In cooperation with genua.

T Security

Secure Remote Maintenance

with Magenta Secure Industrial Remote Access Service (MSIRAS)

Connecting your world.

TABLE OF CONTENTS

Executive summary 3

The challenge: Cybersecurity in industrial environments 4

The solution: MSIRAS – combined expertise 6

The technical core: genubox and genucenter 8

A workflow example: Secure maintenance with remote access service 10

A comparison: MSIRAS vs. traditional VPN 11

Contact: Experts for better security 12

EXECUTIVE SUMMARY

Remote access for maintenance purposes is widespread across the manufacturing and process industries. As automation and digitalization advance, sites and systems have grown more complex. OEMs and third-party service providers are now seeing demand for remote maintenance rise. Cybercriminals are well aware of this. According to Germany's Federal Office for Information Security (BSI), intrusion through remote maintenance connections ranks among the most critical and most frequently observed threats to industrial security, and it's one that continues to grow.

Secure remote maintenance with MSIRAS

These threats are one reason the EU adopted the NIS2 Directive to strengthen cybersecurity. The directive entered into force in early 2026. NIS2, combined with the growing impact of cybercrime, is driving demand for secure remote maintenance and the managed services that accompany it. Magenta Secure Industrial Remote Access Service (MSIRAS for short) is designed to meet this need. Deutsche Telekom Security GmbH and genua GmbH have pooled their expertise to create a trusted, end-to-end solution that's made in Germany.

What makes MSIRAS stand out

- The highly secure **remote maintenance solution genubox**, which is purpose-built for industrial use, together with the central management solution genucenter
- A trusted **virtual private cloud (VPC) hosted in Germany**
- Comprehensive **managed security services**
- A high degree of **sovereignty**: hardware, software, encryption, and operations all come from Germany

MSIRAS delivers secure remote maintenance access by combining expertise, hardware, software, and a dedicated virtualization environment for every customer. The solution comprises the genubox rendezvous servers from genua with the associated genucenter central management system and a virtual private cloud (VPC) hosted in T Cloud Public.

The VPC is completely isolated from other tenant instances within the cloud. The genubox rendezvous architecture ensures that only authenticated users can reach pre-specified services and target systems. Access is further restricted to an agreed time with a defined duration and limited to a specified portion of the OT environment (for instance, a single machine). genubox enforces these restrictions by using a granular and advanced roles and permissions system, making MSIRAS well suited for everything from fine-grained access control to full Zero Trust implementations. The solution supports SIEM integration, offers logging capabilities, and includes a video recording function that provides auditable documentation of all maintenance activities.

genubox-based MSIRAS supports users in managing remote maintenance access with full central control over maintenance actions, access timing, target systems, and the accessing entity. Depending on requirements, operators can either fully outsource the remote maintenance solution to Deutsche Telekom Security or, within a shared management model, assume partial responsibility via a separate management tunnel.

[1] See also SANS Five Critical Controls for ICS: https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

The challenge

CYBERSECURITY IN INDUSTRIAL ENVIRONMENTS

Take back control and maintain sovereignty

Deutsche Telekom Security GmbH and Munich-based genua GmbH now offer a jointly developed security solution called MSIRAS to German industrial businesses.

75% of companies surveyed by the German digital industry association Bitkom have already fallen victim to digital theft of business data. Well over two-thirds have experienced digital sabotage, and 60% have had emails intercepted or other communications spied on. The economic damage amounts to 267 billion euros a year. That's money no longer available for innovation, maintenance, and training.

