Product Brochure Version 04.00

NETWORKS & CYBERSECURITY

Innovation for efficient, modern networks
and effective security

ROHDE&SCHWARZ
Make ideas real

STRIVING FOR A SAFER AND CONNECTED WORLD

With its leading technology solutions, Rohde & Schwarz enables companies and countries to define and keep their technological and digital sovereignty.

Innovation has been part of Rohde & Schwarz since the very beginning. The company founders Dr. Lothar Rohde und Dr. Hermann Schwarz were technological pioneers. With their hands-on entrepreneurial spirit, the two college friends entered the unexplored field of RF engineering with their two-man laboratory. Ninety years later, the privately owned, Munich based company has about 14.400 employees worldwide which in the 2023/2024 fiscal year achieved total revenues of EUR 2.93 billion.

With its Test & Measurement, Technology Systems, and Networks & Cybersecurity divisions, Rohde & Schwarz creates tomorrow's innovation today. The global technology group's leading-edge products and solutions empower industrial, regulatory, and military customers to attain technological and digital sovereignty.

With network, security, and encryption solutions, Rohde & Schwarz protects the digital information and business processes of companies and public institutions from the effects of cyber-attacks.

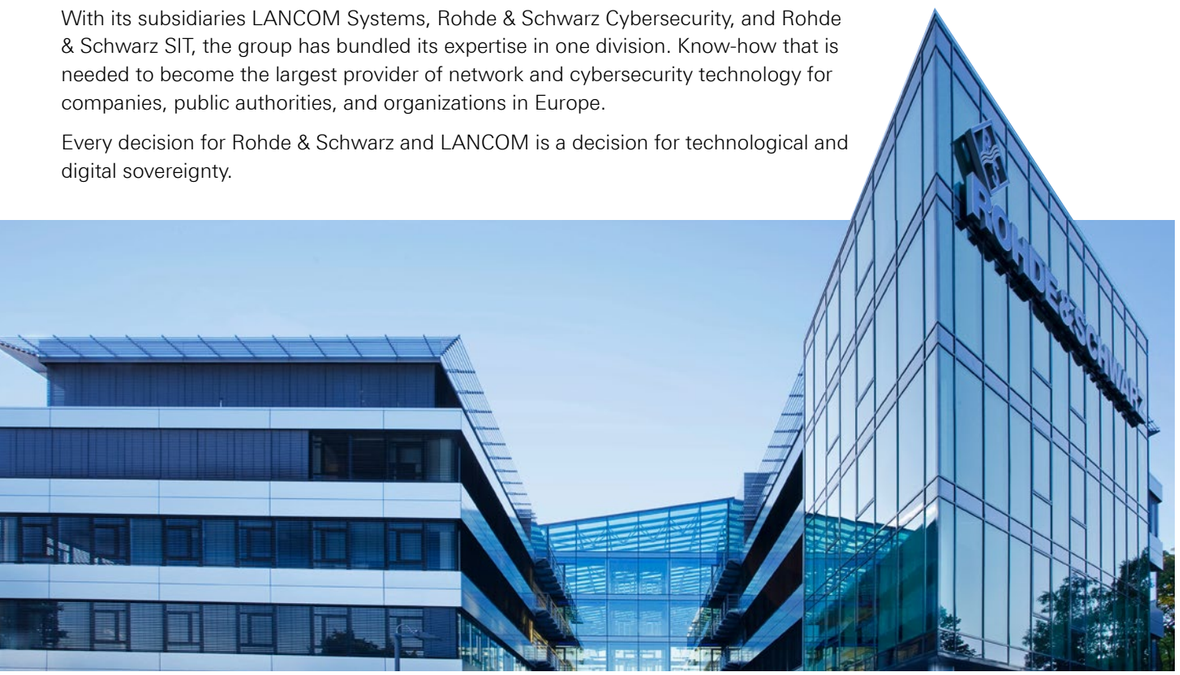
The volume of data is growing exponentially. At the same time, the potential threat to companies, public authorities, and critical infrastructures is increasing. According to the estimates of reliable organizations, cyberattacks like theft of intellectual property cost the global economy hundreds of billions of dollars each year. But intangible assets are not the only assets that need protection. The large quantities of sensitive public sector data as well as personal data generated by the private sector also need to be protected.

SecurITy made in EU

Trust Seal
www.teletrust.de/itsmie

With its subsidiaries LANCOM Systems, Rohde & Schwarz Cybersecurity, and Rohde & Schwarz SIT, the group has bundled its expertise in one division. Know-how that is needed to become the largest provider of network and cybersecurity technology for companies, public authorities, and organizations in Europe.

Every decision for Rohde & Schwarz and LANCOM is a decision for technological and digital sovereignty.



"Our network connectivity and cybersecurity solutions empower digital sovereignty for public and commercial customers. We provide security for mobile devices, laptops, and PCs through a comprehensive portfolio of high-speed encryption for data center networking, VPN solutions for securely networking distributed organizations, SD-WAN gateways, and UTM firewalls to secure IT perimeters, along with cloud-based network management."

Ralf Koenzen,
Executive Vice President Networks & Cybersecurity

Content Overview

ROHDE & SCHWARZ, NETWORKS & CYBERSECURITY

The Rohde & Schwarz Networks & Cybersecurity division provides endpoint security, secure networks, and high-quality cryptography. With products “Engineered in Germany”, we ensure trustworthy, reliable, and secure data transfer, specializing in the Public, Critical Infrastructures, Defense, Health, Retail, and SME verticals. We are the preferred supplier for the sustainable support of organizations, governments, and armed forces in the planning, deployment, operation, and optimization of their network and cybersecurity challenges.

