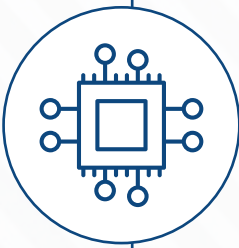




**A Reliable
Cybersecurity
Protocol for IT-OT
Convergence**



Real-time Visibility Enables Safety for Manufacturing Processes / A Framework to Safeguard your Industrial Systems



Operational Technology (OT) is a vital component of critical manufacturing infrastructure systems worldwide, as organizations scale and evolve in the digital era.



Traditionally, manufacturing machinery and equipment has been run and maintained using separate systems with minimal manual intervention.



With the advent of Industry 4.0 about a decade ago, this began to change as manufacturing firms vied with one another to implement the latest technologies to oversee and communicate with their production processes.

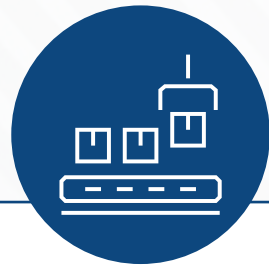


More and more manufacturing firms globally converged their OT (operational technology) with IT systems. The modern Smart OT landscape comprises interconnected heterogeneous devices, controllers, and sensors for real-time equipment monitoring.

IT-OT convergence solutions connect this landscape to internal and external teams across your organization, workflows, and processes spanning your value chain and enable seamless, remote communication through people, devices, platforms, and apps that are part of your digitalized enterprise.



The increasing interconnectedness of IT and OT has delivered strong advantages for manufacturing organizations:



Scale

When a comprehensive, digital fabric provides an overview of your entire OT ecosystem, Scale is easier to manage as compared to legacy isolated OT systems



Optimization

With a single virtual window across all your production floors, you can spot patterns that lead to inefficiencies, proactively analyze them, and implement necessary changes for optimization on the go. This real-time agility is not possible in siloed, traditional scenarios.



But the race to leverage technology to get bigger and better is getting harder.

McKinsey recently found that firms that successfully extended their IT-OT convergence across their manufacturing value chain are rapidly pulling ahead of the pack. There is no time for complacency and manufacturing companies must immediately focus on setting up and expanding their IT-OT convergence.

But, as always, advancement will bring new challenges.



- > IBM X-Force Threat Intelligence Index 2022
- > Gartner Newsroom Article - Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments (July 2021)
- > McKinsey Article - Converge IT and OT to turbocharge business operations' scaling power (June 2022)



The Greater Vulnerability of a Larger Attack Surface

The removal of the hard boundaries between the disparate IT and OT ecosystems exposes your operational technology to the cyber threats IT systems have been dealing with for decades. Manufacturing companies are currently the preferred targets for cyberattacks surpassing finance and insurance verticals for the most number of cyber-attacks experienced.

Manufacturing firms are a crucial component of the always-on global supply chain and can afford very little downtime. With growing end-to-end digitization, accelerated by Industry 4.0 and the pandemic, the critical manufacturing processes of these firms are now online and exposed to the malicious intentions of cybercriminals.

Research by Gartner has found that attacks on integrated OT environments are also increasing in intensity – evolving from process disruption such as shutting down a plant, to tampering with the integrity of industrial environments to create physical harm. Meanwhile, organizations in asset-intensive industries like manufacturing are struggling to define appropriate control frameworks.

Parameters of concern / Windows of risk

Given the alarming scenario, firms must move OT security upward in their risk portfolio. There are three dimensions concerning their IT-OT integration that manufacturing firms should reassess urgently:



Auditability

As you bring your entire OT ecosystem under a single digital layer, a precise protocol is required to record the actions of every stakeholder within and outside your organization who connects or accesses the integrated system.

What you need: A solution that enables your security teams to conduct regular, rigorous audits and up-to-date documentation



Visibility

The growing trend of remote working or a workforce that uses devices accessing mission-critical data on the move in an integrated digital environment translates into any interested party within or external to your organization working from anywhere in the world accessing your manufacturing processes at any time with any device. Live monitoring of these log-ins and activities to ensure your stakeholders' accounts or your system have not been breached is crucial and critical to safeguarding your perimeter and overall security posture.

What you need: A real-time 360 overview of stakeholder access



Governance

Visibility alone will not suffice since an integrated IT-OT system has a diverse set of users across our value chain with diverse objectives and ways of working accessing it round-the-clock. The solution has to pin down access privileges to minimize vulnerability

