



# NETWORKS & CYBERSECURITY

Innovation für effiziente, moderne Netze  
und effektive Sicherheit

**ROHDE & SCHWARZ**  
Make ideas real



# STREBEN NACH EINER SICHEREN UND VERNETZTEN WELT

**Rohde & Schwarz ermöglicht Unternehmen und Staaten technologisch, ihre Digitale Souveränität zu definieren und zu erhalten.**

Innovation gehört bei Rohde & Schwarz seit den Anfängen dazu. Die Firmengründer Dr. Lothar Rohde und Dr. Hermann Schwarz waren technologische Pioniere. Mit zupackendem Unternehmergeist brachen die Studienfreunde in die damals noch unerforschte Welt der Hochfrequenztechnik auf. Neunzig Jahre später beschäftigt das Privatunternehmen mit Sitz in München weltweit etwa 13.800 Mitarbeiter, die im Geschäftsjahr 2022/2023 einen Gesamtumsatz von 2,78 Milliarden EUR erzielten.

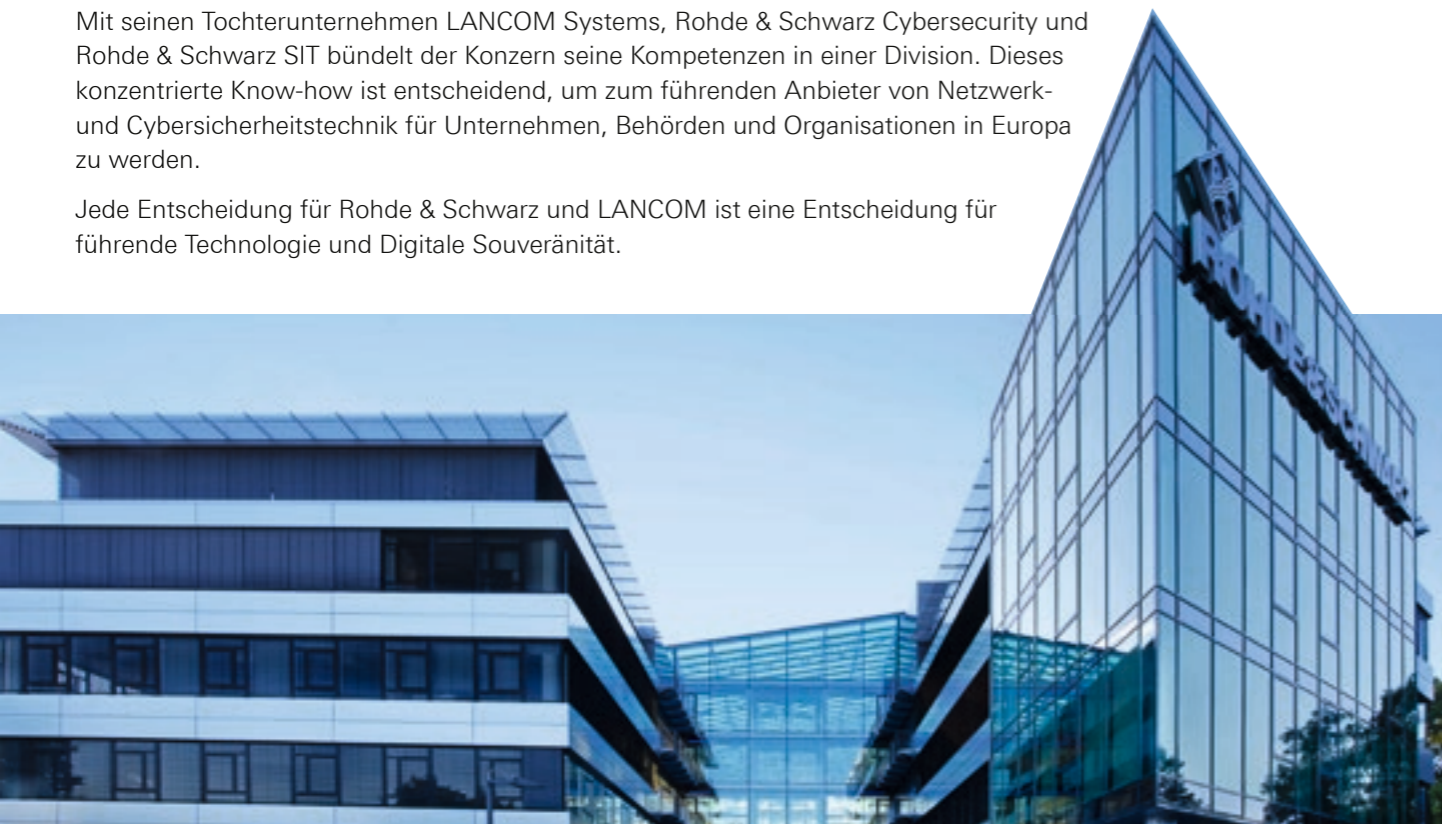
In seinen Divisionen Test & Measurement, Technology Systems und Networks & Cybersecurity realisiert Rohde & Schwarz schon heute Innovationen von morgen. Die führende Produkt- und Lösungskompetenz des globalen Technologiekonzerns befähigt seine Kunden aus Industrie, Behörden und Militär zur Gestaltung ihrer technologischen Selbstbestimmung und Digitalen Souveränität.

Mit Netzwerk-, Sicherheits- und Verschlüsselungslösungen schützt Rohde & Schwarz die digitalen Informationen und Geschäftsprozesse von Unternehmen und öffentlichen Einrichtungen vor den Auswirkungen von Cyberangriffen.

Das Datenvolumen wächst exponentiell. Gleichzeitig nimmt die potenzielle Bedrohung für Unternehmen, Behörden und Kritische Infrastrukturen zu. Nach Schätzungen seriöser Organisationen verursachen Cyberangriffe wie der Diebstahl von geistigem Eigentum jährlich Kosten in Höhe von Hunderten Milliarden Euro für die Weltwirtschaft. Aber nicht nur immaterielle Werte müssen geschützt werden. Auch die großen Mengen sensibler Daten des öffentlichen Sektors sowie personenbezogener Daten, die im privaten Sektor anfallen, müssen geschützt werden.

Mit seinen Tochterunternehmen LANCOM Systems, Rohde & Schwarz Cybersecurity und Rohde & Schwarz SIT bündelt der Konzern seine Kompetenzen in einer Division. Dieses konzentrierte Know-how ist entscheidend, um zum führenden Anbieter von Netzwerk- und Cybersicherheitstechnik für Unternehmen, Behörden und Organisationen in Europa zu werden.

