Secure and scalable remote access for production machines and systems
With the Secure Access Gateway

Secure remote maintenance access for machines and systems
With rising cyber threats and new regulatory requirements such as NIS2, companies face increasing pressure to enable remote access efficiently without compromising the security of sensitive machines and systems.

Traditional VPN solutions can significantly increase the attack surface if insufficiently or improperly configured.
The Zero-Trust approach of TeamViewer Tensor combined with Bechtle Gateway hardware provides — thanks to a "least privilege by design" concept — the perfect answer to the needs of modern OT infrastructures for secure remote access.

Technology that inspires trust

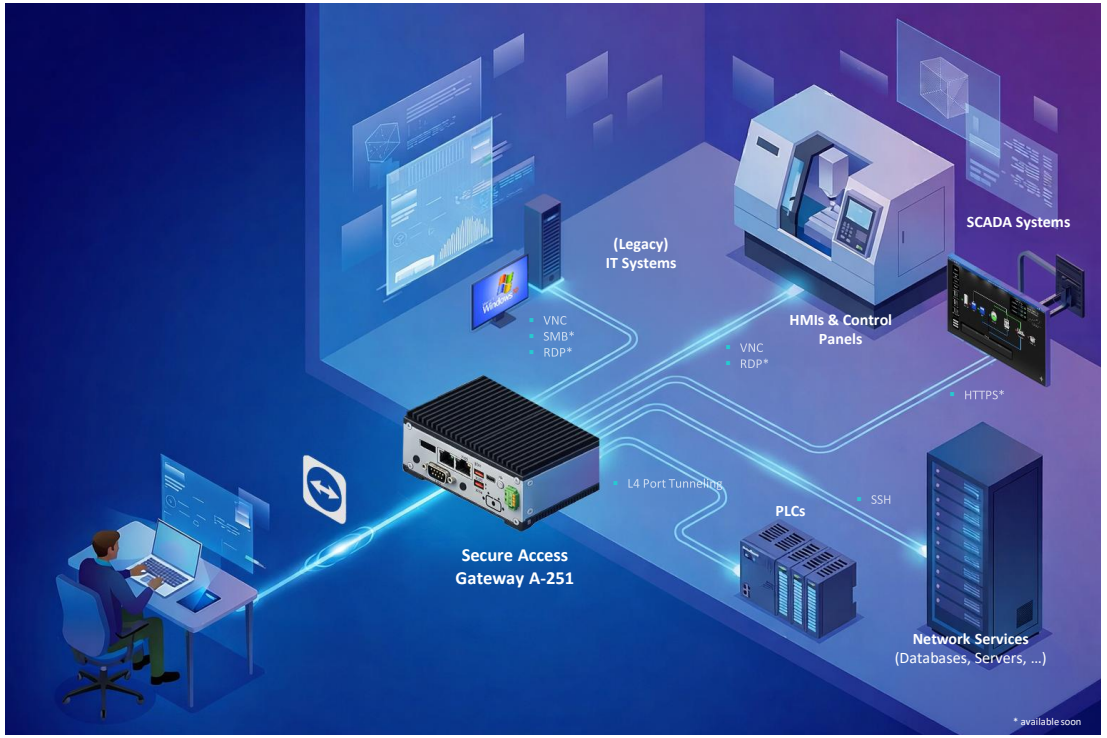
The collaboration between **Bechtle and TeamViewer** combines security, availability, and easy maintenance. By combining robust **edge gateway hardware, a secure and hardened Linux OS**, and **preconfigured TeamViewer Agentless Access**, secure and scalable remote access to industrial systems becomes quick and simple.

Your benefits with the Secure Access Gateway with preconfigured TeamViewer Agentless Access

- Maximum security thanks to a leading Zero-Trust solution ✓
- Fast deployment without complex implementation ✓Easy scalability for growing requirements ✓
- Seamless remote access – anytime and worldwide ✓

Bechtle Services

- Comprehensive consulting on OT data security
- Provision of TeamViewer software licenses
- Hardware procurement, pre-configuration and delivery
- Hardware commissioning, lifecycle and rollout management
- Strategic consulting for integrating IoT applications



If you have any questions or need advice, please feel free to contact:

Daniel Bossert – IoT / AIoT Solution Sales Consultant
daniel.bossert@bechtle.com, +49 170 290 3960

OT Network Isolation
Topology

TeamViewer Tensor OT enables zero-trust remote access in highly segmented network infrastructures, aligned with IEC 62443, to meet the highest security standards and support NIS-2 compliance.

