to have a concise allow list with specific rules for actors, instead of wild card rules that allow everyone.

TeamViewer provisions a separate allow list and blocklist to maintain accounts and profiles that can or cannot connect to a computer, including support for wildcard entries, such as the entire company profile.



Strong Password

Passwords are the most widely used form of credentials for any secured communication. Therefore, it is imperative to cultivate a culture of choosing strong passwords within the organization.

Some of the key attributes of a strong password are:

- Unique passwords without having any dictionary word, names, or publicly identified information such as birth date, or information that can be easily obtained or assumed through social engineering hacks
- Long passwords, with a combination of upper case, lower case, numbers and special characters.
- At least three words, randomized to avoid common sequences of alphabets, numbers, or adjacent keyword combinations.

It is recommended that passwords be changed at regular intervals. Additionally, most systems also offer a password policy setup to enforce certain rules for generating strong passwords.

- TeamViewer supports password randomization after each session. Additionally, it is possible to recover the account using a zero-knowledge account recovery method.



Updates

Software updates are applicable for upgrading third-party applications and operating systems. Out of date versions are a prime target for hackers and pose a security weakness for organizations.

Patch management at scale requires automated software update procedures to avoid human errors and ensures that the systems are always up to date.

TeamViewer enables up-to-date information on all the deployed hardware and software and has the ability to automatically apply patches to fix outdated or vulnerable software.



Backup

Backups are applications for creating a copy of information and saving it to another device or cloud storage. Like updates, backups should also be automated to ensure that the most recent version of the information is preserved.

TeamViewer offers a single-window view to back-up and restore data for every device, with highest security standards of cloud data storage, providing a complete solution for disaster recovery scenarios.

TeamViewer: A Security First, Connectivity Platform for **Remote IT Management**

TeamViewer is a security first, remote connectivity platform that enables companies on a growth path and enterprises operating at scale the ability to provide remote access, support and control to their stakeholders. Employees, partners, customers operating across the value chain, in different business units, geographic locations and time zones can now be easily supported. This increases productivity and agility in a secure manner.

TeamViewer uses 4096-bit RSA key encryption, 256-bit AES session encryption, in addition to ISO/IEC 27001 certification standards for information security management that ensures inherent security risks are minimized at the network level. At an application level, TeamViewer supports a host of modular security alternatives for access management promoting ease of access through

approaches such as single sign-on (SSO) that ensures maximum protection against all interdependent security risks.

Moreover, TeamViewer provides a host of add-on security features to manage access control. These features also augment the protection of critical network resources. For instance, conditional access rules involving device identifiers, time slots and expiry dates, act as additional security layers for access control. Additionally, security provisions based on MFA, and biometric authentication can be enabled. All these choices are designed to offset any possibilities for infused security risks making remote support sessions secure at scale.

Compliance

“Bühler has been certified according to ISO 27001 in 2020. Particularly in the area of security, we were able to take an important step towards this certification with TeamViewer Tensor.”

— **Roland Isler**, Senior System Administrator at Bühler

Remote connectivity is an important component for customers that wish to provide their employees and various stakeholders with a secure and agile digital ecosystem.

Our customers trust in TeamViewer solutions to manage and protect their employees in terms of accessing applications and data.

That trust requires us to:

- Ensure our service meets the requirements of the most recognized certifications and regulations
- Help our customers meet security certifications and regulations from their industries

TeamViewer Service Certifications

TeamViewer complies with a range of certifications. As the compliance and regulatory environment is always changing, a current list can be found at:

www.teamviewer.com/en/trust-center/industry-leading-security/

Meeting your compliance requirements

TeamViewer is certified and in accordance with a majority of the international compliance requirements that are in effect.



SOC2

Service Organization Controls 2 (SOC2) is a reporting framework for service organizations to report on non-financial internal controls for the five Trusted Service Principles (TSP). These principles include system security, availability, processing integrity, confidentiality, and privacy.



HIPAA/HITECH

TeamViewer provides remote access, remote support, and online collaboration capabilities with the level of security and privacy necessary for organizations to remain HIPAA compliant.