Jede Entscheidung für Rohde & Schwarz und LANCOM ist eine Entscheidung für führende Technologie und Digitale Souveränität.



Unsere Netzwerk- und Cybersecurity-Lösungen stärken die Digitale Souveränität für öffentliche und kommerzielle Kunden. Wir bieten Sicherheit für mobile Geräte, Laptops und PCs durch ein umfassendes Portfolio an Hochgeschwindigkeitsverschlüsselung für Rechenzentren, VPN-Lösungen für sichere Netzwerke verteilter Organisationen, SD-WAN-Gateways und UTM-Firewalls zur Sicherung von IT-Perimetern sowie Cloud-basiertes Netzwerkmanagement.



Ralf Koenzen  
Executive Vice President Networks & Cybersecurity

## Inhalt






- 02 Einleitung
- 03 Inhalt
- 04 Rohde & Schwarz, Networks & Cybersecurity
- 06 Digitale Souveränität als strategisch-politische Aufgabe zur Stärkung der Kompetenzen
- 08 Innovation für effiziente, moderne Netze und effektive Sicherheit
- 10 Zuverlässige Netzwerklösungen für Unternehmen und Behörden
- 11 Cybersecurity-Produkte für Kunden aus dem öffentlichen und privaten Sektor
- 12 Mit Smartphones und Tablets hochsicher kommunizieren – R&S Mobile Connectivity
- 14 Netzwerkverschlüsselung – R&S°SITLine
- 16 Zentrale Sicherheitskontrolle – R&S°Trusted Object Manager
- 18 Vollständige Festplattenverschlüsselung – R&S°Trusted Disk Solution
- 20 Hochwertige Krypto-Lösung – R&S°ELCRODAT
- 22 Netzwerksicherheit
- 24 Ausgezeichnetes Netzwerkmanagement – LANCOM Management Cloud
- 26 Sichere und zuverlässige Standortvernetzung
- 28 Kompetenz bei der Konnektivität vor Ort
- 30 Use Cases – Agiles SD-WAN für ATU & hochsichere Verschlüsselung für Behörden

# ROHDE & SCHWARZ, NETWORKS & CYBERSECURITY

Die Rohde & Schwarz Division Networks & Cybersecurity bietet Endpoint-Sicherheit, sichere Netzwerke und hochwertige Kryptographie. Mit Produkten „Engineered in Germany“ sorgen wir für eine vertrauenswürdige, zuverlässige und sichere Datenübertragung und sind spezialisiert auf die Branchen Öffentlicher Dienst, Kritische Infrastrukturen, Verteidigung, Gesundheit, Einzelhandel und KMU. Wir sind der bevorzugte Lieferant für die nachhaltige Unterstützung von Organisationen, Regierungen und Streitkräften bei der Planung, dem Einsatz, dem Betrieb und der Optimierung ihrer Netzwerk- und Cybersicherheits Herausforderungen.



- Öffentliche Auftraggeber, Kritische Infrastrukturen (KRITIS)
 
- Wirtschaft
 
- Verteidigungsindustrie
 

- 
**4 Millionen**  
 installierte Netzwerkgeräte
- 
**100.000**  
 vernetzte Standorte
- 
**>500**  
 Produkte
- 
 Hochsichere Kryptographie für die Verteidigung
- 
 Digitale Souveränität

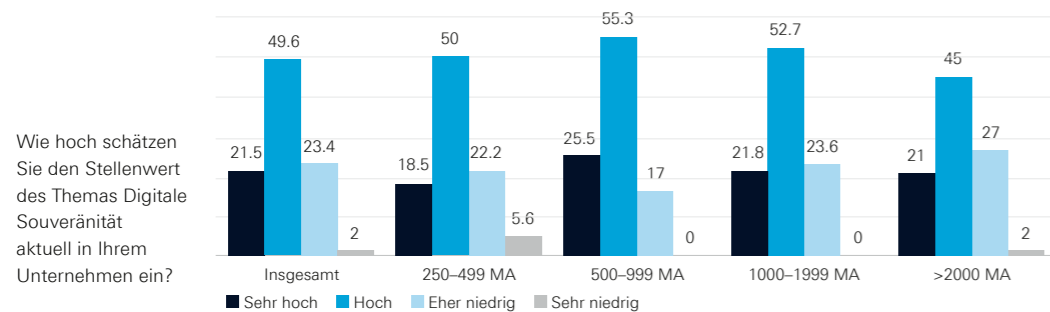
# DIGITALE SOUVERÄNITÄT ALS STRATEGISCH-POLITISCHE AUFGABE ZUR STÄRKUNG VON KOMPETENZEN

Laut Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ist die Digitale Souveränität „ein Thema von großer Relevanz. Lieferengpässe von Computerchips haben vor Augen geführt, wie schnell Abhängigkeiten von außereuropäischen Produzenten wichtige Wirtschaftszweige wie etwa die Autoindustrie ausbremsen können.“

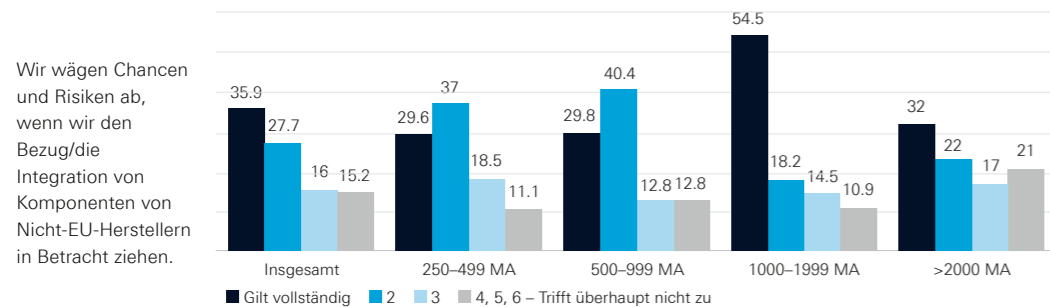
Auch wir sehen die Digitalisierung als Chance für Deutschland und Europa, die eigenen Kompetenzen und Kooperationen zu stärken. Denn nur so können wir in technologischen Bereichen unsere Position festigen. Das BMWK sieht ausdrücklich Handlungsbedarf bei „digitalen Schlüsseltechnologien (z. B. Netzwerktechnologien, Mikroelektronik, Sicherheitstechnologien, Quantentechnologien, Blockchain)“. Hier sollen deutsche und europäische Kompetenzen erhalten und ausgebaut werden.

