



TeamViewer
Tensor

Remote work
is the *new normal.*





TeamViewer
Tensor



would work
remotely more
often

Based on a survey of 1,200 full time employees in the U.S. conducted April 16-17, 2020
Source: getAbstract



TeamViewer
Tensor



intend to shift
some employees
to remote work
permanently

A Gartner, Inc. survey of 317 CFOs and Finance leaders on March 30, 2020* revealed that 74% will move at least 5% of their previously on-site workforce to permanently remote positions post-COVID 19



TeamViewer
Tensor



noticed an increase
in security threats
or attacks since
the beginning of
the Coronavirus
outbreak

<https://securityboulevard.com/2020/05/the-many-ways-your-employees-can-get-hacked-while-working-from-home-and-how-to-respond/>

May 5, 2020

MORE >

“The future of the VPN, with certainty, has limited days. The coronavirus pandemic may have solidified and accelerated those days, leading ultimately to the death of the VPN.”

*Paul Martini
Security Boulevard
May 20, 2020*



What matters right now

1

Securely allowing the use of corporate and non-corporate IT devices to access your network

2

Prevent corporate network intrusions due to increased VPN use

3

Ensure employee efficiency at all times when working from home

Work-from-home opens up three vectors for cyberattacks



In-app access

Lack of multi-factor authentication (MFA), weak authentication, and VPN use

Personal Devices

Lack of centralized control for patching, network access, and endpoint data protection

Social Control

Increased phishing emails and fake call center agents, and inability to prevent human error

CSIA issued the following security alert (March 2020)



Vulnerabilities

More vulnerabilities through
malicious cyber actors

Lack of multifactor authentication
(MFA) for remote access

Increased phishing emails




VPN

Keeping 24/7 VPNs updated with
the latest security and patches

Limited number
of VPN connections

Decreased availability causes
problems in business operations and
in IT performed cybersecurity tasks

Reducing the risks of using BYOD and company-issued devices

	VPN via company issued/owned device	Remote Access via company-issued device	Remote Access with personal device
Employee onboarding	Slow and costly provisioning because of manual installment of VPN certificate by IT	Secure remote access provisioned remotely and instantly by IT	✓
Employee offboarding	Actual data has been processed on the end user device and could have been stored locally	Access can be instantly revoked with one click – no data has left the company	✓
Performance	 <p>Degradation in performance: all processing happens on the employee hardware; large amount of data being sent through network</p>	 <p>Superfast end user: with screen mirroring, only incremental image changes are transmitted and updated on the screen</p>	 <p>Flawless end user experience too: even on low performance computers due to screen mirroring</p>





Future-proof, secure digital remote work environment – for everyone, at enterprise scale