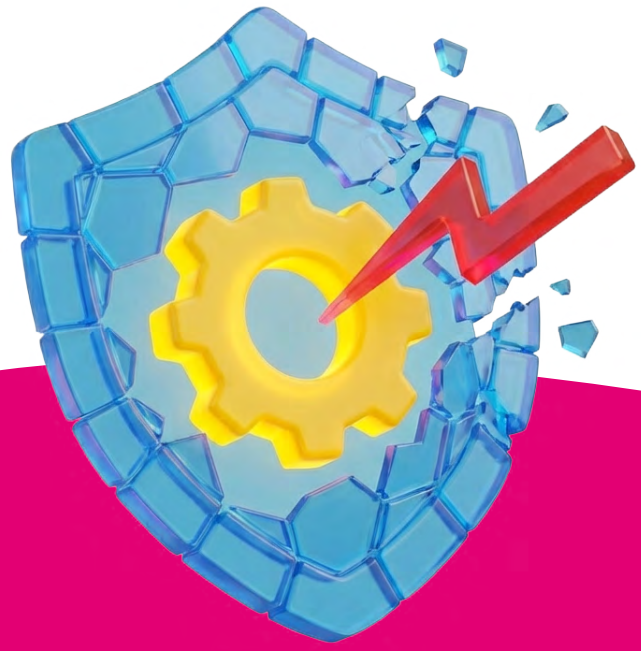
Countless organizations across industry and government are affected. All the while, the odds are shifting in the attackers' favor: Automation, digitalization, and networked (I)IoT continue to expand, and almost all machinery and measurement equipment now ships with a network connection. Meanwhile, AI tools allow attackers to mount successful attacks with ever less specialized knowledge. These attacks also rely less on malware and more on legitimate engineering tools, a shift that makes detection much more difficult.

A look at the factory floor shows why this matters. Operations and business managers must keep optimizing their processes and, above all, keep everything running around the clock. The result: factory systems are becoming more complex. Manufacturers are digitalizing and deploying automation to offset skills shortages and keep costs under control. Take predictive maintenance as an example: to minimize downtime, intelligent software is monitoring more equipment and calling for service before an imminent failure occurs. The sheer complexity of modern equipment increasingly requires the manufacturer's own technicians even for routine maintenance, security updates, fault alerts, or defective components.

Achieve rapid maintenance with remote access

Specialists are in short supply. They often need elevated access to industrial systems from outside to quickly analyze and resolve problems without travelling to the site. A technician can, for instance, resolve many faults by changing a setting or applying a firmware update. For more complex issues, remote diagnostics can enhance efficiency by enabling preparation before maintenance, for example by allowing replacement parts to be ordered in advance. Many manufacturers now offer their own solutions and service plans. Pay-per-use or equipment-as-a-service models also require external access to the machine and production system, for example via an IoT platform.

If detailed process data and device parameters are sent to an external AI for analysis (an open-loop scenario), the data must be protected against theft and unauthorized manipulation. This presents operators with an additional challenge: with so many different suppliers, it is practically impossible to evaluate every external remote maintenance system and monitor its security standards. Each individual vendor would have to be audited at regular intervals. Is the solution carefully configured? Is it updated and monitored on a regular basis? Is remote maintenance access restricted, and is all data encrypted in transit? Given the security landscape described above, the answer to every one of these questions should be yes.



Phishing attacks open the door

Many attacks on OT assets do take an indirect route through the company's IT systems. But remote maintenance connections are also a frequent initial attack vector. Especially when poorly monitored or unmonitored legacy stopgaps are in place and running around the clock . These frequently appear as unrestricted VPN tunnels that sit on the IT or OT network, often set up hastily when equipment goes down to resolve the fault with external help as quickly as possible. Phishing is not the only threat. Insecure remote access points also serve as entry routes through infected engineering workstations, laptops, or portable storage devices. Experts are also seeing supply chain attacks in which criminals first compromise a third-party provider's software and use that stepping stone to reach the actual production system.

The bad news is, these attacks are getting more sophisticated, and criminals continue to learn. Architectures, control logic, and naming conventions are no longer confined to trusted insiders. Artificial intelligence is unfortunately helping to orchestrate ever more complex attacks and compensate for a lack of OT expertise. It is also well documented by now that hostile state actors are backing attacks with personnel and resources, a practice now known as cyber warfare. Cybersecurity for production and critical infrastructure has therefore never been more important.

Preparing for NIS2 compliance

- *Check whether the organization falls under NIS2 scope*
- *Clarify responsibilities and ownership internally*
- *Review (or have reviewed) cybersecurity measures for gaps*
- *Establish processes for incident detection and reporting*
- *Vet and secure external service providers*
- *Prepare a line of contact with the supervisory authority (e.g. BSI)*

The European Union has recognized this, mandating the protection of critical infrastructure in its NIS2 directive, which seeks to achieve a high level of cybersecurity across the EU. Since October 2024, companies and organizations in the energy, water, transport, health, banking, and digital infrastructure sectors in the EU must comply with minimum cybersecurity standards. Penalties for non-compliance are severe and include fines of up to 10 million euros or 2% of annual revenues and even personal liability for senior management.