4 Million
installed network-based devices

100,000
connected branches

>500
products

Highly secure cryptography for defense

Digital sovereignty

DIGITAL SOVEREIGNTY AS A STRATEGIC-POLITICAL TASK TO STRENGTHEN COMPETENCIES

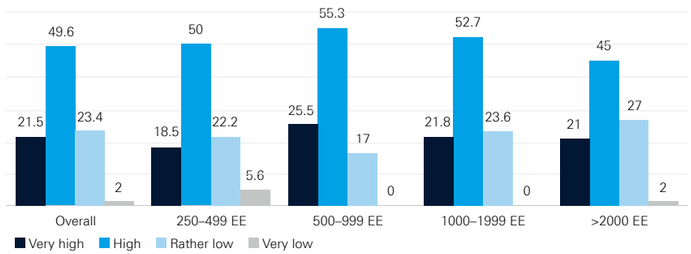
According to the German Federal Ministry for Economic Affairs and Climate Action (BMWK), "Digital sovereignty is an issue of great relevance. The supply bottlenecks of computer chips were a reminder of how quickly dependencies on non-European producers can slow down important economic sectors, such as the automotive industry."

We also see digitalization as an opportunity for Germany and Europe to strengthen their own competencies and cooperations. In this way, we can consolidate our position in technological areas. The BMWK explicitly sees a need for action in "...digital technologies such as network technologies, microelectronics, security technologies, quantum technologies, and blockchain." Here, European competencies are to be maintained and expanded.

We understand digital sovereignty as the ability to decide for ourselves what we do. This includes decision-making competence, the ability to act, and the ability to assess the risk posed by dependencies. According to the definition by bitkom, Germany's digital association, a digitally sovereign company is able to make self-determined and confident decisions between alternatives from competent and trustworthy partners.

This distinguishes digital sovereignty from digital dependency – a state that is probably not desirable for any company – and digital autarky. The latter is generally not feasible in our globalized world.

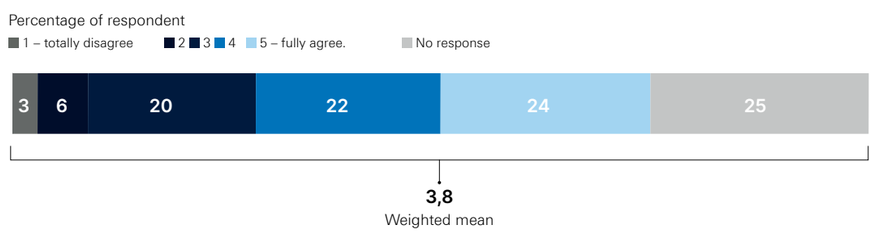
How important do you currently rate the topic of "digital sovereignty" in your company?



Source: Handelsblatt study, 032023, figures in %, 4-point scale, N/A not included in the chart

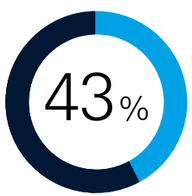
Study participants confirm the severity of the threat with a very high average score of 4.6. Yet, with an average score of only 3.8 for the use of EU-based security components, there is still clear room for improvement.

Intentionally choose security components from EU-based manufacturers



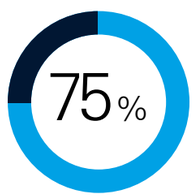
Source: LANCOM Systems / Behörden Spiegel – Quo vadis – The Digitalization of Public Administration in Eastern Germany

"The hardware we use comes from manufacturers in the EU."



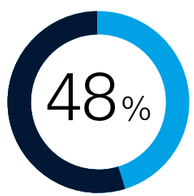
Hardware tends to be purchased from manufacturers outside the EU.
(■ = 3-6/Does not apply at all)

"In the event of failures, we can restore our processes independently or with the help of trusted partners."



The ability to restore IT processes independently in the event of failures is rated as high at 75%.
(■ = 1-2/Applies fully and completely)

"We are not reliant on external help to implement sufficient measures in terms of IT security precautions, skills training, and crisis management."



Dependence on external help for safety precautions, skills, crisis management.
(■ = 3-6/Does not apply at all)

Source: Handelsblatt study, 032023, figures in %, 6-point scale, K.A. not included in the chart, normalized to 100%

Built-in Security

IT SECURITY THAT PROTECTS BY DEFAULT.

Your network infrastructure is responsible for your business

Networks & Cybersecurity products are designed not only to work reliably, but also to meet the highest security requirements. The term "Built-in Security" encompasses all security mechanisms that are integrated into our routers, firewalls, switches, and access points as standard. This means that security, transparency, and traceability are built into every component and every release – engineered in Germany, guaranteed free of hidden backdoors, and digitally sovereign.

Every solution is responsible for the stability and integrity of your infrastructure – in companies as well as in government agencies and public institutions.

What does Built-in Security mean?

Networks & Cybersecurity products offer comprehensive security mechanisms. Built-in Security refers to this factory-integrated network security for every product.

Exemplary built-in security product features:

- → **Certification for tested trustworthiness by the German Federal Office for Information Security (BSI)**
- → **High availability through redundancy and cellular backup**
- → **R&S PACE2 DPI engine for comprehensive data inspection**
- → **IKEv2/IPSec VPN support for secure site networking**
- → **VS-NfD / EU-R / NATO-R**
- → **Complete full-disk encryption solution**

Your advantage in practice

The Built-in Security promise underlines a key principle in Networks & Cybersecurity: security is not an add-on, but a core element of every component. It signals at first glance that you can rely on digital sovereignty – tested, traceable, permanent.

- → **Secure operation: Plannable updates and high availability prevent downtime and follow-up costs.**
- → **Transparency & control: Proprietary operating systems and clear responsibilities create a verifiable security architecture.**
- → **Investment protection: Long-term maintenance and predictable updates extend the service life.**
- → **Remain digitally sovereign: Transparent development and control instead of external black boxes.**

ENGINEERED IN GERMANY

Engineered in Germany

Lifecycle management

DSGVO NIS2 BSI

BSI-Zertifizerung

Guaranteed backdoor-free

INNOVATION FOR EFFICIENT, MODERN NETWORKS AND EFFECTIVE SECURITY

LANCOM MANAGEMENT CLOUD

A fully functional network is the heart of any business. Building it up and controlling it, however, can be time-consuming and error-prone. In an IT world with increasing complexity and a widespread shortage of skilled workers, what your network needs is a reliable control center. Dynamically control all your network operations in the WAN, LAN, Wi-Fi, and security from a single cloud platform – as automated as you like.

