TeamViewer | ivanti

Solution Brief

TeamViewer Mobile Device Management

Secure and manage your complex and ever-growing mobile ecosystem with TeamViewer.

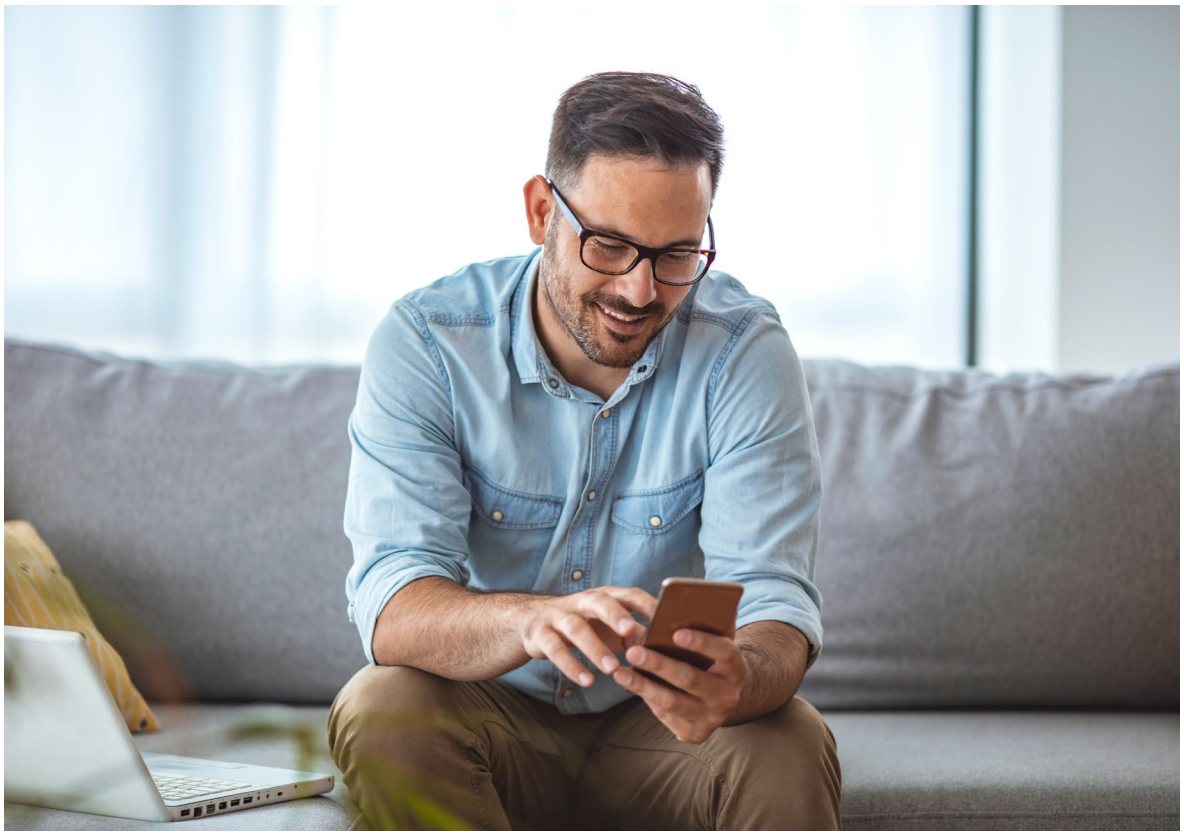
Introduction

Businesses are enabling flexible work by providing their employees with more and more mobile devices.

The use of smartphones, tablets, and other mobile devices has made it harder to track, manage, monitor, and maintain these devices, increasing their risk of getting lost or stolen.

Added to this, the wide-spread use of diverse mobile devices combined with sensitive business data operating in insecure networks also means an expanded attack surface.

Learn how a 360° mobile device management (MDM) helps you stay on top of your mobile device fleet 24/7.