TeamViewer One World – One Solution: Enable A Secure Digital Workplace

A single solution
for tackling the *new
normal*

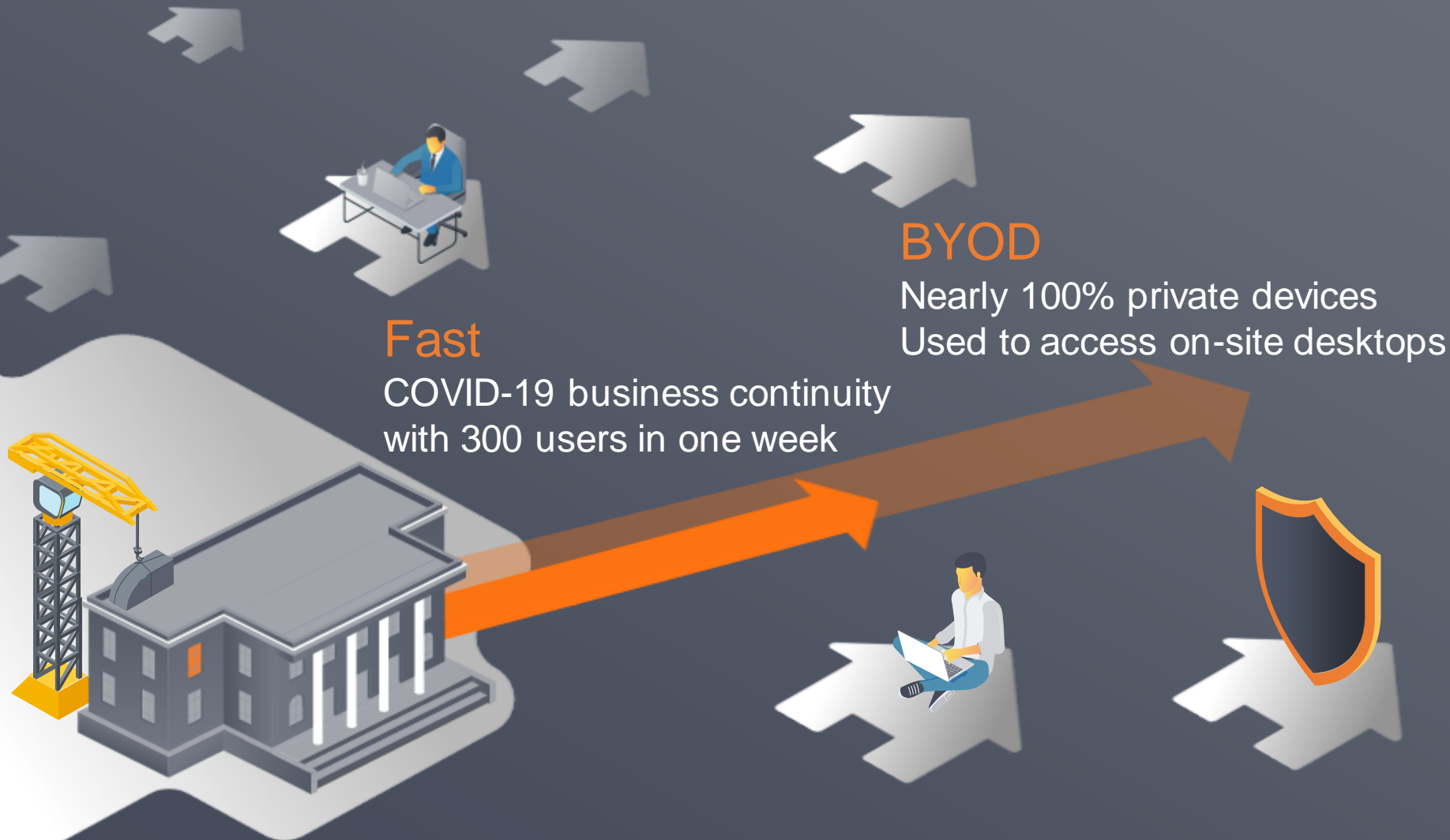
- ✓ Provision secure remote workplaces in hours
- ✓ Enforce access rights for each individual device or group of devices
- ✓ Access rights apply for company-issued or personal devices, including mobile
- ✓ Restrict and suspend file transfer
- ✓ Enable secure, encrypted, locked online meetings and screensharing
- ✓ Automatically remotely patch outdated devices

USE CASE

Work from home, safe and sound in the public sector

Municipality under construction

Use Case: Work from home in the public sector, April 2020



Highly Secure
meeting requirements
of the public sector:

