



Secure Remote Connectivity for Startups

Thriving startups know how to harness the power of collaboration. But it's a challenge to connect teams and empower them to work smarter. It requires intuitive logging and reporting, alongside powerful integrations on a cloud-based remote connectivity platform that is built to navigate the complexities of rapid growth.



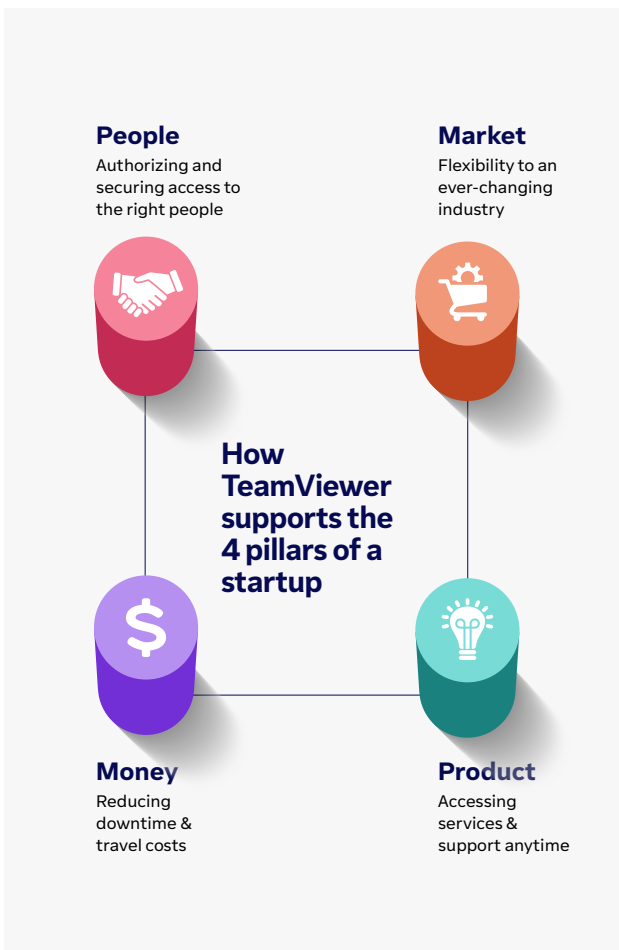
Despite fierce competition and challenging macroeconomic conditions, many startups are finding new ways to create transformative products and services. From tech, finance and retail to health and beauty, this creativity is presented across a wide variety of industries.

In the dynamic realm of startups, the demand for centralized access and comprehensive control over a wide array of critical elements is paramount. Startups rely on this command center to effortlessly manage and orchestrate their myriad applications, intricate systems, intricate integrations, and an assortment of devices. This approach enables them to swiftly respond to shifting market dynamics and

seize emerging opportunities. With centralized access and control at their disposal, startups are not just equipped to navigate the complexities of modern business, but they can also harness their innovative potential to chart a course towards sustained success.

TeamViewer for Startups provides a critical piece of the puzzle: centralized access and control for all the applications, systems, integrations and devices that startups need to stay nimble.

Empower team collaboration on a fast, flexible, and **ultra-secure cloud platform, user-friendly for everyone**, regardless of IT expertise.



TeamViewer makes it easy for authorized team members to gain full remote access to their work desktop, network, files, and applications. They can do so right from their mobile devices or laptops, without the need for a VPN. Should issues arise at home, in the office, or on the go, any team member can quickly access services and support at any time.

Being a cloud-based remote connectivity platform means less downtime due to service disruptions, as well. That includes fewer delays in receiving timely IT assistance, and reduced time and travel costs for field visits (updating and patching physical IT infrastructure, for example).

Essentially, flexible, secure, and budget-friendly remote connectivity that never cuts corners.

Meet stringent security standards and protocols.