CENTRAL-SITE SECURITY FOR LARGE SD-WAN SCENARIOS

A key aspect for very large-scale multi-service IP networks is performance and reliability at the central site. At the heart of your SD-WAN, a multi-Gigabit gateway like the LANCOM ISG-8000 provides security and high performance. A powerful platform with state-of-the-art encryption technologies, high-scalability VPN, and extensive redundancy features delivers a Software-Defined Wide Area Network (SD-WAN) that greatly simplifies your work in administration.

NETWORK ENCRYPTION FOR HIGHLY SECURE DIGITAL COMMUNICATION

Our network encryptors R&S®SITLine protect public and commercial customers from espionage and manipulation of data transmitted via Ethernet over fixed lines, radio links or satellite. They meet the diverse requirements of public institutions, companies and critical infrastructures, which can rely on specially developed, customized solutions.

HIGHLY SECURE COMMUNICATION WITH IPHONE AND IPAD

The R&S®ComSec solution, based on "Apple indigo," enables comfortable and secure work with classified data (VS-NfD) on iPhones and iPads without the need for containers, simplifying the daily work routine for users in security-critical environments.

At the same time, the R&S®ComSec solution guarantees secure private use on company-owned, personally enabled devices (COPE).

TRUSTED NETWORK SOLUTIONS FOR BUSINESS AND GOVERNMENT

Software and hardware development as well as manufacturing take place mainly in Germany, which also applies to the hosting of the network management (LANCOM Management Cloud). Particular attention is paid to providing trustworthy solutions with excellent security features. In addition, backdoor freedom is a key protective feature of the products. The trust mark “IT Security Made in Germany” and certification by the German Federal Office for Information Security (BSI) confirm the trustworthiness and the outstanding level of security.

CYBERSECURITY PRODUCTS FOR PUBLIC AND PRIVATE SECTOR CUSTOMERS

Rohde & Schwarz Cybersecurity products protect government and private-sector customers with special security and regulatory requirements from ever-changing cyber threats. We develop and manufacture high-security, high-speed network encryption and zero-trust endpoint security. Most of these award-winning products are approved by the German Federal Office for Information Security (BSI) for securing VS-NfD-rated data. The trusted security solutions help users on their way to a secure and digitalized world.

LANCOM switches

The LANCOM Gigabit Ethernet switch portfolio is the basis for modern network infrastructures in all industries and areas of application. There is a choice of custom-fit versions with Power over Ethernet (PoE) and ports in varying numbers for various throughput rates (1G, 2.5G, 10G, 25G, 40G, 50G, 100G), protocols and applications.

LANCOM routers & SD-WAN

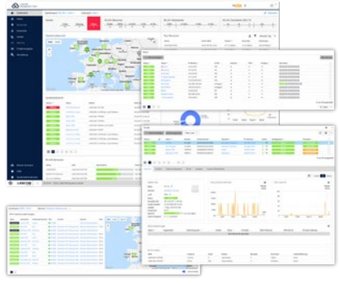
SD-WAN central site gateways guarantee high performance and reliability in the headquarters. LANCOM VPN routers ensure high bandwidths, secure communication, and confidential data exchange in professional networks.

LANCOM access points

LANCOM access points enable wireless network access in every conceivable environment – indoors, outdoors, or in harsh industrial environments. They meet the highest demands in terms of hardware quality (service life, temperature development, etc.) as well as the flexibility and security of the underlying software.

LANCOM Remote & Mobile Access

Provide secure and scalable access to corporate applications for employees in the office, at home, or on the road, protecting modern hybrid working from anywhere and anytime.



LANCOM Management Cloud

Controls, optimizes, and automates your entire network operation, greatly simplifying and streamlining workflows by eliminating manual individual device configurations.

LANCOM R&S®Unified Firewalls

Extensive unified threat management (UTM) in combination with machine learning offers the best protection against new types of viruses and malware. With these powerful firewalls and suitable accessories, you can expand your trusted network infrastructure based on next-generation Deep Packet Inspection Engine (R&S®PACE2).

R&S Network Encryption

Our network encryptors protect public and commercial customers from espionage and manipulation of data transmitted via Ethernet over landlines, radio links, or satellite. They meet the diverse requirements of public institutions, companies, and critical infrastructures, which can rely on specially developed, customized solutions.

R&S Central Security Management

A reliable security level requires simple and centralized control. This is precisely the function of the R&S®Trusted Objects Manager. It helps to easily set up and manage the specialized security products. It offers an intuitive user interface. Users can easily handle configuration, deployment, and monitoring. A modern REST API in the backend enables easy and quick integration into your central monitoring and reporting systems.

R&S®Trusted VPN

The IPSec-based Trusted VPN solution provides highly secure and remotely maintainable communication over public networks by leveraging centralized key management, TPM hardware security, and automated configuration – enabling secure connectivity between different sites.

R&S®ComSec

R&S®ComSec enables both convenient and secure work with sensitive data on iPhone and iPad, as well as separate personal use (COPE) of the devices. It simplifies daily work for users in authorities and security-critical environments.

R&S Endpoint Security

The transparent real-time encryption process guarantees maximum security without compromising user productivity in any way. Full disk encryption for Windows systems and external data carriers protects VS-NfD-rated user data, temporary files, and the entire operating system, especially against theft or sabotage.

R&S High-grade Crypto

The R&S®ELCRODAT 7-MC is a fully ruggedized tactical crypto device used to encrypt and decrypt voice and data communications for German, EU, and NATO security classifications up to SECRET.

FULL OPERATIONAL CAPABILITY – ANYTIME, ANYWHERE.