To protect companies in Europe and beyond from expense and disruption, Deutsche Telekom Security (DTS) now offers a managed service for industrial remote maintenance based on technology from genua, the Magenta Secure Industrial Remote Access Service (MSIRAS). This white paper describes how MSIRAS works: at its core is the genubox, which ensures that only authorized personnel can access sensitive industrial networks. genubox was developed in Germany and purpose-built for industrial environments. It fulfills all recommendations issued by Germany's Federal Office for Information Security (BSI) for secure remote maintenance.

NIS2 sets explicit requirements for operators

Area	Requirements under NIS2
Risk management	Identification and protection of IT and OT systems
IT security technologies	Firewalls, access controls, encryption, backup, monitoring
Incident response	Procedures for responding to security incidents
Incident reporting	Initial report of serious cyber incidents within 24 hours
Business continuity	Contingency plans, recovery procedures
Supply chain security	Monitoring and controlling service provider and partner access
Governance	Management accountability, for instance via supervisory obligations
Documentation & audits	Demonstrable evidence of security measures

THE SOLUTION

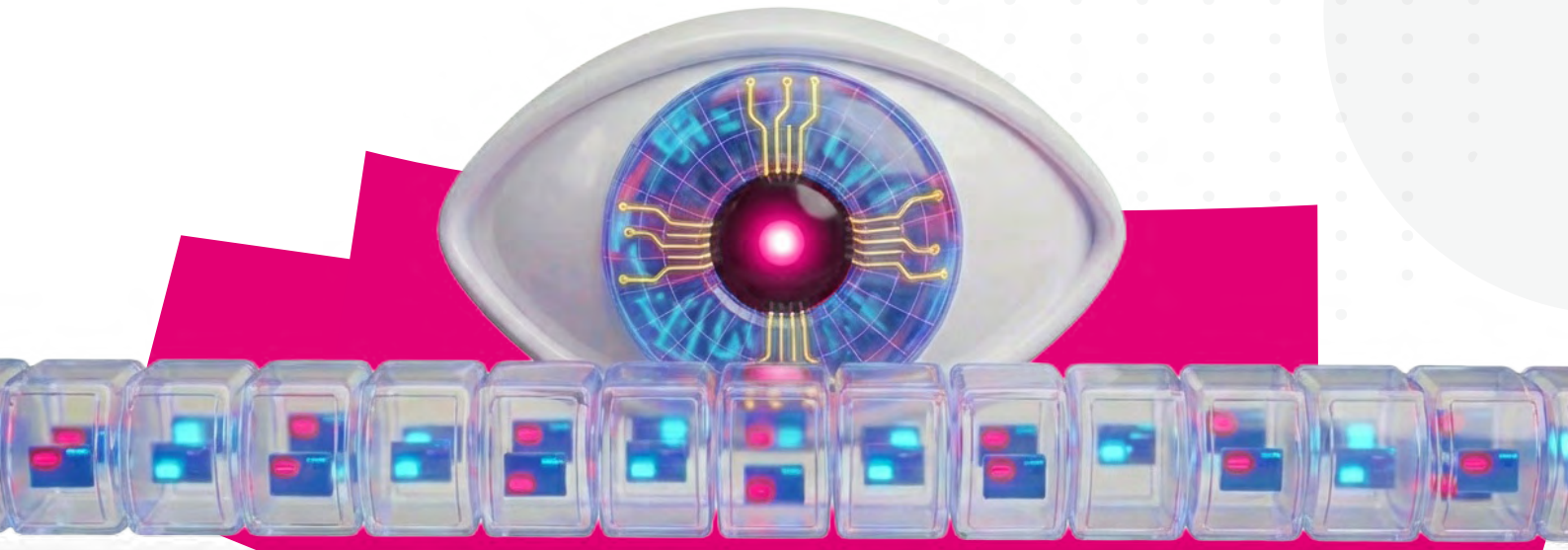
MSIRAS – combined expertise

The pillars of security

Cybersecurity is not a sprint. There are several pillars that any solution aiming to protect operations in the context of remote maintenance must rest upon. These pillars include multi-factor user authentication, granular access rights for every participant, and isolation of the maintenance target. Only necessary actions and only the sections of the site required to complete those actions should be accessible. Another key requirement shows why staying power matters; every activity during a remote session must be recorded in a way that is auditable and compliant with data protection policies. The pharmaceutical industry has practiced this for years, and other critical infrastructure sectors are now following suit.