Als Digitale Souveränität verstehen wir die Fähigkeit, selbst zu entscheiden, was wir tun. Dazu zählt die Entscheidungskompetenz, die Handlungskompetenz und die Fähigkeit, das Risiko durch Abhängigkeiten zu beurteilen. Ein digital souveränes Unternehmen kann gemäß der Definition der bitkom „selbstbestimmt und selbstbewusst zwischen Alternativen leistungsfähiger und vertrauenswürdiger Partner“ entscheiden.

Damit unterscheidet sich die Digitale Souveränität von Digitaler Abhängigkeit – ein Zustand, der vermutlich für kein Unternehmen erstrebenswert ist – und der Digitalen Autarkie. Letzteres ist in unserer globalisierten Welt in der Regel nicht realisierbar.



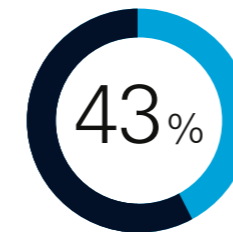
Quelle: Handelsblatt-Studie, 032023, Angaben in %, 4-Punkte-Skala, N/A nicht in der Grafik enthalten



Quelle: Handelsblatt-Studie, 032023, Angaben in %, 6-Punkte-Skala, N/A nicht in der Grafik enthalten

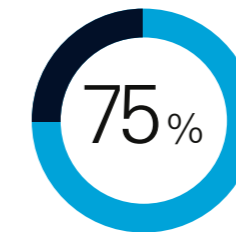


„Unsere eingesetzte Hardware stammt von Herstellern aus der EU.“



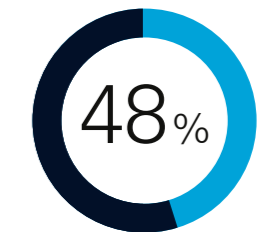
Die Hardware wird in der Regel von Herstellern außerhalb der EU bezogen. (■ = 3-6/trifft überhaupt nicht zu)

„Im Falle von Ausfällen können wir selbstständig oder mit Hilfe vertrauenswürdiger Partner unsere Prozesse wiederherstellen.“



Die Fähigkeit, IT-Prozesse im Falle von Ausfällen selbstständig wiederherzustellen, wird mit 75% als hoch bewertet. (■ = 1-2/Gilt voll und ganz)

„Wir sind auf keine externe Hilfe angewiesen, um ausreichende Maßnahmen hinsichtlich IT-Sicherheitsvorkehrungen, Kompetenzvermittlung und Krisenmanagement durchzuführen.“



Abhängigkeit von externer Hilfe für Sicherheitsvorkehrungen, Fähigkeiten, Krisenmanagement. (■ = 3-6/trifft überhaupt nicht zu)

Quelle: Handelsblatt-Studie, 032023, Angaben in %, 6-Punkte-Skala, K.A. nicht in der Grafik enthalten, normiert auf 100%



# INNOVATION FÜR EFFIZIENTE, MODERNE NETZWERKE UND EFFEKTIVE SICHERHEIT



## LANCOM MANAGEMENT CLOUD

Ein gut funktionierendes Netzwerk ist das Herz eines jeden Unternehmens. Es aufzubauen und zu steuern kann jedoch zeitaufwändig und fehleranfällig sein. In einer IT-Welt mit zunehmender Komplexität und einem allumfassenden Fachkräftemangel benötigen Sie daher eine verlässliche Steuerungszentrale für Ihr Netzwerk. Steuern Sie Ihren gesamten Netzwerkbetrieb in den Bereichen WAN, LAN, WLAN und Security dynamisch über eine einzige Cloud-basierte Plattform – so automatisiert, wie Sie möchten.



## SICHERE STANDORTVERNETZUNG FÜR GROSSE SD-WAN-SZENARIEN

Sehr große Multi-Service-IP-Netzwerke benötigen auf der Zentralseite Hochleistung und Zuverlässigkeit. Ein Multi-Gigabit-Gateway wie der LANCOM ISG-8000 bildet den sicheren und hochperformanten Kern Ihres SD-WAN. Dank leistungsstarker Plattform mit modernsten Verschlüsselungstechnologien, High Scalability VPN und umfangreichen Redundanz-Funktionen erhalten Sie ein Software-defined Wide Area Network (SD-WAN), das Ihnen den Administrationsaufwand deutlich erleichtert.



## NETZWERKVERSCHLÜSSELUNG FÜR HOCHSICHERE DIGITALE KOMMUNIKATION

Unsere Netzwerkverschlüsseler R&S®SITLine schützen öffentliche und kommerzielle Kunden vor Spionage und der Manipulation von Daten, die per Ethernet über Festnetz, Richtfunk oder Satellit übertragen werden. Sie erfüllen die vielfältigen Anforderungen von öffentlichen Einrichtungen, Unternehmen und Kritische Infrastrukturen, die sich auf speziell entwickelte, maßgeschneiderte Lösungen verlassen können.



## HOCHSICHERE KOMMUNIKATION MIT SMARTPHONES UND TABLETS

Die R&S Mobile Connectivity-Lösung basierend auf Indigo verbindet komfortables und sicheres Arbeiten mit sensiblen Daten auf Smartphones und Tablets nach dem VS-NfD-Standard (Verschlusssache - nur für den Dienstgebrauch) und erleichtert Anwendern in Behörden und sicherheitskritischen Umgebungen den Arbeitsalltag. Die R&S Mobile Connectivity-Lösung bietet erhebliche Vorteile für Organisationen und Unternehmen, die eine sichere mobile Kommunikation mit mobilen Endgeräten zur Erledigung ihrer täglichen Aufgaben bevorzugen und dabei höchsten Sicherheitsanforderungen genügen – ohne auf Bequemlichkeit verzichten zu müssen.

# VERTRAUENSWÜRDIGE NETZWERKLÖSUNGEN FÜR WIRTSCHAFT UND STAATEN

Soft- und Hardware-Entwicklung sowie Fertigung finden hauptsächlich in Deutschland statt, dasselbe gilt für das Hosting des Netzwerk-Managements (LANCOM Management Cloud). Besonderes Augenmerk gilt der Bereitstellung vertrauenswürdiger Lösungen mit exzellenten Sicherheitseigenschaften. Darüber hinaus ist Backdoor-Freiheit ein wesentliches Schutzmerkmal der Produkte. Das Vertrauenszeichen „IT-Security Made in Germany“ und eine Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigen die Vertrauenswürdigkeit und das herausragende Sicherheitsniveau.