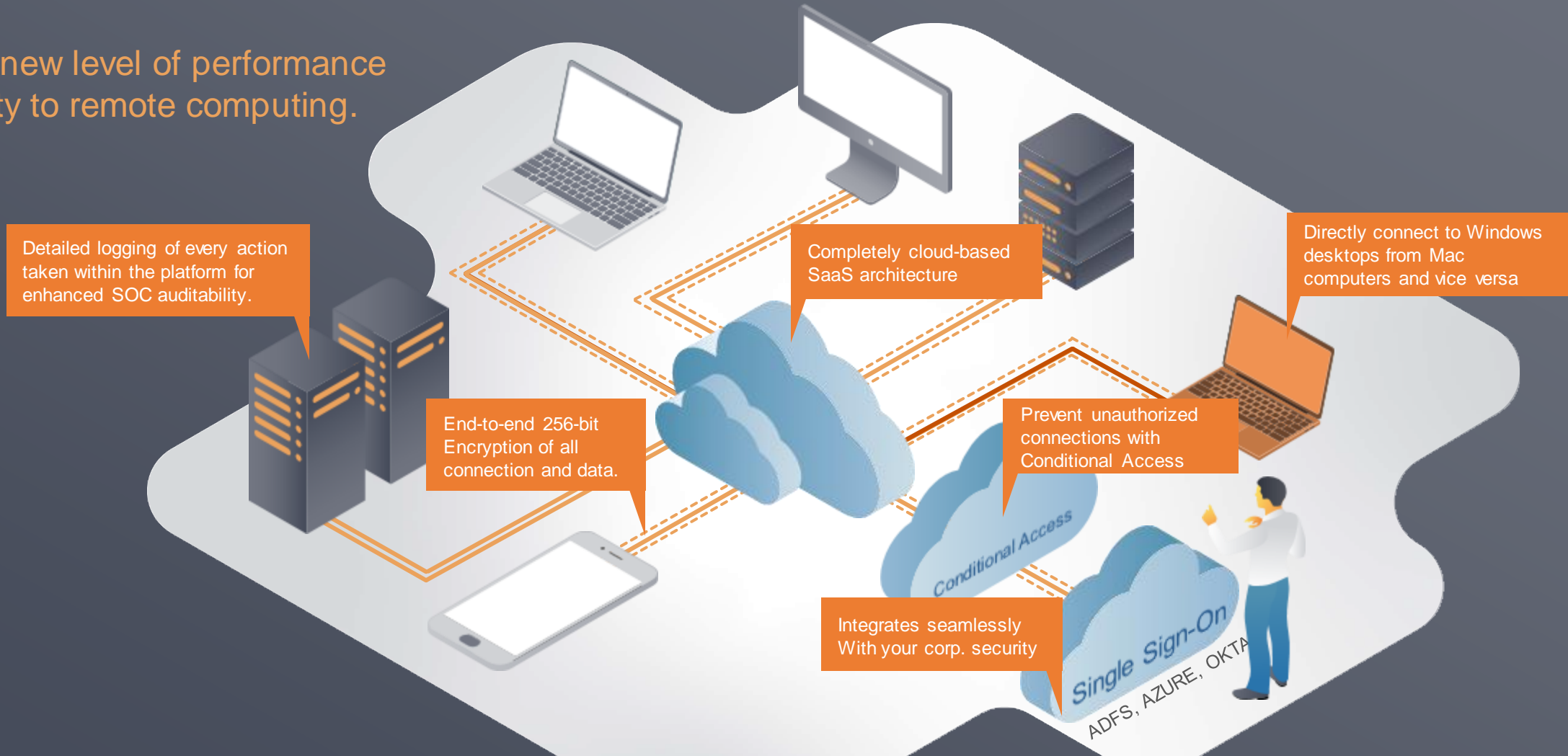
- Conditional Access
- Single Sign-On
- Reporting and Auditability
- Black Screen

Future saving:
1 Mio. EUR
re-building municipality,
not renting lease office

Scalable
all 1,100 users in 2nd wave

TeamViewer Tensor™

Bringing a new level of performance and security to remote computing.



TeamViewer Tensor™ Single Sign-On

Enforce your password and multi-factor authentication policy

Centralized
password
management
reduces IT burden
significantly

- Apply your corporate password authentication policies and rules
- Multi-factor authentication works the same way for BYOD devices used externally as it works on premises – requiring application authentication
- Remote employee uses his company credentials to access any on premises devices and applications
- Grant or revoke access rights instantly for new or exiting employees
- Instantly set and reset account credentials remotely
- IT department can manage the whole company IT infrastructure from home too



TeamViewer Tensor™ Conditional Access

Prevent unauthorized remote access and align with corporate security policies

Enforce your
corporate security
policies at highest
level of granularity

- Define and enforce access rules at user/account, group or device level
- Central management & control of all incoming and outgoing connections
- Restrict the type of connection (Remote Access, File Transfer, Meeting) down to the individual
- Rule based engine, like a firewall, that expands beyond your corporate network and devices
- Dedicated, secure cloud servers, exclusive to the customer