There is also the question of legacy clean-up. Operators should make it a priority to identify unused or makeshift access pathways and systematically migrate them to a compliant solution. These legacy entry points must be sealed off as soon as possible. Forgotten access mechanisms frequently offer an initial entry point for attacks.

Especially in critical infrastructure sectors, businesses can no longer afford to treat cybersecurity as anything less than a top priority. The risks are simply too high. And the threats are expanding. Experts predict a sharp rise in AI-driven and automated attack scenarios. The use of quantum computing for criminal purposes is also likely to increase.



BSI recommendations fulfilled

Faced with the potential damage from cyberattacks and the penalties that regulations like NIS2 can impose, many companies are choosing the highly secure remote maintenance solution genubox. The IT security specialists at genua GmbH (part of the Bundesdruckerei Group) developed the solution especially for industrial environments. Together with genucenter, which acts as a control center for a network of security appliances, genubox fulfills all BSI recommendations for secure remote maintenance. Both products are available as virtual machines for deployment in an organization's own data center or in cloud environments.

Operators who also want expert support for planning, deployment, migration from legacy solutions, and day-to-day operations can now turn to the new managed service package for secure industrial remote maintenance (industrial RAS). It combines genua's secure remote maintenance solutions with managed services from Deutsche Telekom Security GmbH.

MSIRAS scope of services

Magenta Secure Industrial Remote Access Service (MSIRAS) deploys dedicated, virtual genua components for each customer in a Deutsche Telekom data center in Germany. This VPC instance meets the highest data protection standards and guarantees GDPR-compliant security, free from non-European influence. Geo-redundant data centers, top-tier availability standards, and regular independent audits ensure maximum operational reliability.

The MSIRAS managed service also covers all the typical project phases:

- Sales and presales: Specialists describe what a solution might look like, develop a solution outline, and recommend the appropriate scope of services.
- Proof of concept: Customers can trial the solution at a pilot site.
- Planning: The project management team sets up the integration during this phase.
- Installation: Deutsche Telekom specialists handle configuration, cloud deployment, and on-site installation.
- Customers can choose between two service levels
  - S72 offers an appointment within eight hours and a resolution window of 72 hours, equating to 99.17% annual availability.
  - For even faster response times, the round-the-clock S24 service level offers appointments scheduled within two hours and a resolution window of 24 hours. That equates to 99.72% annual availability.

> ***MSIRAS allows companies to quickly establish secure, compliant remote maintenance with infrastructure operated completely by Deutsche Telekom all the way from the cloud through to their on-site interfaces.***