R&S®ComSec

- Combined private and professional use of iPhone and iPad – supporting data up to VS-NfD classification (COPE).
- Seamless access to native Apple apps for Mail, Calendar, and Contacts – without containers – provides a unified view of all information while ensuring secure data separation using per-app and per-account VPNs.
- Optionally expand functionality with approved apps from the BSI, business or personal applications, and custom in-house solutions.

Rohde & Schwarz Hardware and other components

R&S®Trusted Objects Manager
Hardware-based (backend) PKI infrastructure for certificate management and R&S®Trusted VPN Gateway (BSI approved) – a hardware-based Layer 3 gateway with encryption for VS-NfD or non-VS-NfD data.

iPhone and iPad
Hardware-based (frontend) infrastructure based on standard devices and operating systems from Apple, and Apple Business Manager – an Apple service for integrating mobile devices into an MDM service.

BSI-approved MDM server
Installs certificates from the R&S®Trusted Objects Manager onto Apple mobile devices (using the ACME protocol) – optionally as a bright-site or dark-site installation; integration into your existing system is possible without hardware replacement.

The BSI explicitly recommends allowing private use of company devices and confirms that eliminating container solutions is a viable and secure method of communication. Face ID and Touch ID are also approved.

SecurITy made in Germany

NETWORK ENCRYPTION

With over 30 years of crypto expertise, Rohde & Schwarz Cybersecurity is a pioneer in the field of network encryption with its hardware and software for network encryption. The company offers the entire value chain, guaranteeing highest levels of trust and reliability. Our network encryptors protect public and commercial customers from espionage and manipulation of data transmitted via Ethernet, over landlines, radio links, or satellite.

They meet the diverse requirements of public institutions, companies, and critical infrastructures, which can rely on specially developed, customized solutions.

Advantages of our network encryptors

- "IT Security Made in Germany" – over 30 years of crypto competence
- Custom hardware and software for market-leading encryption performance
- State-of-the-art cryptographic methods and standards
- High level of user-friendliness thanks to central security management system
- Approved by the German Federal Office for Information Security:

VS-NfD (RESTRICTED), EU & NATO RESTRICTED

R&S®SITLine ETH

Available in various performance classes, this modern hardware-software architecture combines with the latest cryptography to provide long-term and sustainable security for your infrastructure.

POWERFUL AND SECURE DATA TRANSMISSION

The integration of cyber security solutions in companies is an investment in the future viability and resilience of your organization. At Rohde & Schwarz Cybersecurity, we see IT security as an integral part of the value chain. This approach enables us to offer security solutions that not only ensure protection against cyber-attacks, but also support the smooth operation of your business processes – ensuring business continuity.

Our solutions are characterized by high performance combined with low latency. Our customers benefit from a combination of leading security technology and the knowledge that they can count on Rohde & Schwarz's competent, reliable service in the event of an incident or when technical support is required. Trust in the Rohde & Schwarz brand is based on decades of experience and a deep understanding of the cybersecurity requirements of various industries.

Ultimately, investing in Rohde & Schwarz Cybersecurity solutions not only enables protection against the increasingly complex threats in cyberspace, but also ensures the integrity and availability of your critical data and systems. This ensures that your organization can continue to operate successfully and securely in an increasingly connected and digitalized world.

CENTRAL SECURITY CONTROL

R&S®Trusted Objects Manager

A reliable security level requires simple and centralized control. This is precisely the function of the R&S®Trusted Objects Manager. It helps to easily set up and manage the specialized security products. With this system, IT administrators can access and control applications such as R&S®Trusted VPN, R&S®Trusted Disk, R&S®Trusted Identity Manager, and R&S®Trusted VPN Client. By installing a single instance of the R&S®Trusted Objects Manager, users can seamlessly manage all of these products, enabling scalability up to 50,000 clients. Compatibility with various LDAP directory services, including Microsoft Active Directory, Lotus Domino, Novell eDirectory, and OpenLDAP, ensures smooth integration into network environments of different sizes. Users and groups can be easily imported from existing LDAP structures. For increased reliability and resilience, additional R&S®Trusted Objects Managers can be integrated as standby instances – a supplementary scaling option depending on the required level of expansion.

THE SPECIAL FEATURES OF CENTRALIZED CONTROL WITH THE R&S®TRUSTED OBJECT MANAGER:

Intuitive operation of the manager

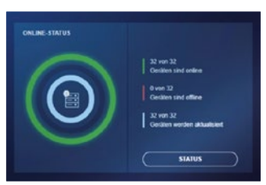
The R&S®Trusted Objects Manager is characterized by its user-friendly operation based on user processes and its flexibility in user and rights management. An IT administrator can manage the entire operating cycle of the Rohde & Schwarz Cybersecurity components via a secure web interface. In addition, the optional, integrated PKI offers the advantage that you can operate it autonomously and independently of third-party providers.

Maximum security thanks to an optional public key infrastructure (PKI)

Optionally, a public key infrastructure (PKI) can be integrated via the R&S®Trusted Objects Manager – a security component for greater confidentiality, integrity, and authenticity of data. The public key infrastructure (PKI) can be set up and operated under your own control, without third parties. R&S Cybersecurity is available to provide support for the setup.

VS-NfD, EU & NATO RESTRICTED-ready

The R&S®Trusted Objects Managers are certified by the German Federal Office for Information Security (BSI) and are authorized to process VS-NfD, EU & NATO RESTRICTED data. This enables public institutions and private companies to secure their workstations and mobile storage devices in such a way that they can store and process VS-NfD classified information.



The effectiveness of a protected environment depends directly on how efficiently the control over the respective components is integrated into the processes. An R&S®Trusted Objects Manager is the daily digital assistant for easy and secure management of R&S security components. Based on the operating process, the focus is on intuitive use of the central control unit. Especially when it comes to significantly reducing process complexity and eliminating sources of error.

Engineered in Germany

HIGHLY SECURE HARD DRIVE ENCRYPTION

R&S®Trusted Disk: BSI-certified hard drive encryption.

The solution provides protection against unauthorized access to classified data – "Nur für den Dienstgebrauch", EU Restricted and NATO Restricted – on powered-down devices, in the event of loss, theft or maintenance.