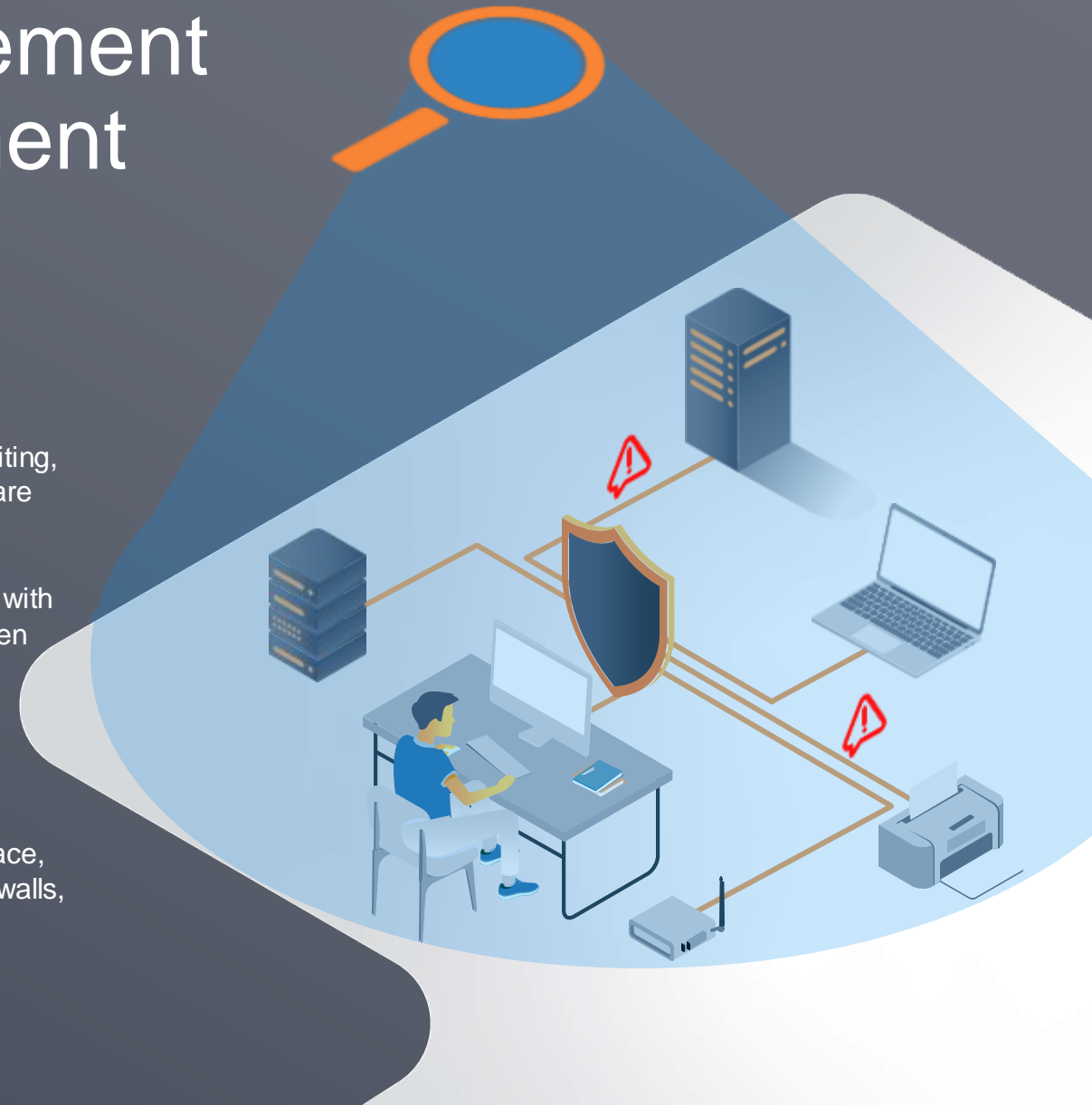


TeamViewer Remote Management Monitoring & Asset Management

Ensure stability and security of your IT systems

Keep your
systems running
smoothly – always
one step ahead

- Track deployed hardware and software for easy auditing, compliance, and safety (e.g., detect forbidden software installations)
- Proactively detect problems in your IT infrastructure with immediate alerts to prevent issues before they happen
- Prevent unplanned downtime and data loss
- Customize definitions of checks and thresholds
- Monitor critical device information, including disk space, CPU usage, system updates, antivirus software, firewalls, event logs, processes, and more