Customer **challenges**

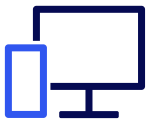
A distributed workforce accessing sensitive business data while working remotely, at home, or on the move can pose a significant risk to businesses. Here are some of the common reasons why businesses with a large mobile device footprint need to implement an MDM solution:

Data security
Ensuring mobile devices accessing sensitive corporate data are properly secured with measures such as encryption, minimum password requirements, and application restrictions.

Compliance
Businesses operating in specific industries are bound by regulations that govern the use of mobile devices.

User productivity
While mobile devices are valuable and help employees stay agile and responsive, they can also be distracting. MDM solutions can enable businesses to manage mobile devices in the workplace by providing capabilities such as app management and content filtering.

Rising IT costs
Managing mobile devices is both, effort and cost intensive. There is also a high risk of data breaches that can attract regulatory fines and penalties in certain industry verticals.



Device theft or loss
A mobile workforce can lead to devices getting lost or stolen in transit. These devices may contain sensitive data that could be exposed or leaked as a result by third-party actors.

Employee turnover
Securing mobile devices issued to employees leaving the organization can be challenging and risky, especially when the device is sent back to the IT department for recommissioning.

Device diversity
Managing an ever growing and diverse mobile device ecosystem with their own operation systems, configurations, and policies can be complex and time consuming.

Solution **highlights**

Enhanced security: MDM protects sensitive business data by enforcing security policies on mobile devices to ensure a prevention of data breaches and unauthorized access to sensitive information.

Improved compliance: MDM can help to ensure that enterprise mobile devices comply with industry regulations, such as SOC 2 Type II compliance, AES 256-bit encryption, and much more. This also includes features such as remote wipe and data loss prevention helping protect the businesses from regulatory fines and penalties.

Increased productivity: MDM can help to improve user productivity ensuring that users only have the apps and content that adhere to company security policies. It can also save time for IT departments that leverage MDM to reduce repetitive tasks.

Reduced IT costs: MDM helps to reduce IT costs by automating many of the tasks involved in managing mobile devices. This includes tasks such as device provisioning, app deployment, and security configurations for hundreds of devices operating across the enterprise.

Enhanced visibility and control: MDM gives businesses visibility into mobile devices such as their uptime, security status, and app usage enabling enterprises to better manage their devices and ensure that they are being used in a secure and compliant manner.

Key features and capabilities

Device management

User groups
Save time by creating custom user groups and using them to deploy content and applications in bulk.

Device management actions
Streamline your workflow by using quick actions such as Lock, Unlock, Retire, Wipe, Send Message, and Force Check-in.

Policies
Enhance your security by configuring and applying predefined critical security policies on specified devices or apps.

Easy onboarding
Enroll devices automatically with Apple Business Manager and Google Zero-Touch Enrollment.

App distribution and configuration
Easily distribute and configure mobile apps.

Security and management

Device security and management
Secure and manage endpoints running iOS and Android operating systems.

Mobile application management
Push applications to devices, manage application access and permissions, and remotely update or remove applications.

Secure email gateway
Manage, encrypt, and secure traffic between the mobile endpoint and back-end enterprise systems.

Secure productivity

Secure email and personal information management (PIM) app
Secure email and PIM application for iOS and Android. This includes government-grade encryption, certificate-based authentication, and passcode enforcement protecting user data from unauthorized access.

Secure web browsing
Make web browsing more secure by protecting both, data-in-motion and data-at-rest. Custom bookmarks and secure tunneling ensure that users have quick and safe access to business information.

Secure content collaboration
Employees working from remote office can securely access and collaborate using key repositories such as SharePoint, Box, Google Drive, and others.

Secure connectivity

Per app VPN
A multi-OS VPN solution that allows organizations to authorize specific mobile apps to access corporate resources behind the firewall without requiring any user interaction.

Conditional Access

Trust engine
Combine various signals such as user, device, app, network, geographic region, and more to provide adaptive access control.

Passwordless user authentication
Passwordless multi-factor authentication using device-as-identity for a single cloud or on-premises application.