Highest level of security for Windows-based endpoints.

- ► Laptops, tablets, and desktop PCs
- ► PCs installed in police and military vehicles
- ► External USB data storage devices connected to them
- ► Windows servers

Highest security for sensitive data

- ► Full encryption of internal and external storage devices
- ► Automatic re-encryption in the event of security-critical events.
- ► Secure boot process
- ► Two-factor pre-boot authentication.
- ► Stealth mode can conceal the use of encryption

User-friendly administration

- ► Easy deployment to a large number of devices with automated initialization
- ► User productivity is not affected, as encryption runs in the background
- ► Maintenance mode enables unattended restarts
- ► Support for data recovery scenarios

Centralized management

- ► Enterprise-grade remote management of endpoints, users, smartcards, groups, and permissions
- ► Integration with LDAP directory services, e.g., Active Directory
- ► Required device and user certificates can be generated using the integrated PKI and easily managed throughout their lifecycle

VS-NfD, EU RESTRICTED, NATO RESTRICTED

VALUE FOR BUSINESSES

- ► Maximum data security and easy administration
- ► Scalable solution for organizations with high security requirements
- ► Centrally enforced security policies and effective operational monitoring

HIGH-GRADE CRYPTO SOLUTION

Ruggedized HF/VHF/UHF/IP security for voice and data

The R&S®ELCRODAT 7-MC is a fully ruggedized tactical crypto device used to encrypt and decrypt voice and data communications for German, EU, and NATO security classifications up to SECRET. TEMPEST-proof, it is interoperable with HF/VHF/UHF radio, satellite communications, line transmission equipment, and IP infrastructure. It is perfectly suited for deployment on stationary and mobile platforms in rugged terrain and in naval and airborne environments.

KEY FACTS OF THE SOLUTION

- ► Protects HF/VHF/UHF satellite communications and line transmission
- ► Supports IP encryption protocols such as NINE and SCIP
- ► Data rates up to 1 Gbps
- ► Fully rugged, tamper-protected, TEMPEST-proof
- ► Stationary and mobile deployment in all military branches (army, navy, air force)
- ► Ideal for end-user handling and management thanks to small size and simplified setup
- ► Upgradability by secure software download ensures that future challenges can be met
- ► Hardware provisioned for future applications, e.g. post-quantum cryptography

The R&S®ELCRODAT 7-MC is designed to be a form-fit replacement for its predecessor, the R&S®ELCRODAT 4-2.

With its modern hardware and software architecture, it also provides the necessary capabilities for state-of-the-art crypto protocols, including post quantum algorithms and data rates up to 1 Gbps. The R&S®ELCRODAT 7-MC allows flexible deployment. It provides serial interfaces for use in traditional radio and modem environments and Ethernet interfaces for integration into IP networks. Additionally, it can install, store, and run multiple crypto applications implementing different crypto modes enabling flexible use needed for different national and coalition scenarios.
The R&S®ELCRODAT 7-MC can be operated either with a control unit, via a web interface or using the MIL-bus module.

R&S®ELCRODAT 7-FN Application SCIP

A crypto solution for the communication of classified information in government and the public sector. Voice, video, and data are encrypted with the international SCIP standard and transmitted via IP networks using standard VoIP telecommunications infrastructure. The solution is approved for classification up to GEHEIM. Approval for NATO, and EU SECRET is in planning. The R&S®ELCRODAT 7-FN crypto device is suitable for office environments and for difficult environmental conditions.
It provides the accustomed, modern features of telephony and video systems. End-to-end encryption ensures that the information is at no time available in unencrypted form anywhere between the source and destination (e.g. within the switching infrastructure).

NETWORK SECURITY

Top priority of a company's network security is the technical and organizational protection of the internal IT infrastructure with all data, systems, devices, and applications – for digitally sovereign and secure digitalization. Staying up-to-date in terms of network security is a never-ending task: Companies face complex types of cyber-attacks (e.g. advanced persistent threats) and new guidelines (e.g. NIS2) on a daily basis. This demand is forcing ever newer and ever more sophisticated protective measures

MULTI-LAYERED PROTECTION IS THE KEY

IT core security

- ► Secure data storage ("data in rest") with security settings for files, clearly defined access, editing rights, and data backups
- ► Protection of physical IT devices including servers and network access control (NAC) against unauthorized access with a central Next Generation Unified Threat Management (UTM) system (e.g. LANCOM R&S®Unified Firewalls) and the resulting implementation of features such as regular security patches, functionality checks, software updates, sandboxing with machine learning, network segmentation, and rights management
- ► Strengthen security awareness among employees through IT security and compliance training and refresher courses, phishing simulations, and security guidelines

IT security at work level

- ► Endpoint security (e.g. mobile and IoT devices) via individual, fine-grained access rights per user (e.g. LANCOM Trusted Access Client)
- ► Data encryption via VPN networks using encryption parameters and algorithms according to the current BSI standard
- ► Application security via application monitoring / steering and use of current security standards