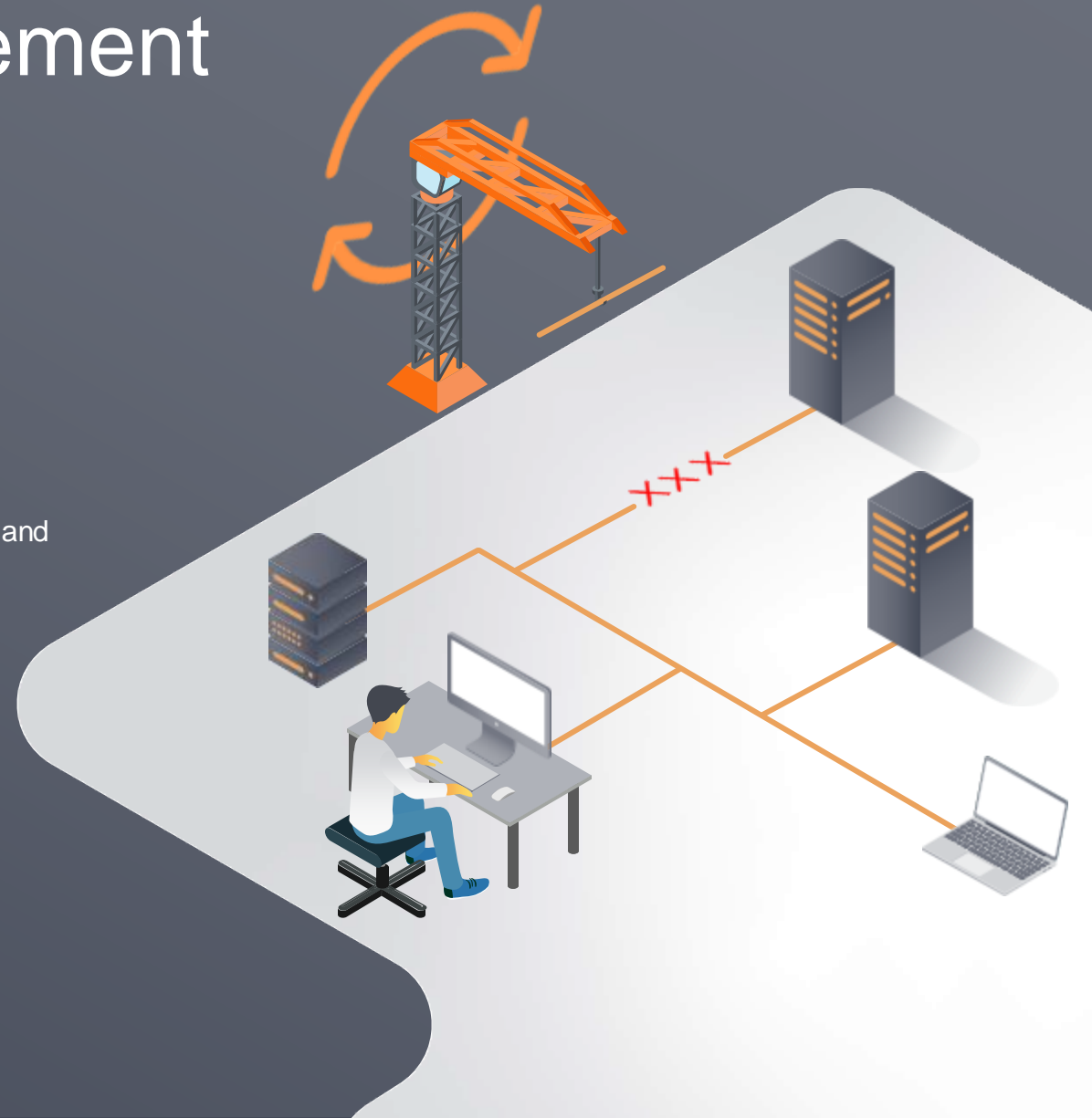


TeamViewer Remote Management Patch Management

It takes one unpatched device to put your entire IT at risk

Automatically
detect and patch
computer
vulnerabilities

- Proactively protect your IT systems, increase safety and integrity of your networks
- Detect outdated, vulnerable software
- For Windows and third-party applications
- Automated and policy-driven
- Fully integrated into TeamViewer



TeamViewer Meetings

Online Meeting & Collaboration

blizz by Teamviewer, instantly available for every Remote Worker

Integrated end-to-end encrypted online meetings and collaboration

- Start and participate in online meetings from any device
- End-to-end encrypted video calls, screen sharing, chat, and VoIP connections
- Lock meetings to prevent unauthorized attendees
- Easy session recording with opt-in for every attendee to have their video and audio included
- Proprietary blizz meeting recording format, optimized for screen-recordings



TeamViewer Tensor™ Enterprise Reporting & Auditing

Document all activities with a complete audit trail

Support internal
audit requirements
and adhere to
corporate security
policies

- Log relevant actions associated with a remote session (who, what, where, when)
- Trace all actions taken in the management console (add/delete user, rights)
- Centrally manage and restrict who has access to captured logs
- Search for specific events (user, data, session, action taken)
- Ability to integrate into existing third-party audit environments through API
- Zero-knowledge network ensures data privacy at all points



“Don’t assume legacy infrastructure will sufficiently enable and support remote work.”