- Markus Maier, Product Owner
Industrial Products at genua

The technical core

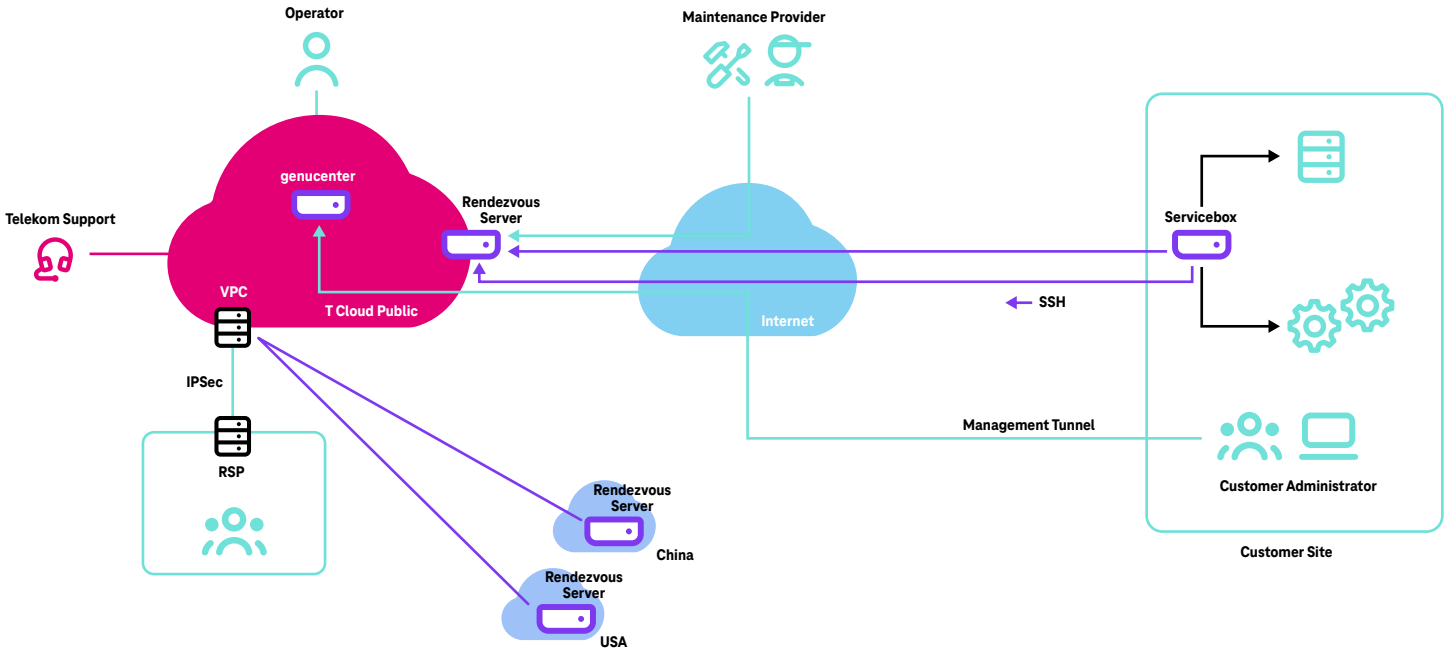
GENUBOX AND GENUCENTER

Roles within MSIRAS are clearly defined. Deutsche Telekom Security and its more than 1,800 security specialists supports customers as needed throughout the remote access lifecycle. That includes high-level architectural planning, site readiness assessments, integration planning, migration, and ongoing operations including CERT management and monitoring.

genua's rendezvous solution forms the technical core and prevents external maintenance providers from obtaining unilateral access. Every connection into the operations environment for analysis or maintenance must pass through a rendezvous server deployed inside a demilitarized zone (DMZ). The service technician and a responsible party on the operator side each build a connection to this meeting point. This approval step creates the end-to-end link that allows maintenance data to flow. The engineer can then read machine data and error messages and take action. Throughout, access stays limited in both time and scope. The external service may only operate within the pre-defined role and only on the target system. genua uses the robust SSH protocol to ensure that communications are secure.

Security by design

Prevention is better than remediation. That's why genua follows a security-by-design approach. The secure architecture together with all associated workflows, behavioral rules, and operating procedures is defined during the initial design phase and embedded in every aspect of the subsequent development. The result is a unified framework of technical safeguards and organizational processes that catches potential vulnerabilities early. Systems run reliably and are built to last; risks are minimized and data stays protected.