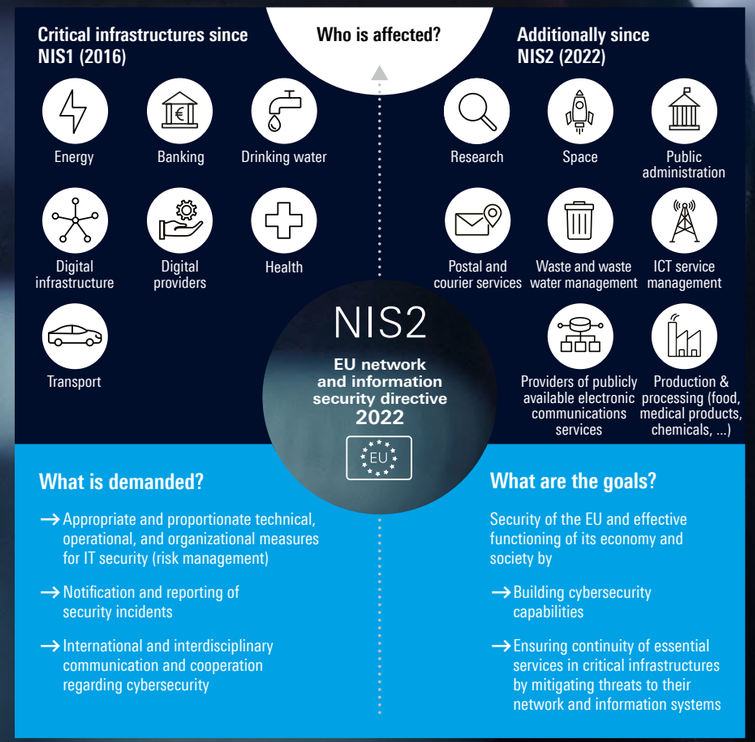
Transmission security

- ► Lateral protection of the own network ("data in motion") with e.g. network segmentation (VLANs) and caching routines to prevent public access
- ► Data use in accordance with legal requirements and processing with GDPR-compliant applications and systems, backdoor-free network components and cloud services hosted in the EU.
- ► Cloud security through geo-redundancy and careful access controls of external cloud services

Take a close look at network and information security guidelines (NIS2)

The NIS2 Directive, published by the European Commission in December 2022, requires EU member states to implement network security measures into their national law.

The stated aim is to strengthen the resilience of critical infrastructures according to the European Programme for Critical Infrastructure Protection (EPCIP), such as companies in the healthcare sector, postal services, research, and public administration, and thus increase the general level of cybersecurity in the EU.



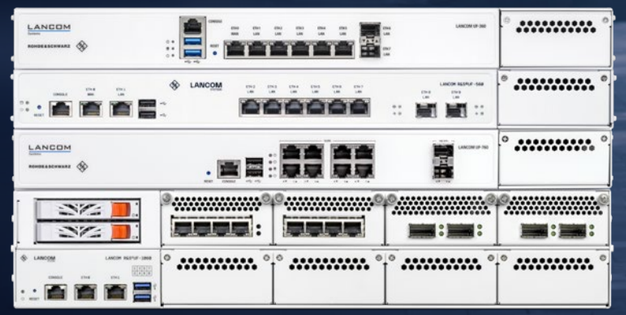
NETWORK SECURITY FOR LARGE, DISTRIBUTED ENTERPRISES

Phishing, advanced persistent threats, DDoS attacks...

The threat situation for companies is getting more serious every day. Especially growing, distributed enterprises with demanding networks and high data volumes need powerful security technologies. With the rack models of the next-generation firewalls (NGFW) and Unified Threat Management (UTM), you rely on a holistic security solution. With the "One-Click Security" concept of the LANCOM Management Cloud, precisely tailored security architectures are implemented in an automated, transparent, and uncomplicated manner. All LANCOM R&S®Unified Firewalls are developed in Germany and guarantee freedom from backdoors.

RACK UNIFIED FIREWALLS

- Next-generation IT security through UTM „Engineered in Germany" and guaranteed freedom from backdoors for protection against spam, viruses and malware as well as cyber attacks
- State-of-the-art security techniques such as R&S®PACE2 Deep Packet Inspection and SSL Inspection
- Preventive security against as yet unknown threats through integrated Sandboxing and Machine Learning
- Custom application and filter rules for increased security via Application Management and Content Filter
- Convenient firewall management via intuitive Web interface, LANCOM Management Cloud, or LANCOM R&S®UF Command Center
- LANCOM UF Extension Modules for port expansion and maximum flexibility available separately
- Also available as a virtual, software-based firewall (LANCOM vFirewall)
- Operation in a high-availability cluster (HA cluster) possible without additional costs or licenses
- Runtime-based licensing model (1, 3, or 5 years)



HIGHLIGHTS

Our security pledge: next-generation security with UTM

With threats to networks constantly growing, trusted security is anything but a given. As the keystone of network security, next-generation firewalls (NGFW) combine common security mechanisms with the latest generation technologies. In the triad of security, compliance, and usability, the top priorities are effective protection of your network and maximum prevention against threats that are not yet known – this promise applies without restriction to all LANCOM R&S®Unified Firewalls, regardless whether they are desktop or rack models. All LANCOM R&S®Unified Firewalls are developed in Germany, are guaranteed to be free of hidden access options (backdoors), and thus bear the trust mark "IT Security made in Germany".

Powerful: convincing firewall performance

Large and distributed enterprises as well as schools have particularly high demands on the data throughput of firewalls. Even in large IT infrastructures, our high-performance, future-proof rack models of the LANCOM R&S®Unified Firewalls impress with high and concentrated data volumes. The UF-1060 in particular, with its 100G interface and 10G UTM performance, offers the necessary performance to implement high-throughput security functions for branch infrastructures on the central site. For maximum connection flexibility, you can add additional ports to the Rack Unified Firewalls with optional expansion modules and thus individually adapt them to your network requirements.

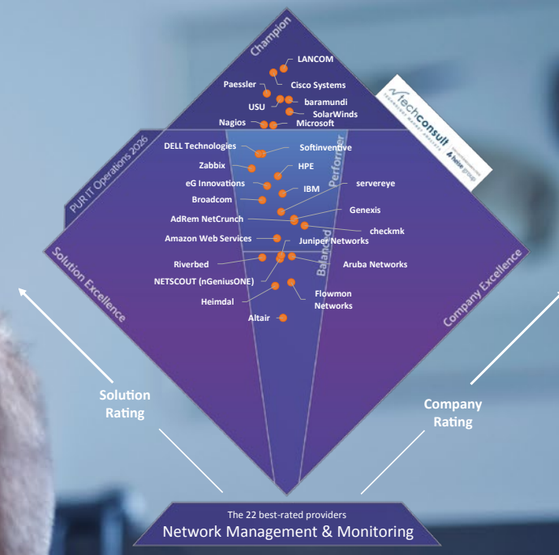
Concise: intuitive usability

Especially in large networks of enterprises and schools with numerous firewall rules, simple firewall management is valuable. That is why the LANCOM R&S®Unified Firewalls offer an intuitive "easy to use" operating concept that focuses on a clear, graphical representation of your settings. This not only minimizes potential sources of error, but also saves a lot of time on troubleshooting. As a result, the firewalls enable a stress-free working life in which you can concentrate fully on your business – without worrying about network security.