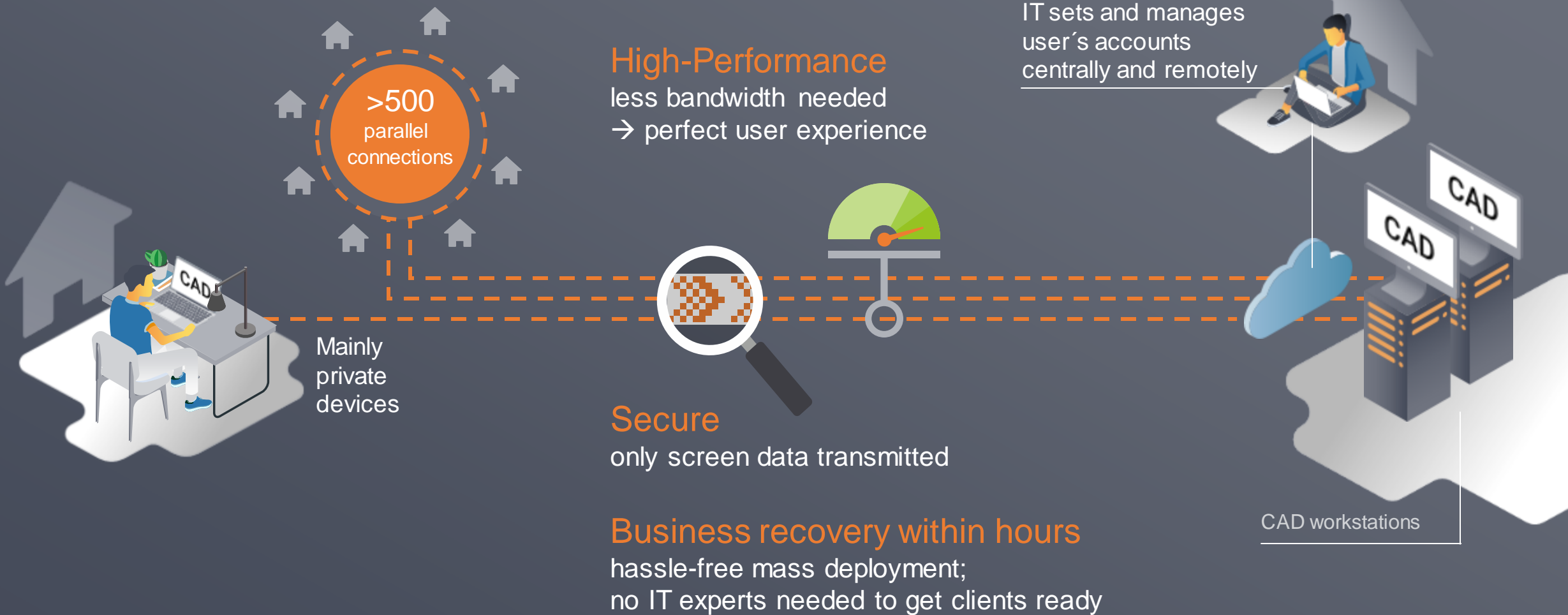
*Gregg Siegfried,
Gartner Research Director for Cloud and IT Operations,
was recently quoted by [Diginomica](#).*

USE CASE

Access CAD workstation power from home on private laptops

Italian automotive OEM continues to engineer at home within hours

Use Case: 500 CAD engineers work from home despite COVID-19 outbreak



VPN vs. Remote Access

Setup

Maintenance

Compatibility

Performance

Cost

VPN

Complex configuration process for host devices, remote devices, and networks.

Requires dedicated certificate, which often needs to be rolled out manually to each client or device.

Remote Access

Simple installation process and ability to roll out to thousands of devices simultaneously, with a few clicks and done in hours.

Exchange from security certificates not necessary



VPN vs. Remote Access

Setup

Maintenance

Compatibility

Performance

Cost

VPN

Needs constant maintenance and patching to ensure that they are running optimally.

Cumbersome with setting up AD account, then VPN gets installed resulting in manual provision/decommission of users. Overall user management = labor intense

Remote Access

Is centrally configured, auto-scaling and optimized for best enduser experience.