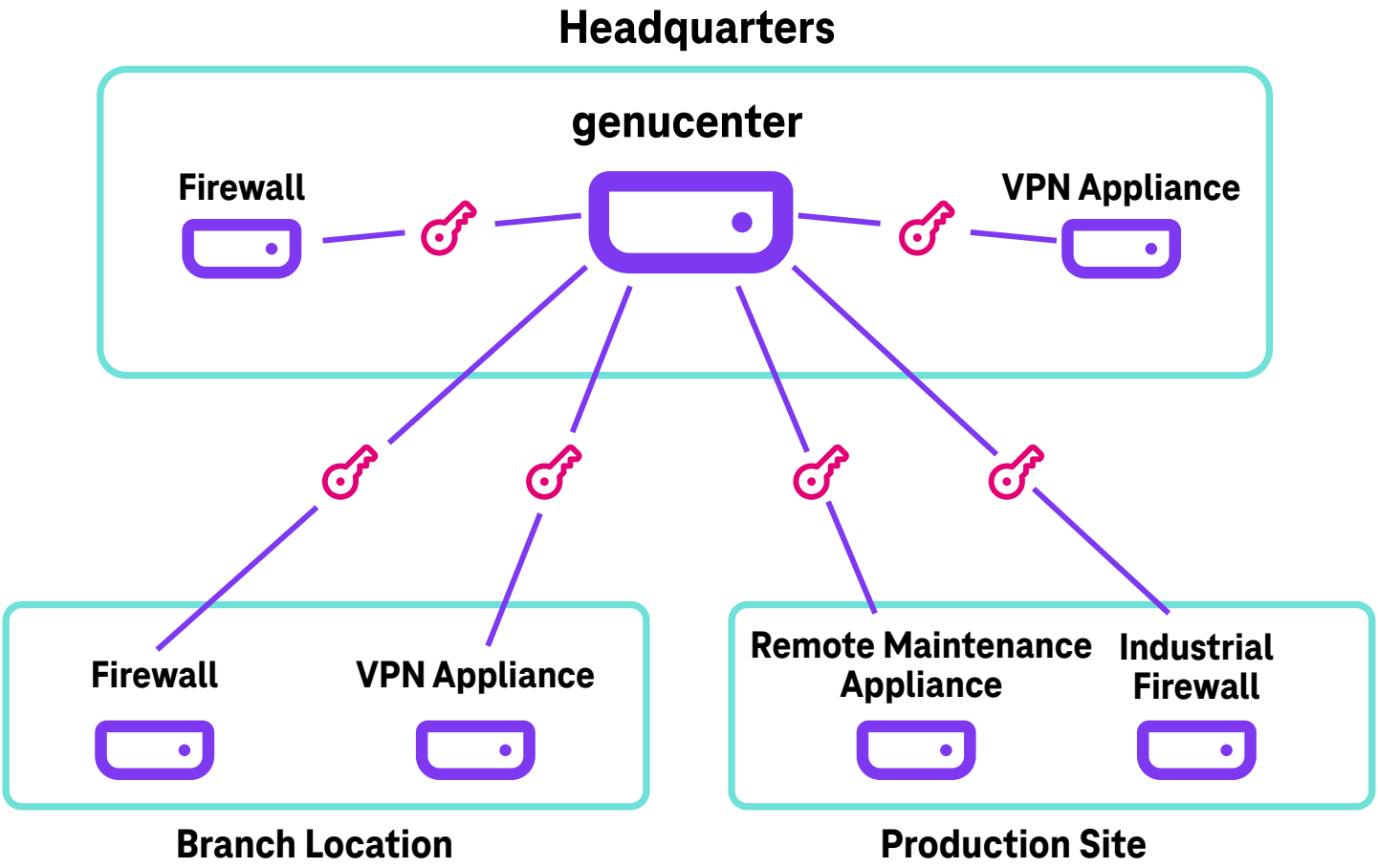
Schematic workflow of a remote maintenance session: Following approval by the operator, the maintenance provider can use the service box on the rendezvous server to access the machine.

Depicting complex structures clearly

The central management platform genucenter functions as the control hub within MSIRAS. It provides a clear picture of the system and enables efficient, secure management of the platform's complex technical processes, such as distributing cryptographic keys or pushing a local firewall configuration to branch sites by using straightforward remote maintenance policies. Instead of configuring each device individually, you can roll out updates, adjust settings, monitor devices, detect faults, and generate reports from a single location.

The hierarchical management capability in genucenter is one of its key features. genucenter provides a granular representation of even the most complex networks. The permissions structure mirrors the organization chart, from corporate headquarters down to individual departments at different sites. Separate user rights can be defined for different areas, for example which engineering role has access to which OT assets, and at what times.

Alternatively, you can group systems in a tree structure and simply let configurations inherit downwards. Organization-wide policies are also possible. Managing everything from one place makes it possible to consistently enforce even of complex policy frameworks without putting production at risk.



genucenter structure: Firewalls and access rights can be managed from a single console even for complex structures.

A WORKFLOW EXAMPLE

Secure maintenance with remote access service

A secure maintenance session always follows a set pattern. First, rights and responsibilities are clarified. Next, with the help of the secure remote maintenance app, the engineer uses the RAS service to establish an encrypted SSH tunnel to the rendezvous server over the internet. This virtual meeting point can be hosted in T Cloud Public, for example. The connection is encrypted and protected by two-factor authentication. Establishing the session using the native SSH protocol works as well, but the Windows app makes things simpler. The app helps both the maintenance provider and the operator to start, manage, and end the remote maintenance session.