- ✓ RSA 4096 private/public key exchange
- ✓ 256-bit AES session encoding
- ✓ SOC2 certified and compliant
- ✓ SO 27001 certification
- ✓ HIPAA compliant
- ✓ HTTPS/SSL protocol

Make security your top priority

Protection from brute force attacks

Automatically safeguard against this common attack method used against state and local governments. With enforced password reset, TeamViewer increases the time between failed login attempts, and resets only when the correct password is entered.

Dynamic passwords

Create a policy that auto-generates new dynamic session passwords after every TeamViewer service restart or individual session.

Two-factor authentication

Add another layer of authentication requiring a unique code generated each time by an algorithm and supplied from a mobile device.

Conditional Access

Control all incoming and outgoing remote support connections to mitigate risks, boost efficiency, and increase overall IT security.





Encryption

Protect all TeamViewer interactions — including file transfers, VPN, chat, remote access, and more—with 256-bit end-to-end session encryption and a 4096-bit RSA public/private key exchange.

Secure remote password protocol (SRP)

Ensure that passwords are never sent over the internet, even when encrypted, while maintaining optimal protection from outside access. All passwords also receive backend encryption for another layer of protection.

Robust protection for constituents, employees, and infrastructure

 <p>Integrations</p>	<p>Integrations connected through one platform can help you optimize your operations. Use TeamViewer with your mission-critical applications.</p> <ul style="list-style-type: none"> ✓ Leverage existing software such as Microsoft Teams, Freshworks, and Jira, etc. ✓ Improve issue resolution time and increase efficiency ✓ Reduce costs and manual errors between applications
 <p>Single Sign-On (SSO)</p>	<p>Limit access to user accounts with city or state emails only and provide IT more control over provisioning and deactivation of user accounts.</p> <ul style="list-style-type: none"> ✓ Centralize password control so IT doesn't have to handle every password-reset request ✓ Automatically apply password policies to every authorized user ✓ Enable remote login for employees using SSO credentials
 <p>Multitenancy</p>	<p>Always have a detailed overview of existing licenses throughout the platform, while offering secure and scalable support experiences for employees and associated business units.</p> <ul style="list-style-type: none"> ✓ Track, monitor and control license usage across central and remote organizational units. ✓ Scale support experiences without inflating cost ✓ Prevent over- and under-use of Tensor licenses ✓ Easily group users and devices based on specific requirements
 <p>Conditional Access</p>	<p>Maintain enterprise-wide oversight and centralized control of all TeamViewer connections with a dedicated conditional access rule-based router, fully maintained in a private cloud by TeamViewer.</p> <ul style="list-style-type: none"> ✓ Assign user and device permissions for remote access, remote control, file transfer, and TeamViewer Assist AR ✓ Configure rules at the account, group, or device level, with support for Active Directory Groups ✓ Provision and schedule remote access permissions with expiry dates and times for third-party vendors, contractors, or temporary employees ✓ Block all incoming and outgoing connections from unauthorized TeamViewer accounts and free users



User group and roles

Automate user life cycle management for TeamViewer Tensor users. Organize users into groups to apply bulk changes in permissions while eliminating repetitive, manual tasks.

- ✓ **Spend less time** creating, updating, and deleting users
- ✓ **Organize users into groups** for easier administration
- ✓ **Move users between groups** for role or department changes
- ✓ **Filter user groups** based on various roles for more efficient user management



Auditability

Built-in reporting log captures all remote session activities and management console actions: who did what, when, and for how long for every incoming and outgoing connection. Designated IT admins can only view these audit logs with appropriate user permissions.

- ✓ **Decide if activity log for remote sessions and management console is needed or not**
- ✓ **Assign specific user permissions** authorizing access to view reports
- ✓ **Maintain accountability** and provide precise billing for services
- ✓ **Track customer satisfaction** with session comments and customer feedback forms to improve services
- ✓ **Cut costs by** eliminating the need for third-party logging tools

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.

Stay Connected