# CYBERSICHERHEITSPRODUKTE FÜR KUNDEN AUS DEM ÖFFENTLICHEN UND PRIVATEN SEKTOR

Rohde & Schwarz Cybersecurity Produkte schützen hoheitliche und privatwirtschaftliche Kunden mit besonderen Sicherheits- und Zulassungsanforderungen vor den sich stetig ändernden Cyberbedrohungen. Wir entwickeln und produzieren Hochgeschwindigkeits-Netzwerkverschlüsselung und Zero-Trust-basierte Endpoint-Sicherheit. Die meisten dieser preisgekrönten Produkte sind vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Absicherung von VS-NfD-eingestufter Daten zugelassen. Diese vertrauenswürdigen Sicherheitslösungen unterstützen Anwender auf ihrem Weg in eine sichere und digitalisierte Welt.



## LANCOM Switches

Das LANCOM Gigabit Ethernet Switch-Portfolio ist die Basis für moderne Netzwerkinfrastrukturen in sämtlichen Branchen und Anwendungsbereichen. Zur Wahl stehen passgenaue Varianten mit Power over Ethernet (PoE) und Ports für verschiedene Durchsatzleistungen und Einsatzzwecke (1G, 2,5G, 10G, 25G, 40G, 50G, 100G) verschiedener Anzahl.



## LANCOM Router & SD-WAN

SD-WAN Central Site Gateways garantieren hohe Performance und Zuverlässigkeit in der Zentrale. LANCOM VPN-Router sorgen für hohe Bandbreiten, sichere Kommunikation und vertraulichen Datenaustausch in professionellen Netzwerken.



## LANCOM Access Points

Die LANCOM Access Points ermöglichen den kabellosen Netzwerkzugriff in jeder denkbaren Umgebung – ob outdoor, indoor oder in rauen Industrieumgebungen. Sie erfüllen sowohl höchste Ansprüche in Bezug auf die Hardware-Qualität (Lebensdauer, Temperaturentwicklung, etc.) als auch auf die Flexibilität und Sicherheit der zugrundeliegenden Software.



## R&S Netzwerkverschlüsseler

Unsere Netzwerkverschlüsseler schützen öffentliche und kommerzielle Kunden vor Spionage und der Manipulation von Daten, die per Ethernet über Festnetz, Richtfunk oder Satellit übertragen werden. Sie erfüllen die vielfältigen Anforderungen von öffentlichen Einrichtungen, Unternehmen und Kritische Infrastrukturen, die sich auf speziell entwickelte, maßgeschneiderte Lösungen verlassen können.



## R&S Zentrales Sicherheitsmanagement

Ein zuverlässiges Sicherheitsniveau erfordert eine einfache und zentrale Steuerung. Genau das ist die Aufgabe des R&S®Trusted Objects Managers. Er hilft, die spezialisierten Sicherheitsprodukte einfach einzurichten und zu verwalten. Er bietet eine intuitive Benutzeroberfläche. Anwender können Konfiguration, Deployment und Monitoring einfach handhaben. Eine moderne REST API im Backend ermöglicht die einfache und schnelle Integration in Ihre zentralen Monitoring- und Reporting-Systeme.



## LANCOM Remote & Mobile Access

Bieten Sie Mitarbeitenden im Büro, zu Hause oder unterwegs sicheren und skalierbaren Zugriff auf Unternehmensanwendungen und schützen Sie so das moderne hybride Arbeiten von überall und jederzeit.



## LANCOM Management Cloud

Steuert, optimiert und automatisiert Ihren gesamten Netzwerkbetrieb und vereinfacht und rationalisiert die Arbeitsabläufe durch die Eliminierung manueller individueller Gerätekonfigurationen erheblich.



## LANCOM R&S® Unified Firewalls

Umfassendes Unified Threat Management (UTM) in Kombination mit maschinellem Lernen bietet den besten Schutz vor neuen Arten von Viren und Malware. Mit diesen leistungsstarken Firewalls und geeigneten Zubehörteilen können Sie Ihre vertrauenswürdige Netzwerkinfrastruktur erweitern, basierend auf der Next-Generation der Deep Packet Inspection Engine.



## R&S Mobile Connectivity

R&S Mobile Connectivity verbindet komfortables und sicheres Arbeiten mit sensiblen Daten auf Smartphones und Tablets im Einklang mit der VS-NfD-Norm, was die tägliche Arbeit für Benutzer in Behörden und sicherheitskritischen Umgebungen erleichtert.



## R&S Endpoint Security

Der transparente Echtzeit-Verschlüsselungsprozess garantiert maximale Sicherheit – ohne jede Produktivitätseinschränkung. Die vollständige Festplattenverschlüsselung für Windows-Systeme und externe Datenträger schützt VS-NfD-bewertete Benutzerdaten, temporäre Dateien und das gesamte Betriebssystem, insbesondere vor Diebstahl oder Sabotage.



## R&S Kryptogeräte

Der R&S®ELCRODAT 7-MC ist ein robustes taktisches Kryptogerät zum Ver- und Entschlüsseln von Sprache und Datenkommunikation für deutsche, EU- und NATO-Sicherheitsklassifizierungen bis zu SECRET.

# HOCHSICHER KOMMUNIZIEREN MIT SMARTPHONES UND TABLETS

R&S Mobile Connectivity-Lösung – basierend auf Indigo für Smartphones und Tablets

Die R&S Mobile Connectivity-Lösung basierend auf Indigo verbindet komfortables und sicheres Arbeiten mit sensiblen Daten auf Smartphones und Tablets nach dem VS-NfD-Standard und erleichtert Mitarbeitenden in Behörden und sicherheitskritischen Umgebungen den Arbeitsalltag.

Mit der R&S Mobile Connectivity-Lösung machen Organisationen und Unternehmen, die eine sichere mobile Kommunikation mit mobilen Endgeräten zur Erledigung ihrer täglichen Aufgaben bevorzugen und dabei höchsten Sicherheitsanforderungen entsprechen wollen, einen wichtigen Schritt nach vorne.

## BESONDERE MERKMALE DER R&S MOBILE CONNECTIVITY-LÖSUNG

### Standardgeräte und garantierte Updates

Standard-Smartphones und -Tablets können verwendet werden. Der Anbieter garantiert kostenlose Updates für mindestens 5 Jahre. Nach dem Ende der Nutzung ist ein Wiederverkauf möglich, wobei hohe Wiederverkaufswerte zu erwarten sind.