Users can be managed on device or group level, same applies for provisioning /decommissioning



VPN vs. Remote Access

Setup

Maintenance

Compatibility

Performance

Cost

VPN

VPN client and VPN server from different vendors may result in incompatibilities and challenges in resolving issues

Remote Access

One complete, integrated solution, including:

- online meetings
- IT infrastructure monitoring
- patch management

One company vendor relationship



VPN vs. Remote Access

Setup

Maintenance

Compatibility

Performance

Cost

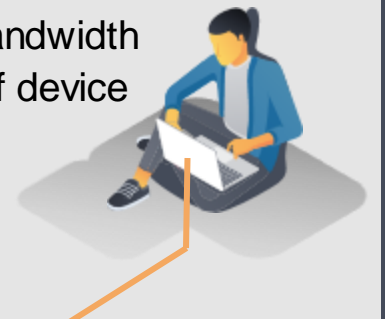
VPN

Massive degradation, as all data is sent through the network, and processing is done on the users' remote device

Remote Access

Screen images are transmitted (increments and desktop optimized) and very little bandwidth is required.

Result: an incredibly fast and reliable user experience, even on low bandwidth connections – regardless of device



VPN vs. Remote Access

Setup

Maintenance

Compatibility

Performance

Cost

VPN

Setup and maintenance are labor intensive, cost is high for server, bandwidth, and often additional gateways.

Application licensing often requires additional licenses for BYOD devices

Additional requirements for license compliance checks (risk compliance)

Remote Access

Setup and rollout are done in a matter of hours

No additional server or gateway costs, with low impact on bandwidth

As data and applications are accessed remotely, no additional licenses are required.



TeamViewer Tensor™ -
Work from Anywhere



Working remotely can be as efficient as working at your office.

Work remotely without losing efficiency due to network latency caused by VPN or processing power.

- ✓ Instant, secure connections to on-premises desktop
- ✓ Access local storage at work at LAN speeds
- ✓ Remote in to powerful workstations to use resource-intensive applications from anywhere
- ✓ Secure access from any device, including BYOD
- ✓ Ensure data privacy through black screen functionality
- ✓ Integrated chat and online collaboration functionality

Why TeamViewer Tensor for Remote Access?

4

Comply with corporate security policies with Single Sign-On and Conditional Access

3

Industry-certified security for data protection with comprehensive logging and reporting for auditing and compliance

5

Harness the power, security and lower TCO of remote access over VPN

2

Scale instantly and linearly for corporate needs

6

Run your business remotely with one integrated cloud solution for:

- remote access,
- remote support,
- device management, endpoint security, and collaboration

1

Enable a productive, secure remote workplace for business continuity in any market conditions





TeamViewer
Tensor

Addendum

TeamViewer Tensor™ Key Benefits

Enterprise SaaS Platform

Security

- Conditional Access
- Single Sign-On based on SAML 2.0
- Extended authentication options including MFA
- Define access rules at account, device, group level
- End-to-end encryption
- Centralized management of access rights
- Comply with corporate policies

Auditability

- Comprehensive reporting and audit trails
- Opt-in / opt-out
- Remote session logs
- Management console logs
- Track activities for audit, incident management, or security purposes
- Only authorized users access event logs

Scalability

- Mass deployment with msi package
- Deploy silently, no end user disruption
- Roll out to a large number of devices
- Easier account assignment
- Work with RMM solutions
- Cloud-based solution
- Fast ramp-up

Manageability

- Device agnostic platform
- Access, control, and support thousands of devices remotely
- Centralized management of access rights
- Enhanced user management
- One-Click script execution to perform repetitive tasks
- Reduce complexity for password recovery

Productivity

- Prebuilt software integrations
- Support mobile devices, across operating systems
- Improved user provisioning capabilities
- Device management and app customization
- Easy to operate
- User-friendly interface
- No maintenance burden