TeamViewer is a global organization that values the personal information of customers and its employees and works in accordance with GDPR. To learn more about TeamViewer's data privacy commitment and GDPR, visit the TeamViewer and GDPR page in our Knowledge Base.



All of the data centers that TeamViewer uses have achieved ISO/IEC 27001 certification, which is the international standard for information security management systems and security controls.

The data centers have implemented state-of-the-art security controls, which means that personal access control, video camera surveillance, motion detectors, 24x7 monitoring, and on-site security personnel ensure access to the data center is only granted to authorized personnel and guarantee the best possible security for hardware and data. There is also a thorough identification check at the single point-of-entry to the data center.



ISO 9001:2015 is the globally recognized standard that specifies requirements for quality management systems (QMS). Organizations use the standard to demonstrate their ability to consistently provide products and services that meet customer and regulatory requirements. With the ISO 9001:2015 certification, TeamViewer has demonstrated dedication to total quality management, customer focus, and a continuous improvement of processes to work more efficiently and enhance the quality of products and services offered.



As an additional security feature, all of our software is signed via DigiCert Code Signing. In this manner, the publisher of the software is always readily identifiable. If the software has been changed afterwards, the digital signature is automatically invalidated.



TeamViewer has been awarded the TISAX label, which is designed to streamline high-quality IT security assessments in the automotive industry based on ISO 27001.



Additional Resources

Security Documentation

Security handbook:

community.teamviewer.com/English/kb/articles/108686-welcome-and-introduction

Six golden security rules

community.teamviewer.com/English/kb/articles/108694-six-golden-security-rules

Multi-Factor Authentication

Activating two-factor authentication

community.teamviewer.com/English/kb/articles/66-activate-two-factor-authentication

Access Management

Conditional access and how administrators can control incoming and outgoing connections

community.teamviewer.com/English/kb/articles/57261-get-started-conditional-access

In addition to your password protect your accounts with a physical security key

community.teamviewer.com/English/kb/articles/109554-security-key-redirection

Single Sign-On (SSO)

Reduce time and effort with SSO

community.teamviewer.com/English/kb/articles/30784-single-sign-on-sso

Compliance & Audits

Compliance and international standards followed at TeamViewer

community.teamviewer.com/English/kb/articles/108692-compliance-international-standards

Auditability:

Protect your business and also keep track of support experiences happening within your company

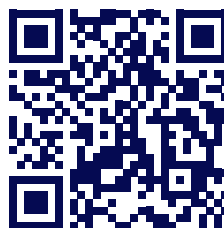
community.teamviewer.com/English/kb/articles/54970-auditability-event-log

TeamViewer Community and Knowledge Hub

English (EN)	community.teamviewer.com/English
German (DE)	community.teamviewer.com/German
Japanese (JP)	community.teamviewer.com/Japanese
French (FR)	community.teamviewer.com/French
Spanish (ES)	community.teamviewer.com/Spanish
Portuguese (PT)	community.teamviewer.com/Portuguese
Chinese (CN)	community.teamviewer.com/Chinese



Do you want to know more



Visit our website:
www.teamviewer.com

About TeamViewer

As a leading global technology company, TeamViewer offers a secure remote connectivity platform to access, control, manage, monitor, and support any device — across platforms — from anywhere. With more than 600,000 customers, TeamViewer is free for private, non-commercial use and has been installed on more than 2.5 billion devices. TeamViewer continuously innovates in the fields of Remote Connectivity, Augmented Reality, Internet of Things, and Digital Customer Engagement, enabling companies from all industries to digitally transform their business-critical processes through seamless connectivity.

Founded in 2005, and headquartered in Göppingen, Germany, TeamViewer is a publicly held company with approximately 1,400 global employees. TeamViewer AG (TMV) is listed at Frankfurt Stock Exchange and belongs to the MDAX.

www.teamviewer.com/support

TeamViewer Germany GmbH

Bahnhofplatz 2 73033 Göppingen Germany
+49 (0) 7161 60692 50

TeamViewer US Inc.

5741 Rio Vista Dr Clearwater, FL 33760 USA
+1 800 638 0253 (Toll-Free)

Stay Connected

www.teamviewer.com