Hybrid Conditional Access

On-premise deployable Hybrid Conditional Access allows implementing TeamViewer in highly secure segmented network infrastructures by maintaining isolation of all OT assets from direct cloud access. Hybrid CA acts as last-bastion for every TeamViewer remote access network traffic into the OT zone.

Agentless Access Gateway

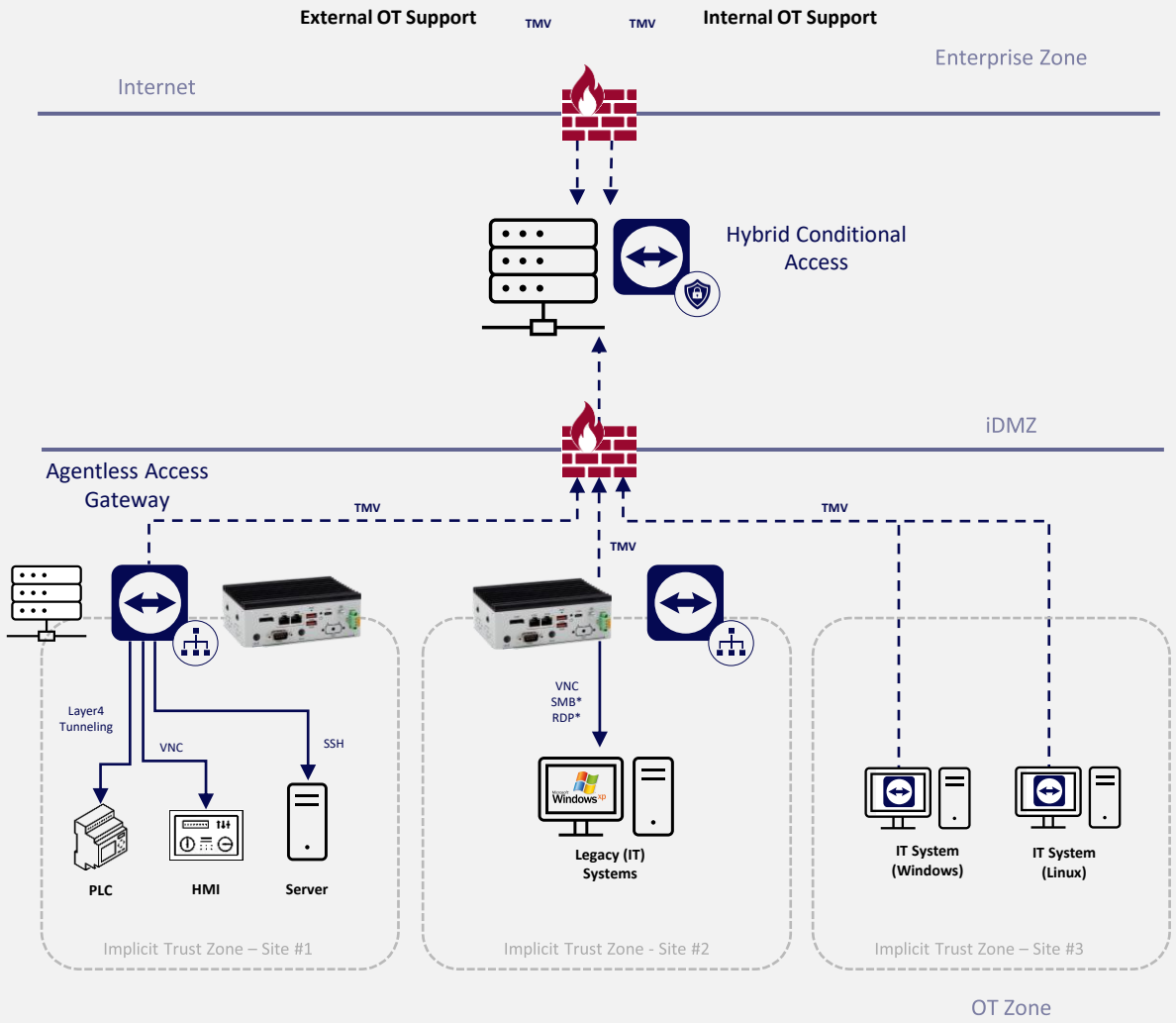
Agentless Access offers the ability to use TeamViewer Tensor for zero-trust network access and to control access to any OT asset (such as PLCs, HMIs, legacy IT systems, …) without the need to install TeamViewer Host on these endpoints directly.

