Rohde & Schwarz Cybersecurity

YOUR TRUSTWORTHY IT SECURITY SPECIALIST

We provide protection against the constant changing cyber threats to governmental and commercial customers with special IT security needs and certification requirements.

As pioneer of highly secure encryption technologies we deliver high-speed network encryption, zero trust based endpoint security and innovative data protection solutions for cloud environments. The majority of these products is approved for securing “classified information – for official use only” by the German Federal Office for Information Security. These trusted security solutions support users along their way into a secure and digitalized world and thus make a significant contribution to digital sovereignty.

Rohde & Schwarz Cybersecurity is a subsidiary of the technology group Rohde & Schwarz, a leading supplier of solutions in test & measurement, technology systems and networks & cybersecurity.
ENCRYPTION OF GOVERNMENT NETWORKS

For government agencies, it is essential to secure digital communications - to maintain data privacy, protect sensitive information and meet regulatory requirements. This is where high-speed network encryptors come in, ensuring that confidential data is encrypted end-to-end in real time as it is transmitted over a computer network. The data is only encrypted during transmission, so it is unencrypted at both the sender and receiver.

With over 30 years of cryptographic expertise, Rohde & Schwarz Cybersecurity is one of the pioneers in the field of high-speed network encryption. Our Layer 2 and Layer 3 encryption solutions securely protect public authorities from espionage and manipulation and ensure reliable and secure site-to-site connections.

Your benefits:

- „Security Made in Germany“ – more than 30 years of cryptographic expertise
- State-of-the-art cryptographic methods and standards
- Approved by the German Federal Office for Information Security: VS-NfD (RESTRICTED), EU & NATO RESTRICTED
PROTECTION OF CLASSIFIED WORKSTATIONS

When classified information is processed using IT systems, cybersecurity becomes directly relevant. Depending on the level of classification, authorities must take protective measures to ensure the availability, integrity and confidentiality of classified information. These include technical and organizational measures such as access control, data deletion and destruction, and data backup.

With our cybersecurity software products, developed in Germany and approved by the German Federal Office for Information Security (BSI) for securing classified data, we enable public institutions and private companies to secure workstations in such a way that classified information can be stored and processed.

Our solutions for secure mobile and stationary work have been developed with special attention to usability and administrability, and allow high flexibility in the choice of end devices.

Your benefits:

► High-security for laptops und PCs
► Zero-trust-to-Windows approach
► Approved by the German Federal Office for Information Security: VS-NfD (RESTRICTED), EU & NATO RESTRICTED
SECURITY FOR AEROSPACE AND DEFENSE INDUSTRY

The protection of sensitive information is subject to various legal regulations on secrecy and requires special security precautions. In this context, the protection of secrets does not only come into play in public institutions. In the private sector, too, classified information is processed, for which regulations relevant to secrecy are mandatory.

Our solutions offer the highest level of IT security for companies subject to secrecy regulations by protecting data at classified level from the workplace through the network to the cloud. You thus benefit from secure interfaces and encrypted transmission paths to transfer classified data securely. The approvals granted by the German Federal Office for Information Security (BSI) are valid for the classification levels EU and NATO RESTRICTED.

Your benefits:

► Data protection from workplace via network to cloud
► Secure transmission of classified data
► Approved by the German Federal Office for Information Security: VS-NfD (RESTRICTED), EU & NATO RESTRICTED
SECURITY FOR CRITICAL INFRASTRUCTURES

IT security is of particular importance for operators of critical infrastructures, i.e. energy, water, waste management, food, health, transport and traffic, information technology and telecommunications, finance and insurance, government and administration, and media and culture.

Due to their importance to society and economy, critical infrastructure organizations and institutions are subject to comprehensive and strict guidelines. Ensuring data protection and data integrity is a top priority. This requires IT products that ensure availability, integrity, authenticity and confidentiality. We support operators of critical infrastructures in complying with the highest security standards and deliver solutions for optimal protection of the IT infrastructure.

Your benefits:

► Ensuring data protection and data integrity

► Optimal protection of the IT infrastructure

► Approved by the German Federal Office for Information Security: VS-NfD (RESTRICTED), EU & NATO RESTRICTED
GDPR COMPLIANT USE OF CLOUD SERVICES

Regulatory measures such as the General Data Protection Regulation (GDPR) place an obligation on companies and organizations to ensure comprehensive protection of the personal data they process in cloud platforms. In this regard, it is not enough to rely on the measures or promises of the cloud service providers.