Configurations for maintenance sessions take place in genucenter, the central management system, which also runs on T Cloud Public. To simplify things for users, genucenter supports sign-on via identity providers (IdPs) such as Microsoft Active Directory, Keycloak, Okta, or Azure AD. The IdP stores and manages user information, group memberships, roles, and permissions. After successful authentication, the IdP returns a confirmation, for example an OIDC token.

Alongside the software components in the VPC, MSIRAS also includes the genubox hardware (referred to in the diagram as the Servicebox), which is installed on the site's network for the systems that are to be maintained. Remote maintenance connections to the network or to the OT system being serviced terminate at this hardware.

Once the work is complete, or even during access, the operator can monitor the work by viewing video of all the actions that have been taken. If something goes wrong, access rights can be revoked at any point.

Comparison:

MSIRAS VS. TRADITIONAL VPN

Criterion	VPN connection (traditional, OpenVPN/IPSec etc.)	Magenta Secure Industrial RAS (MSIRAS)
Security level	Depends on configuration; open ports increase the attack surface	Very high, driven by the Zero Trust principle, connection-initiated communication, and genubox as a secure foundation
Connection setup	Manual or automatic, typically via public IP or dynamic DNS and port forwarding (which can pose a security risk)	Outbound only: no ports are opened; genubox, acting as the Rendezvous server, initiates the connection from the inside, so there is no inbound connection
Access control	Usually via username and password or certificates	Granular access control down to system, user, and time period; roles and permissions system
Auditability & logging	Limited or dependent on the VPN server	Seamless logging of all remote access sessions, auditable and GDPR-compliant
IT security integration	The operator's responsibility (firewall, updates, etc.)	Managed by Telekom Security including regular maintenance and updates
Industrial & OT compatibility	Often difficult in complex networks: since only the IP layer is tunneled (Layer 3), certain industrial protocols used for machine control, for example, do not work	Purpose-built for OT networks; also supports complex industrial protocols
Scalability	Yes, but labor-intensive, as certificates and user profiles must be created and maintained	Central management, multi-tenant architecture, easy to scale across large numbers of users and sites
Access approval	Often permanent access	Operators can grant temporary access approvals
Endpoint requirements	VPN client required	Web-based access possible; additional clients as needed (e.g. for machine manufacturers)
Hosting and operations	Can run on-premises hardware or in the cloud. When self-hosted, the operator is responsible for installation, updates, user management, security configuration, and monitoring/maintenance	Hosted in Deutsche Telekom data centers, multi-tenant, easy to scale via central management, 24/7 expert support
Cost model	Low license costs but high internal resource utilization	Monthly or annual plans, service-based, reduces internal IT costs

SECURE YOUR SUCCESS

MSIRAS helps you build remote maintenance that complies with critical infrastructure and NIS2 requirements. genua GmbH and Deutsche Telekom Security GmbH have combined their expertise here to deliver a full security package.

Your benefits at a glance

- Remote access, VPN, and firewalling in a single solution
- Central management with complete, real-time control over maintenance tasks, access time, target system, and accessing party
- High operational reliability through inbound connection confirmation for instance with a Windows app or key switch (via volt-free contact on the genubox)
- Security level adjustable to requirements spanning everything from open, continuous access to full control
- Sophisticated, corporate-ready role and permissions system for hundreds of remote service providers worldwide
- Maximum security and control through port-level access to the target system, isolated from the wider OT environment, with a rendezvous point in the DMZ or in the cloud
- Video recording and logging
- Trusted virtual private cloud (VPC) hosted in Germany
- Support for planning, integration, migration, and operations including CERT management
- Comprehensive managed security services: configuration of the remote maintenance solution can be fully outsourced to Deutsche Telekom Security

> *In 2025, more security incidents in production environments were caused by poorly implemented or inadequately monitored remote access than by ransomware attacks. Yet robust, proven solution architectures for secure remote access have been established for years. The problem is not a technical one — we need to focus more closely on the organizational side.*
>
> - Bernd Jäger, Practice Lead Industrial & IoT Security, Deutsche Telekom

Choose secure remote maintenance

Our experts are here to advise you on implementing secure remote maintenance. More information on OT security is waiting for you here.

Contact
security.dialog@telekom.de
security.telekom.de

Publisher
Deutsche Telekom Security GmbH
Office Port 1
Friedrich-Ebert-Allee 71–77
53113 Bonn, Germany

Connecting your world.

Deutsche Telekom Security GmbH | 03/2026