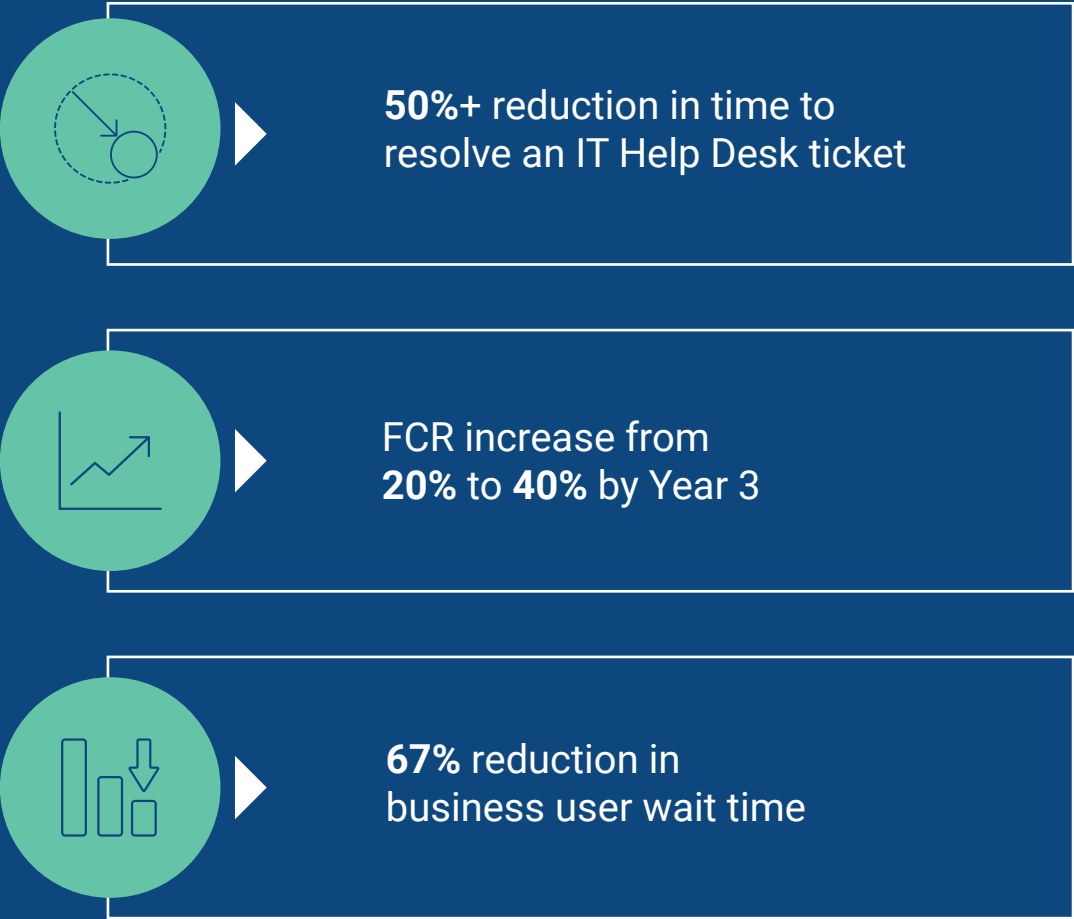
What you need: A well-defined, rapidly scalable governance framework

Your answer: TeamViewer Tensor – A Secure, Single Window for IT-OT Convergence

TeamViewer Tensor is a highly scalable remote connectivity cloud-based platform with enterprise-grade security. Its in-built connectivity stack provides seamless integration of the enterprise network with IT and OT, paving the way for unified, single window access to all IT and OT assets.

We have been at the forefront of using IT-OT convergence to deliver business benefits to our clients.

In October 2021, a study conducted by Forrester Consulting determined the total economic impact (TEI) of the TeamViewer platform. It included a manufacturing perspective and found that TeamViewer Tensor offered an ROI of 167% over three years and a net present value (NPV) of \$636,000. The payback period kicked off within three months.



How does TeamViewer achieve this impact?

We ensure your integrated IT-OT environment is secure, monitored and responsive at all times, ensuring minimal downtime.



Auditability

TeamViewer Tensor empowers the organization with comprehensive auditing, logging, and reporting capabilities. Every connection made to and from PCs to the TeamViewer Tensor platform can be audited and all activities are logged onto the management console from the implementation phase itself



Visibility

The Centralized Management Console enables a real-time 360° view as well as management of all incoming and outgoing connections to the assets from the implementation stage itself



Governance

Centralized Permission Control helps teams put together a fine-grained governance framework to define access for users, groups and roles



Optimized processes

Digitalize and streamline IT and OT assets on the go across employees, customers, service providers and partners



Multi-layered security

With a multi-point check and balance mechanism to proactively identify and thwart any security risks, ensuring best-in-class experiences and enterprise-grade security



TeamViewer Tensor Secures your Integrated IT-OT Environment with Industry-Leading End-to-End Encryption

Cutting-edge 4096-bit RSA key encryption and 256-bit AES session encryption to ensure industry-leading end-to-end encryption.



Brute-Force Protection

Countermeasures against brute-force attacks, including exponential time delays after failed login attempts and AI-based network monitoring



Two-Factor Authentication (TFA) for Connections

To secure user devices. Alternatively, devices can be configured to be accessible via a TFA-protected account only



Two-Factor Authentication (TFA) for Accounts

To secure user accounts. If not enabled, account logins from unknown devices must be confirmed via email



Conditional Access

To enforce company-specific security policies and protocols with highly granular access rights management



Secure Remote Password Protocol

Account passwords never leave the client and remain unknown to our servers

Why TeamViewer Tensor is Secure



Unlock opportunities without worry

Manufacturing firms are bringing their operations online during a period of global volatility. While the scenario demands you display greater flexibility, agility and responsiveness than before for competitive advantage, leveraging interconnectedness to achieve this also exposes your operations to far greater risk. As your integration partner, TeamViewer Tensor effectively resolves this conundrum with secure, remote access accompanied by real-time oversight and optimization of your OT systems.



About TeamViewer

TeamViewer is a leading global technology company that provides a connectivity platform to remotely access, control, manage, monitor, and repair devices of any kind — from laptops and mobile phones to industrial machines and robots. TeamViewer continuously innovates in fields such as Augmented Reality, enabling companies from all industries to digitally transform their workforce and business-critical processes. Through strategic acquisitions of Ubimax, Upskill, and Viscopic, TeamViewer has built a fully comprehensive, end-to-end AR solution on the market. TeamViewer Frontline optimizes processes along the entire industrial value chain, closing the loop to an entirely digital industrial workspace.

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.

Questions?

Connect with us to request a free consultation or schedule a personalized demo of TeamViewer Tensor

 +49-7161-60692-50

 tensor_emea@teamviewer.com

Stay Connected



www.teamviewer.com