AWARD-WINNING NETWORK MANAGEMENT

LANCOM Management Cloud

Network management with LANCOM means: Security, routing, switching, and Wi-Fi from the cloud! The LANCOM Management Cloud (LMC) is the one system that controls your entire network infrastructure featuring our portfolio of R&S®Unified Firewalls, SD-WAN gateways, switches, access points, and remote access clients. You decide whether to switch over your entire network to innovative cloud management either right now, or one step at a time: migrating individual sites one by one is no problem.



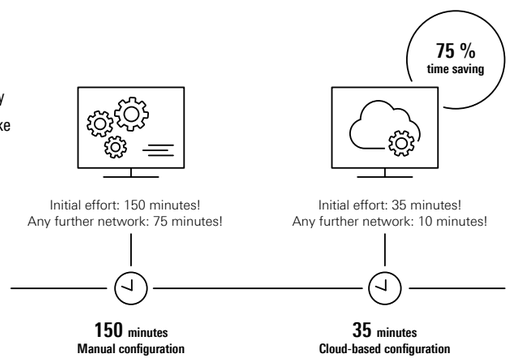
NETWORK MANAGEMENT OF A NEW ERA

More performance. More security.

The success of a business often depends on a powerful and secure network infrastructure. By optimally coordinating all the components involved, the LANCOM Management Cloud enormously optimizes the speed and efficiency of your network. Traffic analysis and optimization features make the best possible use of your network bandwidth.

Maximum productivity.

As the control center for your network, the LANCOM Management Cloud is the efficient deployment and maintenance tool for network designers. Configuration adjustments, firmware updates, monitoring, rollouts, and troubleshooting to your specifications are implemented automatically and efficiently. Expect time savings of 75 %!



ARC 2.0

Automatization with Active Radio Control 2.0

LANCOM Active Radio Control 2.0 is the answer to increasingly complex networks coupled with increasing cost pressure and a shortage of IT specialists: the self-learning automation solution optimizes Wi-Fi installations on the basis of real usage data, and minimizes the workload for IT administrators. As a true market-first in Wi-Fi optimization, LANCOM Active Radio Control 2.0 is patent-pending and offers the best possible user experience for every scenario: from office, hotel, or hospital Wi-Fi, to large-scale installations in stadiums and event arenas.

Immediate return on investment.

On average, IT administrators spend 40 percent of their working time troubleshooting. Especially in distributed networks with numerous sites, the LMC makes much more efficient use of valuable resources such as manpower, time, and money.

Put entire sites into operation without expensive on-site visits, provide new applications, or use real usage data to optimize even the most complex Wi-Fi infrastructures with a click of the mouse. The LMC helps to keep running costs under control and to set up companies to be lean and sustainable for the future.

SECURE AND RELIABLE SITE NETWORKING

A connection far beyond the network

Professional site networking aims for smooth workflows and clear, fluid communication – whether it's about data or people. Both should be in flow and constantly move the company forward. A holistic concept with coordinated WAN, LAN, Wi-Fi, security and remote access solutions is required here.

Location-independent networking with SD-WAN and SD-Branch

A software-defined wide area network (SD-WAN) replaces traditional, static and manually configured network infrastructures. At the same time, SD-WAN allows data-intensive networking of distributed company locations to be scaled and implemented under the highest data protection requirements for cross-location working. Your advantage: on-site deployment of qualified technicians at the respective company locations is no longer necessary and smooth network operation becomes the "new normal".

Automation **Performance** **Security** **Trust**

Secure network access with clever remote access solutions

LANCOM Remote & Mobile Access solutions enable secure and scalable access to corporate applications for employees in the office, at home or on the move, thus protecting modern hybrid working from anywhere and at any time. The only requirement is a software client on the laptop or PC. Once access has been configured, a highly encrypted connection is established with just one click. Whether as a classic VPN client, a cloud-managed VPN client, or based on the zero-trust principle with granular access rights to specific applications for individual user groups: LANCOM Remote & Mobile Access solutions scale for small businesses as well as for very large networks with several thousand users.

LANCOM Trusted Access

Best reception with professional Wi-Fi solutions

Whether wireless LAN is required outdoors, e.g. in the form of Wi-Fi solutions for campsites, indoors as classic corporate Wi-Fi or hotspot and guest Wi-Fi, or particularly resilient Wi-Fi in industrial or high-density environments: planning for optimum Wi-Fi coverage is a must.

Indoor Wi-Fi **Outdoor Wi-Fi**

High-density Wi-Fi **Industrial Wi-Fi**

Experience the future of wireless connectivity

LANCOM Wi-Fi 7 access points offer impressive speeds and extremely low latencies. But in addition to simply providing the next generation of Wi-Fi, these access points come with a unique offering for more security, sustainability, and automation. Find out more now and consciously strengthen your digital sovereignty with LANCOM Wi-Fi 7!