- Zero-Trust Network Access through point-to-point layer-4 tunneling
- Remote Protocol Isolation through native support of VNC, SSH, SMB*, RDP*, HTTPS*
- Hardware offering (Secure Access Gateway) by Bechtle


Secure Access Gateway A-251: Gateway hardware with Agentless Access pre-configured


Supporter: TeamViewer Full-Client installed / WebClient used


Remote IT Device: TeamViewer Host installed on device



If you have any questions or need advice, please feel free to contact:

Daniel Bossert – IoT / AIoT Solution Sales Consultant
daniel.bossert@bechtle.com, +49 170 290 3960

Secure Access Gateway
With preconfigured TeamViewer Agentless Access

TeamViewer Tensor

TeamViewer Tensor is an all-in-one platform for secure, flexible, and integrable IT and OT remote access.

Zero-Trust-Security
The platform is based on a holistic Zero-Trust architecture and protects every connection through: End-to-end encryption, SSO, 2FA, conditional access, RBAC, BYOC, audit logging, cloud session recording, servers located in Austria and Germany.

Granular access control is ensured using conditional-access rules, security policies, as well as supervised and unsupervised access.

Optimized for OT environments
TeamViewer Tensor for OT is designed for complex OT infrastructures and enables direct, controlled access to proprietary or closed OT endpoints without installing additional software. Native support for numerous protocols such as VNC, SSH, SMB*, RDP*, and HTTPS*, combined with remote protocol isolation, enables secure access even to legacy systems. The solution is flexibly scalable — from individual machines to global industrial sites.

Compliance & Certificates
SOC 2 & 3, ISO 27001, ISO 9001, BSI C5, CSA STAR, NIST SP 800-53, NIS2, TISAX, HIPAA, DCB 129, IEC 62443*

*comming soon

Price on request

Secure Access Gateway A-251

Compact access gateway for secure Zero-Trust network access. Designed for 24/7 operation

Operating system and security
Kontron OS (secure, hardened Linux-based OS)
TeamViewer Agentless Access preconfigured
Secure Boot / HAB and encrypted OS partition
Stateful inspection firewall
All connections encrypted;
separation of OS and applications



Update & fail-safe mechanism
Redundant bootloader and OS partition
Encrypted OTA or offline updatesDelta updates for low bandwidth
Automatic fallback process
Signature verification for all updates (bootloader, OS, applications)

Interfaces
Graphic interfaces 1xDisplayPort
USB: 2× USB 3.2 Type A, 1× USB-C with USB + DP signals (DP Alt-Mode)
Ethernet: 2× 2.5 GbE Intel I226-V/IT
Serial: 1× RS232 COM port

Device properties
Fanless cooling
Operating temperature: 0 °C to +60 °C (32 °F to 140 °F) standard, −40 °C to +60 °C (-40 °F to 140 °F) extended
Housing:
- Steel housing; DIN rail mounting or rugged DIN RAIL
- Dimensions: 137 × 50 × 95 mm, Weight: approx. 1,0 kg

Certificates
CE, UL 61010-1, CB, FCC, UKCA

Price on request

If you have any questions or would like a consultation, please feel free to contact us:

Daniel Bossert – IoT / AIoT Solution Sales Consultant
daniel.bossert@bechtle.com, +49 170 290 3960

Bechtle Gateway for TeamViewer OT Remote Access
Bechtle Gateway Services

Bechtle Standard – Services for the Secure Access Gateway

Configuration and remote commissioning

- Initial configuration
- Inclusion in monitoring and monitoring

Monitoring and Event Management

- Monitoring of the gateway(s)
- Categorization and prioritization of events
- Creating Bechtle's internal incidents

Release and development management

- Release evaluation and testing and the Bechtle environment
- Release rollout after testing within the service period

Incident Management

- Informing the customer by e-mail

Vulnerability Management

- Informing the customer and updating the gateway(s) when a vulnerability becomes known

Your benefits with Bechtle IoT Services

We offer everything from a single source. Clear responsibilities minimise complexity. Relief of your internal resources and transparent billing models



Price on request *

*per month and device, services 5x8, incl. remote setup

If you have any questions or need advice, please feel free to contact:

Daniel Bossert – IoT / AIoT Solution Sales Consultant
daniel.bossert@bechtle.com, +49 170 290 3960

Contact Person
Do you have any questions?



Daniel Bossert

Solution Sales Consultant Managed AIoT / IoT

- Dipl.-Ing. (FH), MBA
- Responsible for the development and expansion of the Managed IoT business unit
- Management experience, co-founder and expertise in digitalization with a focus on discrete manufacturing and intralogistics (mechanical engineering, automotive)
- +10 years of IoT experience (business models, sensor technology, connectivity, platforms, open ecosystems, Auto-ID)
- Consulting of value-adding IoT End2End solutions including professional life cycle management

+49 170 2903960

daniel.bossert@bechtle.com