### Ein Gerät – für die private und gesicherte berufliche Nutzung

Zwei Aufgaben können mit nur einem mobilen Gerät abgedeckt werden: private und geschützte Nutzung – alles ohne die Einhaltung der VS-NfD-Richtlinien zu vernachlässigen. E-Mail, Kalender, Kontakte und optional Messenger; Intranet-Browser können als vorinstallierte Standardanwendungen im hochsicheren Bereich genutzt werden – keine Containerlösung.

### R&S Mobile Connectivity-Lösung hat BSI-Zulassung

Die Indigo-Plattform erhielt im Oktober 2022 die Zulassung des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Aufgrund der BSI-Bestätigung der Sicherheit der Plattform sind keine zusätzlichen Smartcards oder SD-Karten als Sicherheitsanker erforderlich.

### VS-NfD-Komponenten

Die Lösung verwendet drei Hauptkomponenten: ein Smartphone oder Tablet als Endgerät, ein VS-NfD-zugelassenes VPN-Gateway und ein MDM.

### Eine Lösung – von der Planung bis zum Betrieb

Die beiden Sicherheitsspezialisten Rohde & Schwarz Cybersecurity und agilimo Consulting bieten eine umfassende Lösung an: komplettes VPN-Backend, Mobile Device Management (MDM) und automatisiertes Zertifikatsmanagement.



Diese besondere Partnerschaft zwischen Rohde & Schwarz Cybersecurity und agilimo Consulting bietet Behörden, Organisationen und Unternehmen eine ausgereifte, alltagstaugliche Lösung, die den Sicherheitsanforderungen des BSI für die Verarbeitung von VS-NfD-verschlüsselten Daten entspricht. Engineered in Germany.

SecurITy  
made  
in  
Germany

# NETZWERKVERSCHLÜSSELUNG

Mit über 30 Jahren Kryptokompetenz gehört Rohde & Schwarz Cybersecurity zu den Pionieren auf dem Gebiet der Hochgeschwindigkeits-Netzwerkverschlüsselung. Das Unternehmen deckt die gesamte Wertschöpfungskette ab und garantiert so ein Höchstmaß an Vertrauen und Zuverlässigkeit. Unsere Netzwerkverschlüsseler schützen hoheitliche und privatwirtschaftliche Kunden vor Spionage und der Manipulation von Daten, die per Ethernet über Festnetz, Richtfunk oder Satellit übertragen werden.

Sie erfüllen die vielfältigen Anforderungen von öffentlichen Einrichtungen, Unternehmen und Kritische Infrastrukturen, die sich auf speziell entwickelte, maßgeschneiderte Lösungen verlassen können.

## Vorteile unserer Netzwerkverschlüsseler

- ▶ „IT-Sicherheit made in Germany“ – über 30 Jahre Kryptokompetenz
- ▶ Dedizierte Hardware und Software für marktführende Verschlüsselungs-Performance
- ▶ Modernste kryptografische Methoden und Standards
- ▶ Hohe Benutzerfreundlichkeit durch zentrales Sicherheitsmanagementsystem
- ▶ BSI-Zulassung:

**VS-NfD (RESTRICTED), EU & NATO RESTRICTED**

## R&S®SITLine ETH

Erhältlich in verschiedenen Leistungsklassen, bietet diese moderne Hardware-Software-Architektur in Kombination mit neuester Kryptographie langfristige und nachhaltige Sicherheit für Ihre Infrastruktur. Das neue Hochleistungsgerät hat einen Durchsatz von 2x100 GBit/s.



## LEISTUNGSFÄHIGE UND SICHERE DATENÜBERTRAGUNG

Die Integration von Cybersicherheitslösungen in Unternehmen ist eine Investition in die Zukunftsfähigkeit und Resilienz Ihrer Organisation. Wir von Rohde & Schwarz Cybersecurity sehen IT-Sicherheit als integralen Bestandteil der Wertschöpfungskette. Dieser Ansatz ermöglicht es uns, Sicherheitslösungen anzubieten, die nicht nur den Schutz vor Cyberangriffen gewährleisten, sondern auch den reibungslosen Betrieb Ihrer Geschäftsprozesse unterstützen – und damit die Kontinuität des Geschäftsbetriebs sicherstellen.

Unsere Lösungen zeichnen sich aus durch hohe Leistung in Verbindung mit schneller Reaktionszeit. Unsere Kunden profitieren von der Kombination aus führender Sicherheitstechnologie und der Gewissheit, dass sie im Falle eines Sicherheitsvorfalls oder bei Bedarf an technischer Unterstützung auf den kompetenten und zuverlässigen Service von Rohde & Schwarz zählen können. Das Vertrauen in die Marke Rohde & Schwarz begründet sich auf der jahrzehntelangen Erfahrung und dem tiefen Verständnis der Cybersicherheitsanforderungen verschiedener Branchen.

Letztlich gewährleistet die Investition in Cybersecurity-Lösungen von Rohde & Schwarz nicht nur den Schutz vor den immer komplexeren Bedrohungen im Cyberspace, sondern auch die Integrität und Verfügbarkeit Ihrer kritischen Daten und Systeme. So wird sichergestellt, dass Ihr Unternehmen in einer zunehmend vernetzten und digitalisierten Welt weiterhin erfolgreich und sicher agieren kann.



# ZENTRALE SICHERHEITSKONTROLLE

## R&S®Trusted Objects Manager

Ein zuverlässiges Sicherheitsniveau erfordert eine einfache und zentrale Kontrolle. Genau diese Funktion erfüllt der R&S®Trusted Objects Manager. Er hilft, die spezialisierten Sicherheitsprodukte einfach einzurichten und zu verwalten. Mit diesem System können IT-Administratoren auf Anwendungen wie R&S®Trusted VPN, R&S®Trusted Disk, R&S®Trusted Identity Manager und R&S®Trusted VPN Client zugreifen und diese steuern. Durch die Installation einer einzigen Instanz des R&S®Trusted Objects Manager können Benutzer all diese Produkte nahtlos verwalten, was eine Skalierbarkeit auf bis zu 50.000 Clients ermöglicht. Die Kompatibilität mit verschiedenen LDAP-Verzeichnisdiensten, einschließlich Microsoft Active Directory, Lotus Domino und Novell eDirectory und OpenLDAP, gewährleistet eine reibungslose Integration in Netzwerkumgebungen unterschiedlicher Größe. Benutzer und Benutzergruppen können problemlos aus bestehenden LDAP-Strukturen importiert werden. Um die Zuverlässigkeit und Ausfallsicherheit zu erhöhen, können zusätzliche R&S®Trusted Objects Manager als Standby-Instanzen integriert werden – eine optionale Skalierungsmöglichkeit abhängig vom erforderlichen Ausbau-Niveau.

