TeamViewer

Secure, unified remote access for your shop floor

Remote access that complies with NIS2, NIST and other security standards .

Solution Brief

TeamViewer Tensor

With cyber attacks against industrial facilities on the rise, manufacturers have never been under greater pressure to harden their security.

With TeamViewer Tensor for operational technology, you get market-leading remote access and support that is secure by design.

When you secure your operational technology (OT) and information technology (IT) with TeamViewer Tensor, you get:

A **zero-trust framework** for secure, encrypted remote access.

Compliance with NIS2, NIST and other security standards.

Simplified, streamlined, advanced support for your entire ecosystem.

Support for diverse assets on your shop floor, including legacy and closed systems.

Support for complex, secure micro-segmented networks.

Overcome remote access fragmentation and variable security

The cyber-security risk for manufacturers is higher than it's ever been. According to the most recent IBM survey, manufacturing is the sector most often targeted by cyber-criminals[1].

At the same time, manufacturers are under pressure to improve efficiency, reduce costs and increase output. One of the best ways of doing this, is by using remote access tools to rationalise support, minimize downtime and optimize manufacturing systems.

But many manufacturing environments still use a mix of heterogeneous remote access tools, some from commercial providers, others built in-house. This causes a range of problems, with productivity, staff experience and above all, with security. This leads to a range of challenges:

[1]IBM

A mixed set of remote access tools used by external supporters increases the number of attack vectors.

Without a single-unified remote access administration platform, it's difficult to ensure your different remote access tools are patched and secure.

In-house remote access systems often lack support for micro-segmented networks, role-based access control and other advanced features.

A heterogeneous remote access environment is difficult and expensive to scale as your operations evolve and grow.

Tools such as VPNs make it hard to track how many external vendors have access or to restrict access to only those systems the vendor needs to access.

Demonstrating compliance with national and other relevant security standards can be expensive, time consuming and complex.

Meeting strict cybersecurity insurance requirements demands continuous adoption of the latest protection measures across production environments.

Remote access and NIS2 compliance

Failure to comply with the EU's Second Network and Information Security Directive (NIS2) can lead to fines of €10 million or 2% of global annual turnover. If the company is found to have committed gross negligence, senior management can be held personally liable. And for importers based elsewhere in the world, an inability to comply makes it difficult or impossible to do business in the EU.

Insecure, heterogenous or over-complicated remote access set-ups create specific problems with NIS2 compliance. These include access-control difficulties, increased third-party risk with each external connection, audit and logging gaps — and so on.

This is why it's crucial that manufacturers have a remote access platform that's secure by design and comes with all the necessary monitoring, auditing and other functions required to demonstrate NIS2 compliance.

Secure, compliant, effective remote access with TeamViewer Tensor.

TeamViewer Tensor for operational technology is designed to work with maximum efficiency across manufacturing environments. It provides a unified solution that standardizes remote access to all endpoints – minimizing security risks and ensuring regulatory compliance. The advantages of using TeamViewer Tensor for your remote access include:

One shopfloor. One solution. Full access
Standardized remote access to programmable logic controllers (PLCs) and human-machine interfaces (HMIs).

Standardized remote access operations
Use a single solution for screen-control access and network appliance access for secure, instant and efficient remote access to the production environment.

Enhanced security as standard
Protect remote access on the shopfloor from cyber-security threats with zero-trust security, role-based access, strong encryption and more.

Seamless external access
Easily invite external partners and vendors to secure remote access via an encrypted browser session with no need to open inbound firewall ports.

Advanced authentication
Prevent unauthorized access with multi-factor authentication (MFA), Single Sign-on (SSO), Conditional Access and support for Bring Your Own Certificate (BYOC).

Easy access
Access individual endpoints directly with the Agentless Access feature – without installing a TeamViewer client on every endpoint.

Market-leading encryption
TeamViewer remote access sessions are protected by 4096-bit RSA and 256-bit AES session encryption; even TeamViewer servers cannot decrypt session data.

Advanced, easy-to-use auditability
By design, TeamViewer Tensor logs all significant events during a session — and you can also opt to record sessions for added transparency.

Segmented network support
TeamViewer Tensor supports secure segmented networking using last bastion and gateway components to control access to each separate segment.

Bypass the limitations of a conventional VPN setup

Unlike standard VPN setups and unmanaged remote access tools, TeamViewer Tensor for operational technology combines traditional perimeter-based security concepts (such as network segmentation) with a modern zero-trust architecture. It also provides fine, granular access control down to the level of each individual industrial device or IP port. This adds multiple layers of security to protect systems on the shop floor during both internal and external remote access for central access control and auditing.

The benefits of using TeamViewer Tensor for operational technology

Choosing TeamViewer Tensor for operational technology makes it easy to deliver secure, transparent, auditable remote access across your entire manufacturing environment.

Benefits of choosing TeamViewer Tensor include:

- Maximize uptime and productivity with market-leading remote access and support that enables rapid, effective maintenance.
- Grant secure, scalable access to all your corporate IT and shop floor endpoints from a single interface.
- Reduce your attack surface with unified remote access across your environment.
- Give third-party vendors fast, secure, policy-controlled access to your environment and to specific endpoints.
- Achieve regulatory compliance with structured security frameworks aligned to data-protection and industry regulations.
- Minimize human error with awareness-driven controls and pre-set safe configurations to guide and assist users.
- Simplify patch and update management with support for secure, remote software maintenance across device types.

Get started with TeamViewer Tensor for operational technology

Find out how TeamViewer Tensor for operational technology can help you achieve your productivity, security and compliance goals.

Speak to our experts

About TeamViewer

TeamViewer provides a Digital Workplace platform that connects people with technology – enabling, improving and automating digital processes to make work work better.

In 2005, TeamViewer started with software to connect to computers from anywhere to eliminate travel and enhance productivity. It rapidly became the de facto standard for remote access and support and the preferred solution for hundreds of millions of users across the world to help others with IT issues. Today, more than 640,000 customers across industries rely on TeamViewer to optimize their digital workplaces - from small to medium sized businesses to the world's largest enterprises - empowering both desk-based employees and frontline workers. Organizations use TeamViewer's solutions to prevent and resolve disruptions with digital endpoints of any kind, securely manage complex IT and industrial device landscapes, and enhance processes with augmented reality powered workflows and assistance - leveraging AI and integrating seamlessly with leading tech partners. Against the backdrop of global digital transformation and challenges like shortage of skilled labor, hybrid working, accelerated data analysis and the rise of new technologies, TeamViewer's solutions offer a clear value add by increasing productivity, reducing machine downtime, speeding up talent onboarding, and improving customer and employee satisfaction.

The company is headquartered in Göppingen, Germany, and employs more than 1,800 people globally. In 2024, TeamViewer achieved a revenue of around EUR 671 million. TeamViewer SE (TMV) is listed at Frankfurt Stock Exchange and belongs to the MDAX. Further information can be found at www.teamviewer.com..

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