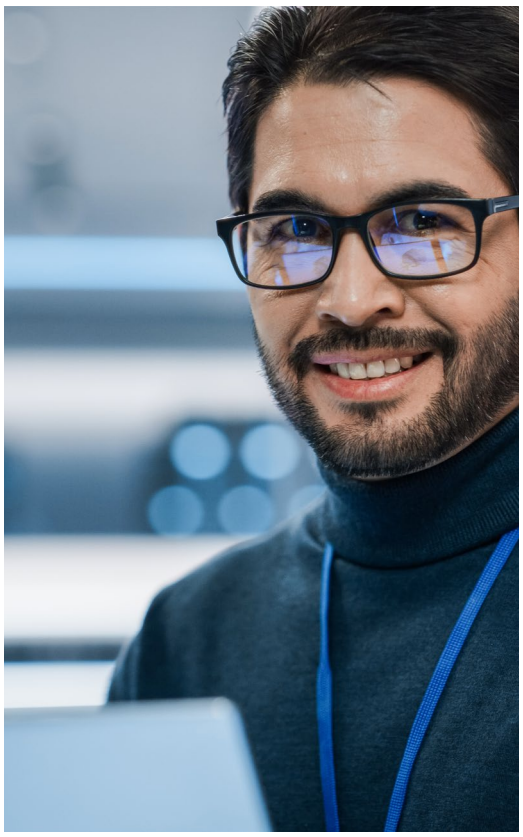
Secure by design

BITSIGHT
The Standard in SECURITY RATINGS

BitSight Security ranks TeamViewer as Top 1% in the Tech Industry.

People trust you to fix their IT problems. You need a powerful and secure tool to come through for them. Especially in the face of a complex tech stack and constantly changing threat landscape.

That's why TeamViewer remote support is secure by design. It's also why we innovate continuously — to make sure you're always one step ahead.



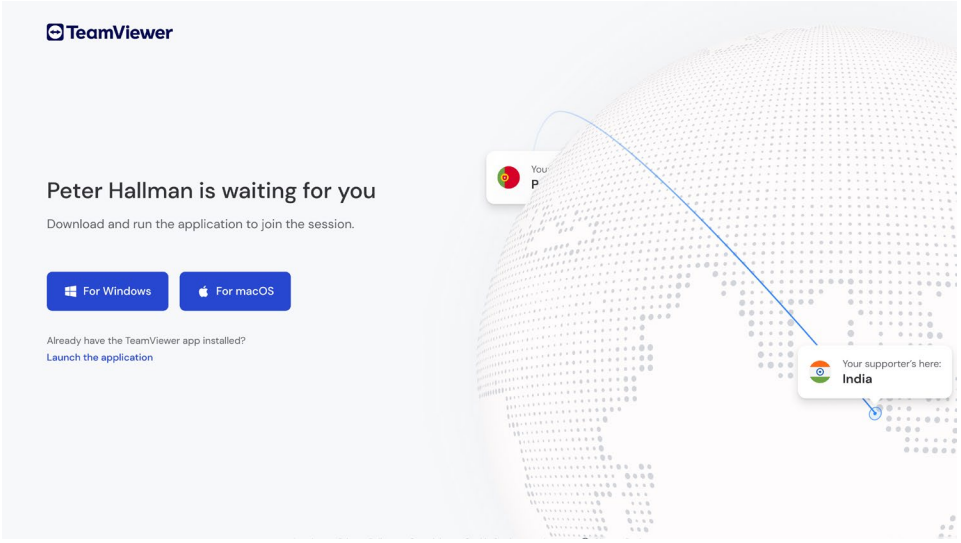
256-bit AES Encryption

Two-Factor Authentication

Brute Force Protection

Scam Protection

Allow- and block-list



TeamViewer shows you who wants to connect and where they are located.

Certified and **trusted**

TeamViewer is certified by major standards authorities and fulfills strict European data protection regulations as well as HIPAA requirements for North America.

Internal IT teams and service providers across the world rely on TeamViewer Remote Support to increase their efficiency and provide better support.

Do you want to know more

Visit our website:
www.teamviewer.com

TeamViewer

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
Bahnhofsplatz 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