## DIE SPEZIELLEN EIGENSCHAFTEN DER ZENTRALEN STEUERUNG MIT DEM R&S®TRUSTED OBJECT MANAGER:

### Intuitive Bedienung des Managers

Der R&S®Trusted Objects Manager zeichnet sich aus durch prozessorientierte Benutzerführung mit intuitivem Benutzererlebnis und seine Flexibilität in der Benutzer- und Rechteverwaltung. Ein IT-Administrator kann den gesamten Betriebszyklus der Rohde & Schwarz Cybersecurity-Komponenten über ein sicheres Webinterface verwalten. Darüber hinaus bietet die optionale, integrierte PKI den Vorteil, dass Sie diese eigenständig und unabhängig von Drittanbietern betreiben können.

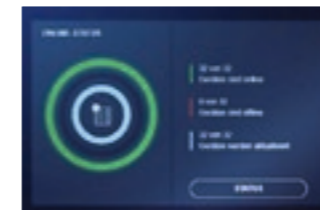
### Maximale Sicherheit dank einer optionalen Public-Key-Infrastruktur (PKI)

Optional kann über den R&S®Trusted Objects Manager eine Public-Key-Infrastruktur (PKI) integriert werden – eine Sicherheitskomponente für größere Vertraulichkeit, Integrität und Authentizität von Daten. Die Public-Key-Infrastruktur (PKI) kann in Eigenregie, ohne Dritte, aufgebaut und betrieben werden. R&S Cybersecurity unterstützt Sie bei der Einrichtung.

### VS-NfD-, EU & NATO RESTRICTED-ready

Die R&S®Trusted Objects Manager sind vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert und berechtigt, VS-NfD, EU & NATO RESTRICTED-Daten zu verarbeiten. Damit können öffentliche Einrichtungen und private Unternehmen ihre Arbeitsstationen und mobilen Speichergeräte so absichern, dass sie VS-NfD-Verschlusssachen speichern und verarbeiten können.

Die Schutzwirkung einer abgesicherten Umgebung hängt direkt davon ab, wie effizient die Kontrolle über die jeweiligen Komponenten in die Prozesse integriert ist. Ein R&S®Trusted Objects Manager ist der tägliche digitale Assistent für die einfache und sichere Verwaltung von R&S-Sicherheitskomponenten. Ausgehend vom Betriebsprozess liegt der Fokus auf der intuitiven Bedienung der zentralen Steuereinheit. Insbesondere wenn es darum geht, die Prozesskomplexität deutlich zu reduzieren und Fehlerquellen zu eliminieren. **Engineered in Germany**



# FESTPLATTENVOLLVERSCHLÜSSELUNG

## R&S®Trusted-Disk-Lösung

Der transparente Echtzeit-Verschlüsselungsprozess garantiert maximale Sicherheit, ohne jede Produktivitätseinschränkung. Die Festplattenvollverschlüsselung für Windows-Systeme und externe Datenträger schützt VS-NfD-eingestufte Benutzerdaten, temporäre Dateien und das gesamte Betriebssystem auf allen internen Festplatten Ihrer Computer, externen USB- und Thunderbolt-Datenträgern – insbesondere gegen Diebstahl oder Sabotage. Die R&S®Trusted-Disk Lösung sorgt mit transparenter Echtzeitverschlüsselung für die uneingeschränkte Produktivität aller Rechner (Laptops, Desktops, Serversysteme) – basierend auf einer Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit VS-NfD-Zulassung. Ein sicherer Zugang wird z. B. durch den Einsatz von Smartcards wie dem elektronischen Dienst- und Truppenausweis erreicht. Damit sind Ihre Daten auch im Falle eines Diebstahls tragbarer Datenträger oder Laptops sicher vor dem Verlust sensibler Daten geschützt.

## BESONDERE MERKMALE DER R&S®TRUSTED DISK:

### Mehr Sicherheit durch High-End-Kryptografie

Die R&S®Trusted-Disk Lösung verwendet hochsichere Verschlüsselungsalgorithmen wie AES-XTS mit einer Schlüssellänge von 512 Bit und RSA-Blinding. Sie nutzt die sicheren Botan-Krypto-Bibliotheken und ermöglicht eine sichere Datenlöschung. Sie bietet auch eine Benutzerauthentifizierung im Pre-Boot-Authentifizierungsprozess, der auf einer Smartcard und einer PIN basiert. Die Lösung verwendet sichere Boot-Mechanismen und einen SHIM-Bootloader. Diese Technologie umfasst auch die Erzeugung aktueller Zufallszahlen und die flexible Neuberechnung von Verschlüsselungsschlüsseln auf der Grundlage von Zeit und geschriebenen Daten.

### Erweiterter Schutz auch für mobile Datenträger

Darüber hinaus können beliebige und komfortable tragbare Speichermedien wie USB-Sticks, Thunderbolt-Laufwerke und externe Festplatten sicher verschlüsselt und authentifiziert werden. Gerade hier bietet die Lösung einen effizienten Datenschutz im Falle eines Diebstahls der mobilen Datenträger.

### Zentralisierte Verwaltung von geschützten Endpunkten

Die zentrale Verwaltung von Benutzerberechtigungen ermöglicht eine schnelle und flexible Anpassung von Installationen. Die Unterstützung für Secure Boot mit dem Microsoft SHIM-Bootloader erleichtert und beschleunigt umfangreiche Rollouts.

### VS-NfD, EU & NATO RESTRICTED

Alle R&S®Trusted Disk Lösungen sind vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert und für die Verarbeitung von VS-NfD, EU & NATO RESTRICTED Daten zugelassen. Damit können öffentliche Einrichtungen und private Unternehmen ihre Arbeitsplätze und tragbaren Speichergeräte so absichern, dass sie VS-NfD-Verschlußtatsachen speichern und verarbeiten können.

Herstellerqualifikation für  
das qualifizierte VS-NfD-  
Zulassungsverfahren des BSI

Der Schutz vor Datenverlusten und Cyberangriffen ist für öffentliche Einrichtungen und Unternehmen ein Risiko für die Geschäftskontinuität. Laut der TÜV-Cybersecurity-Studie 2022 war jedes zehnte deutsche Unternehmen bereits von einem Cyberangriff betroffen. Die Bedrohungen sind also real und die Auswirkungen können verheerend sein. Denn die Arbeitswelt und ihre täglichen Arbeitsprozesse sind digitaler denn je, und Daten sind die wertvollste Ressource für die digitale Wertschöpfung.