4

About TeamViewer

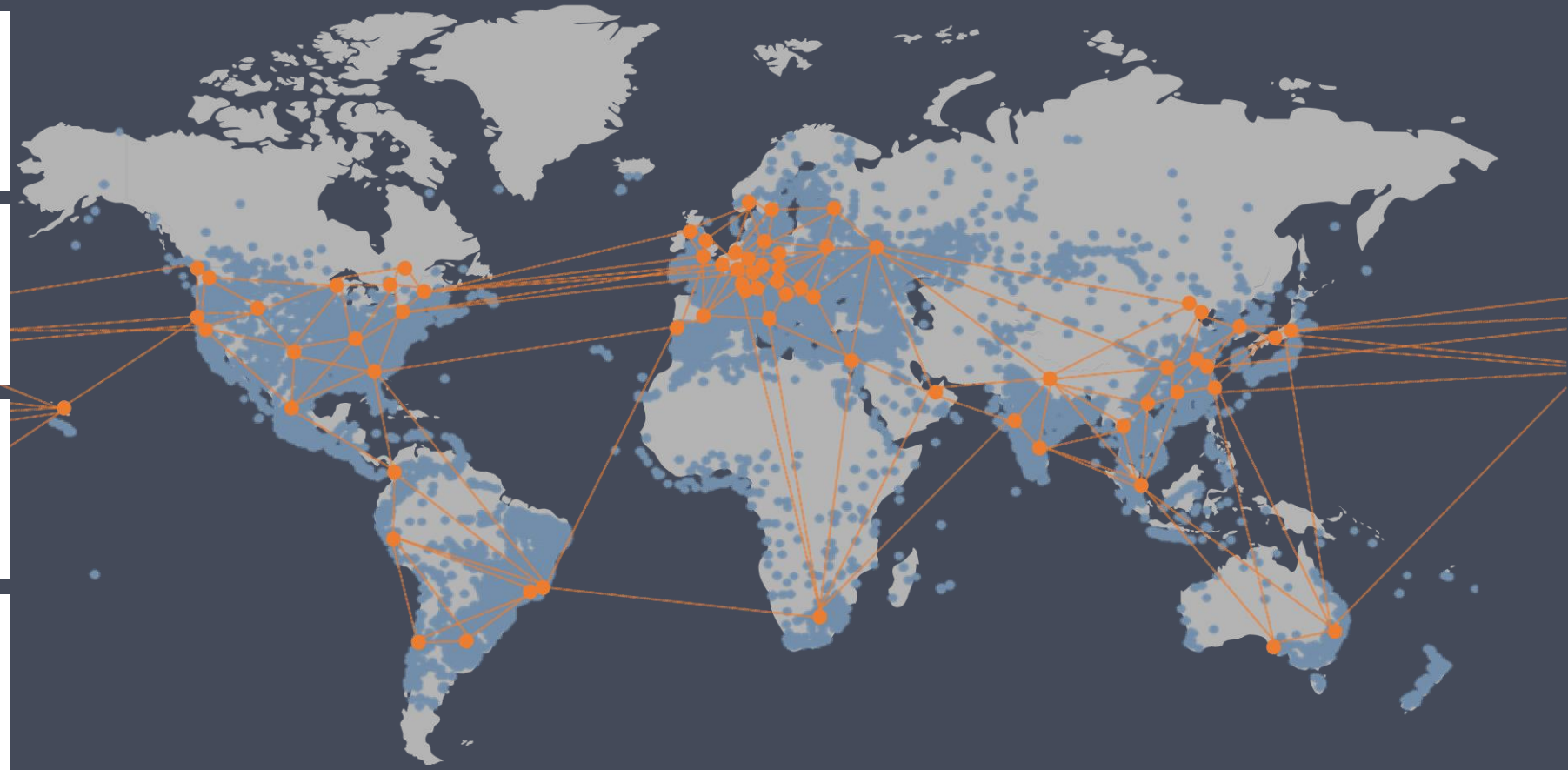
100% Cloud Delivered, Truly Global Distributed Architecture

Highly scalable cloud platform
with automatic load balancing
and embedded redundancy

Widely distributed over 81
locations for lowest latency

Optimized routing algorithms
to achieve best performance

Infrastructure agnostic resources
managed by TeamViewer



● Real location of our global router network

● Usage across one 24-hour period

Source: Company information

Leader Across Multiple Dimensions: Scale, Performance And Quality

PRODUCT

45m

Devices online
concurrently (up to)

>20

App releases per month



#1



Best Remote Desktop Software
(Top right of quadrant)
by G2 Crowd score

PLATFORM

100%

Cloud Hosted

>1,000

Routers worldwide

30-40ms

Latency on WAN
connections ⁽²⁾

PERFORMANCE

~99.9%

Uptime ⁽¹⁾

60FPS

Frames per second ⁽²⁾ leading to
seamless interface

120MBPS

Average transfer rate ⁽²⁾