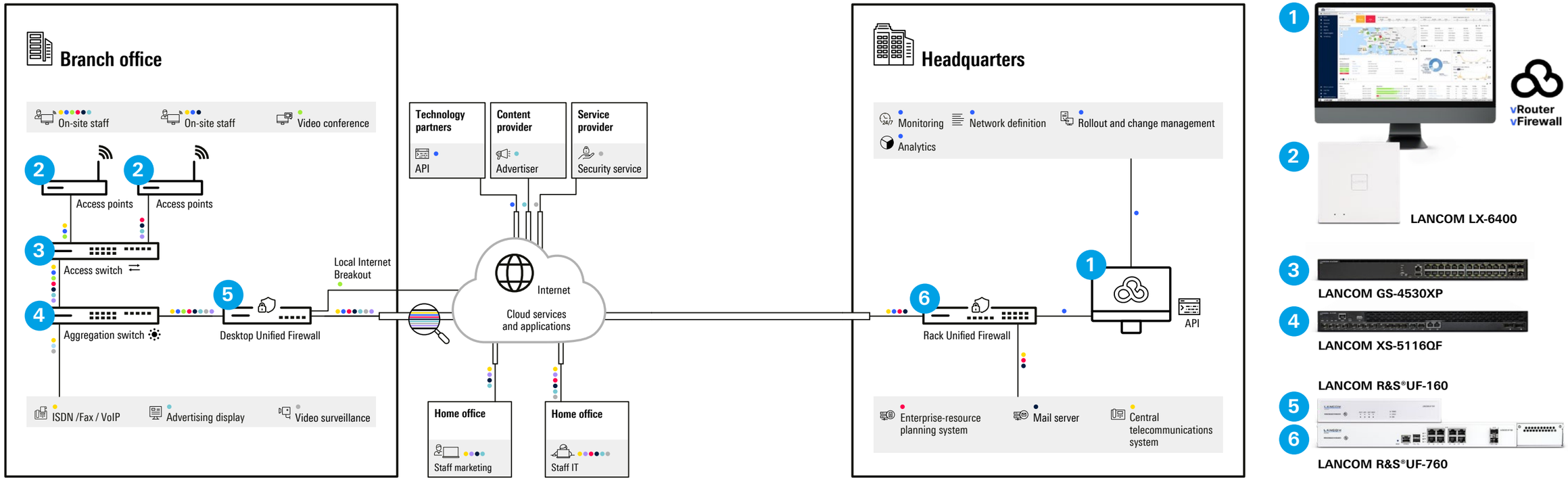
SITE CONNECTIVITY COMPETENCE

Efficient and secure data communication is crucial for companies that work across multiple locations. As a full-range provider, our holistic solutions guarantee the best network security and optimized connections within and between branch offices – whether in the wide area network (WAN), local area network (LAN), wireless network (Wi-Fi), or remote & mobile access connections.

Modern SD-WAN and SD-Branch solutions play a central role here by reducing the complexity of the network and enabling uniform administration and smooth operation. Based on central network management via the LANCOM Management Cloud, networks are designed, automatically rolled out, reliably operated, and optimized. Compliance requirements are implemented, and requirements regarding bandwidth, connection quality and application availability are also ensured at all locations.

The result is holistic management of all network processes, a secure connection of all locations and external service providers as well as secure network separation of the various digital applications – 100% GDPR-compliant for your digital sovereignty.

HIGH-PERFORMANCE SD-BRANCH ORCHESTRATION



AGILE SD-WAN FOR ATU

Modern network management for Germany's largest car repair chain with over 500 branches today

The SD-WAN is the basis for the entire ATU branch network. Therefore, it forms the backbone for the digitalization of all of the sites and their connection to the company headquarters. ATU also relies on a comprehensive digital network at the local sites. All components – from the branch routers, Wi-Fi access points, and switches through to the multi-Gigabit gateways in the head office – are managed via a central instance, the LANCOM Management Cloud (LMC). Numerous automated processes ensure efficient and secure management from the cloud. Especially during the rollout and network expansion, ATU benefits from functions such as the automatic provisioning of all devices.

Redundancy and reliability play an important role at ATU. After all, the failure of a branch router or a central gateway not only impacts the loss of critical remote connectivity, but also takes serious time and money to fix. ATU uses four central gateways, each in a separate data center at two different, geo-redundant locations. The branches also have backup scenarios via mobile communications to ensure maximum availability.

"We wanted to implement an alternative solution to MPLS: a more attractive and agile type of site networking. Standard broadband access, high reliability, performance, and a secure connection have been the core requirements for our site connectivity."

Volker Hermann
Team leader "Communication & Collaboration" at ATU

HIGHLY SECURE ENCRYPTION FOR AUTHORITIES

The Saarland has been the first federal state in Germany to introduce modern, flexible, and comprehensive encryption

The Saarland uses a multipoint-to-multipoint encryption including a modern layer 2 encryption solution that fulfills the strict BSI requirements for the transfer of VS-NfD data. The R&S®SITLine ETH effectively prevents exchanged documents, data streams or e-mails from being read by outsiders. This concept was implemented separately twice in the Saarland: once for the police and once for the IT-DLZ with the connected state authorities.

Our partner T-Systems carried out the detailed planning of the concept, including the rollout, and implemented the security solution. This project not only included preparing and supporting the commissioning of the hardware boxes, but also adapting them to the specific requirements of the state data network and the authorities. Thanks to the hardware integrated in these encryption boxes, users experience no loss of performance.

"The public authority decided to take existing IPsec-based encryption to a new level and will be replacing it with the high-performance encryption solution from Rohde & Schwarz Cybersecurity."

Marian Rachow
CEO Rohde & Schwarz Cybersecurity

Rohde & Schwarz

Rohde & Schwarz is striving for a safer and connected world with its Test & Measurement, Technology Systems and Networks & Cybersecurity Divisions. For 90 years, the global technology group has pushed technical boundaries with developments in cutting-edge technologies. The company's leading-edge products and solutions empower industrial, regulatory and government customers to attain technological and digital sovereignty. The privately owned, Munich based company can act independently, long-term and sustainably.

www.rohde-schwarz.com

Sustainable product design
Environmental compatibility and eco-footprint
Energy efficiency and low emissions
Longevity and optimized total cost of ownership

Certified Quality Management
ISO 9001

Certified Environmental Management
ISO 14001

Rohde & Schwarz training
www.training.rohde-schwarz.com

Rohde & Schwarz customer support
www.rohde-schwarz.com/support

PD 3685.0611.62 | Version 04.00 | October 2025 (dh)
Networks & Cybersecurity
Data without tolerance limits is not binding | Subject to change