Eine R&S®Trusted Disk Lösung ist Ihr Schutzschild gegen diese Bedrohungen. Sie nutzt modernste Verschlüsselungstechnologien, um Ihre Daten zu schützen – vor Veränderung, Sabotage und Diebstahl von Datenträgern. Gehen Sie keine Kompromisse ein, wenn es um Sicherheit geht. Handeln Sie jetzt, um Ihre Datenbestände zu sichern und Ihre Institution oder Ihr Unternehmen mit einem weiteren wichtigen Baustein vor den wachsenden Bedrohungen der Cyberwelt zu schützen.

# HOCHKLASSIGE KRYPTO-LÖSUNG

## Robuste HF/VHF/UHF/IP-Sicherheit für Sprache und Daten

Der R&S®ELCRODAT 7-MC ist ein robustes taktisches Kryptogerät zur Ver- und Entschlüsselung von Sprach- und Datenkommunikation für deutsche, EU- und NATO-Sicherheitseinstufungen bis SECRET. Es ist TEMPEST-fest und interoperabel mit HF/VHF/UHF-Funk, Satellitenkommunikation, Fernmeldeleitungen und IP-Infrastruktur. Es eignet sich perfekt für den Einsatz auf stationären und mobilen Plattformen im rauen Gelände sowie auf See und in der Luft.

## DIE WICHTIGSTEN FAKTEN DER LÖSUNG

- ▶ Schützt HF/VHF/UHF, Satellitenkommunikation und Fernmeldeleitungen
- ▶ Unterstützt IP-Verschlüsselungsprotokolle wie NINE und SCIP
- ▶ Datenraten bis zu 1 GBit/s
- ▶ Äußerst widerstandsfähig, manipulationssicher, TEMPEST-fest
- ▶ Stationäre und mobile Einsätze in allen militärischen Bereichen (Heer, Marine, Luftwaffe)
- ▶ Ideal für die Handhabung und Verwaltung durch den Endbenutzer dank der geringen Größe und der vereinfachten Einrichtung
- ▶ Aktualisierbarkeit durch sicheres Herunterladen der Software gewährleistet, dass zukünftige Herausforderungen bewältigt werden können
- ▶ Hardware für künftige Anwendungen, z. B. Post-Quantum-Kryptographie

## Der R&S®ELCRODAT 7-MC ist als form- und passgenauer Ersatz für seinen Vorgänger R&S®ELCRODAT 4-2 konzipiert

Mit seiner modernen Hard- und Software-Architektur bietet er auch die notwendigen Fähigkeiten für moderne Krypto-Protokolle, einschließlich Post-Quantum-Algorithmen und Datenraten bis zu 1 GBit/s. Der R&S®ELCRODAT 7-MC lässt sich flexibel einsetzen. Er bietet serielle Schnittstellen für den Einsatz in traditionellen Funk- und Modemumgebungen sowie Ethernet-Schnittstellen für die Integration in IP-Netzwerke. Darüber hinaus kann er mehrere Kryptoanwendungen installieren, speichern und ausführen, die verschiedene Kryptomodi implementieren, was einen flexiblen Einsatz für unterschiedliche nationale und koalitionsfähige Szenarien ermöglicht. Der R&S®ELCRODAT 7-MC kann entweder mit einem Steuergerät, über ein Web-Interface oder über das MIL-Bus-Modul betrieben werden.

## R&S®ELCRODAT 7-FN für SCIP-Anwendungen

Eine Kryptolösung für die Kommunikation von Verschlusssachen in Behörden und dem öffentlichen Sektor: Sprache, Video und Daten werden gemäß dem internationalen SCIP-Standard verschlüsselt und über IP-Netze mit der Standard-VoIP-Telekommunikationsinfrastruktur übertragen. Die Lösung ist für die Klassifizierung bis GEHEIM zugelassen und eine Zulassung für NATO und EU SECRET befindet sich in der Planung. Das Kryptogerät R&S®ELCRODAT 7-FN ist sowohl für Büroumgebungen als auch für schwierige Umgebungsbedingungen geeignet. Es bietet die gewohnten, modernen Funktionen von Telefonie- und Videosystemen. Die Ende-zu-Ende-Verschlüsselung gewährleistet, dass die Informationen zu keinem Zeitpunkt unverschlüsselt zwischen Quelle und Ziel verfügbar sind (z. B. innerhalb der Vermittlungsinfrastruktur).



# NETZWERKSICHERHEIT

Oberste Priorität der Netzwerksicherheit eines Unternehmens ist der technische und organisatorische Schutz der internen IT-Infrastruktur mit allen Daten, Systemen, Geräten und Anwendungen – für eine digital souveräne und sichere Digitalisierung. In puncto Netzwerksicherheit auf dem neuesten Stand zu bleiben, ist eine nie endende Aufgabe: Unternehmen sind täglich mit komplexen Arten von Cyberangriffen (z. B. Advanced Persistent Threats) und neuen Richtlinien (z. B. NIS2) konfrontiert, die immer wieder neue und ausgefeiltere Schutzmaßnahmen erfordern.

## MEHRSCICHTIGER SCHUTZ IST DER SCHLÜSSEL

### IT-Kernsicherheit

- Sichere Datenspeicherung („data in rest“) mit Sicherheitseinstellungen für Dateien, klar definierten Zugriffs- und Bearbeitungsrechten und Datensicherungen
- Schutz der physischen IT-Geräte inklusive Server und Netzwerkzugangskontrolle (NAC) vor unbefugten Zugriffen durch ein zentrales Next-Generation Unified Threat Management (UTM)-System (z. B. LANCOM R&S® Unified Firewalls) und die daraus resultierende Implementierung von Features wie z. B. regelmäßige Sicherheitspatches, Funktionsprüfungen, Software-Updates, Sandboxing mit maschinellem Lernen, Netzwerksegmentierung und Rechteverwaltung
- Stärkung des Sicherheitsbewusstseins der Mitarbeitenden durch Schulungen und Auffrischkurse zu IT-Sicherheit und Compliance, Phishing-Simulationen und Sicherheitsrichtlinien

### IT-Sicherheit bei der täglichen Arbeit

- Endpunktsicherheit (z. B. mobile und IoT-Geräte) durch individuelle, feinkörnige Zugriffsrechte pro Benutzer (z. B. LANCOM Trusted Access Client)
- Datenverschlüsselung über VPN-Netzwerke unter Verwendung von Verschlüsselungsparametern und -algorithmen nach dem aktuellen BSI-Standard
- Anwendungssicherheit durch Anwendungsüberwachung/-steuerung und Nutzung aktueller Sicherheitsstandards