So-called data exporters, i.e. any entity that transfers personal data to the sphere of influence of a third country, must check whether the European legal obligations can nevertheless be complied with and an adequate level of protection is guaranteed.

Our **Cloud Data Protection Gateway** offers a tailored solution for this: by **decoupling user data from the services of the cloud platforms**, users can continue to use their daily workflows in cloud applications, while the data to be protected is encrypted in compliance with the GDPR and stored in freely definable local or cloud-based data storage. The cloud service providers do not have access to the protected data at any time, effectively preventing third party access.

**Your benefits:**

- Decoupling of user data and GDPR compliant
- Effective prevention of third party access to protected data
- Confirmation of the legal security of our patented approach by a legal opinion
PROTECTION OF SENSITIVE DATA IN PUBLIC CLOUDS

Two aspects are crucial when it comes to protecting sensitive data: the location and type of data storage. With our Cloud Data Protection Gateway customers can ensure that their data is stored in exactly the places and regions where it is allowed to be located in compliance with data protection regulations. In addition, the data is encrypted at all times. The encryption methods correspond to the current state of the art and cannot be overcome by today’s means.

Data is also protected against future risks - with a method for the distributed storage of data. Each encrypted file is split into a definable number of data particles. These particles can then be stored in a distributed manner at different definable locations in the cloud or on-premises. This greatly reduces the risk of an attacker obtaining all parts of an encrypted file. However, as long as not all data particles of a file are accessible, it is mathematically impossible to gain access to the information even if the encryption process is broken.

Your benefits:

► Data protection compliant storage of data
► State-of-the-art cryptographic methods
► Future-proofing through methods for the distributed storage of data
LOCAL DATA COMPLIANCE FOR GLOBAL ORGANIZATIONS

Almost every day data protection regulations are being established and tightened around the world. Global corporations and organizations in particular must therefore ensure that they can keep pace with this extremely dynamic development and work worldwide in compliance with data protection regulations.

Our Cloud Data Protection Gateway makes it possible to store data that is not allowed to leave certain regions completely in these regions and to prevent access from other regions. Nevertheless, users can continue to collaborate in a centrally managed cloud service and use a shared infrastructure. This not only ensures data security and compliance with local data protection requirements, but can also avoid significant IT infrastructure costs by preventing regional duplication of work environments.

Your benefits:

► Effortless compliance with all international data protection regulations

► Data security and compliance with local data protection requirements

► Avoidance of significant IT infrastructure costs
Next generation encryption

**POST-QUANTUM CRYPTOGRAPHY AND QUANTUM KEY EXCHANGE**

Quantum computers promise to greatly expand the limits of computing efficiency, solving problems that today’s systems are overwhelmed with. As a result, they could render all current public key encryption methods insecure in the future.

IT security solutions must be oriented towards developments in the fields of post-quantum cryptography and quantum key exchange. That is why we are already researching today on how to protect against tomorrow’s threats. To drive this forward, Rohde & Schwarz Cybersecurity is making its cryptographic expertise and experience in building and implementing secure devices and systems available to numerous research projects.

**Selected research projects:**

- **DemoQuanDT:** Development and construction of a demonstrator route with trusted nodes between Bonn and Berlin.

- **OPENQKD:** A European project aiming at strengthening Europe’s global position at the forefront of quantum communication capabilities.

- **QNET:** Establishment of a pilot network for quantum communication in Germany, which is used for tap-proof and tamper-proof data transmission. Initially, the network is intended for communication between federal authorities.
At a glance

ROHDE & SCHWARZ CYBERSECURITY

► A leading provider of IT security solutions
► More than 30 years of cryptographic expertise
► Extensive project experience in the area of state and federal networks and classified workstations
► All-in-one solutions approved for securing classified data with a unified security management
► A company of the Rohde & Schwarz Group
  • Independent family business, in the market for over 85 years
  • Subsidiaries in more than 70 countries
  • Revenue of 2.28 billion € (FY 2020 / 2021)
  • Around 13,000 employees worldwide