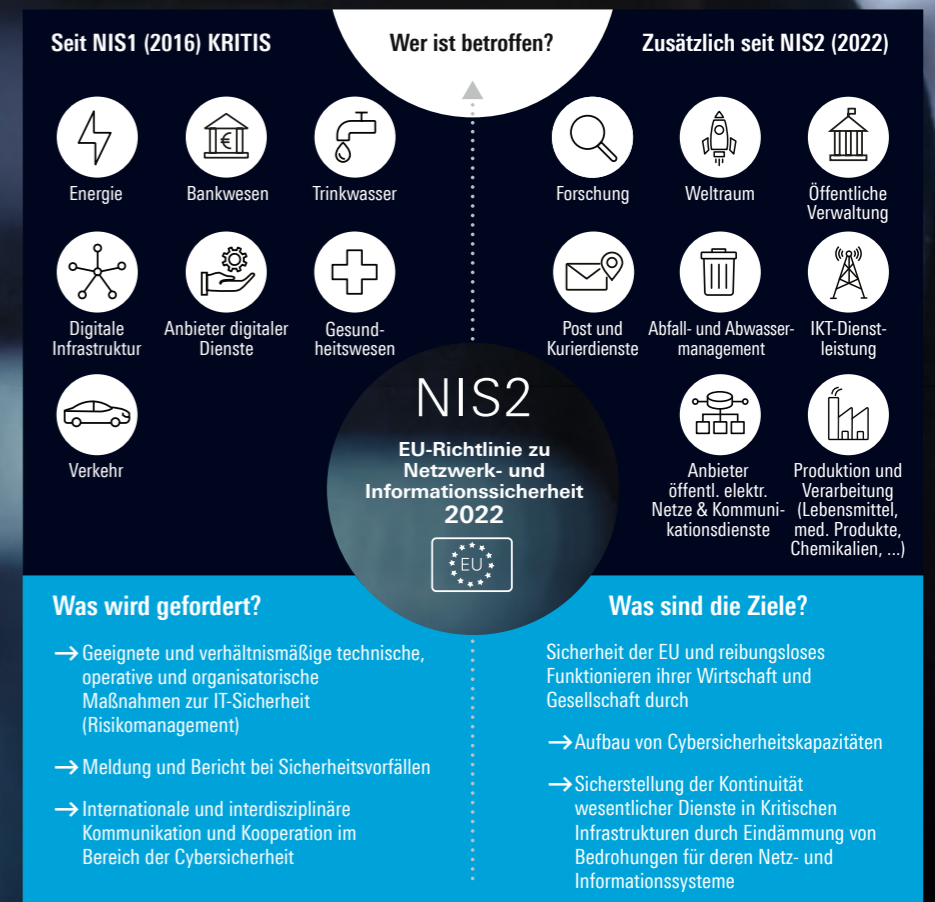
### Übertragungssicherheit

- Seitlicher Schutz des eigenen Netzes („data in motion“), z. B. durch Netzwerksegmentierung (VLANs) und Caching-Routinen zur Verhinderung des öffentlichen Zugriffs
- Rechtskonforme Datennutzung und -verarbeitung mit DSGVO-konformen Anwendungen und Systemen, Backdoor-freien Netzwerkkomponenten und in der EU gehosteten Cloud-Diensten
- Cloud-Sicherheit durch geografische Redundanz und Prüfung der Sicherheit von genutzten externen Cloud-Diensten

## Machen Sie sich ein umfassendes Bild zu den Leitlinien Netz- und Informationssicherheit (NIS2)

Die NIS2-Richtlinie ist die im Dezember 2022 von der Europäischen Kommission veröffentlichte Handlungsanweisung, bis zum 17. Oktober 2024 gewisse Netzwerksicherheitsmaßnahmen in nationales Recht umzusetzen.

Das erklärte Ziel ist es, die Widerstandsfähigkeit der Kritischen Infrastrukturen gemäß dem Europäischen Programm für den Schutz Kritischer Infrastrukturen (EPCIP) – wie zum Beispiel Unternehmen im Gesundheitswesen, in der Forschung, Postdienste oder die öffentliche Verwaltung – zu verbessern und so das allgemeine Niveau der Cybersicherheit in der EU zu erhöhen.



# AUSGEZEICHNETES NETZWERKMANAGEMENT

## LANCOM Management Cloud

Netzwerkmanagement mit LANCOM heißt: Security, Routing, Switching und WLAN aus der Cloud heraus! Die LANCOM Management Cloud (LMC) ermöglicht die Steuerung der gesamten Netzwerkinfrastruktur mit unserem Portfolio bestehend aus R&S® Unified Firewalls, SD-WAN Gateways, Switches bis hin zu Access Points über nur ein System. Dabei entscheiden Sie, ob Sie gleich Ihr komplettes Netzwerk auf innovatives Cloud-Management umstellen oder Schritt für Schritt: Ein sukzessiver Umstieg einzelner Standorte ist problemlos möglich.



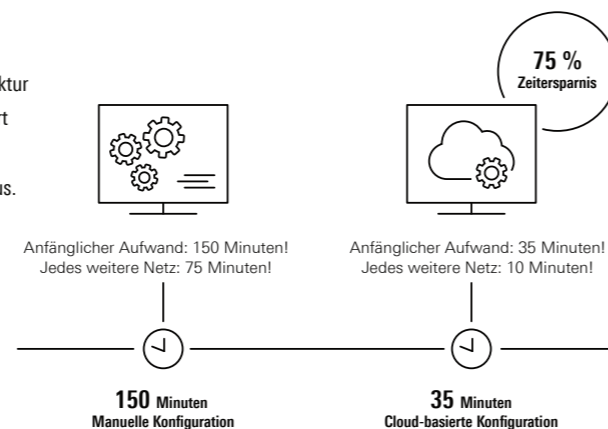
## NETZWERKMANAGEMENT IN EINER NEUEN ÄRA

### Mehr Leistung. Mehr Sicherheit.

Ihr Geschäftserfolg hängt maßgeblich mit einer leistungsstarken und sicheren Netzwerkinfrastruktur zusammen. Durch die optimale Abstimmung aller beteiligten Komponenten aufeinander, optimiert die LANCOM Management Cloud die Geschwindigkeit und Effizienz Ihres Netzwerkes enorm. Funktionen zur Traffic-Analyse und -Optimierung nutzen Ihre Netzwerkbandbreite bestmöglich aus.

### Maximale Produktivität.

Als Steuerungszentrale für Ihr Netzwerk ist die LANCOM Management Cloud das effiziente Bereitstellungs- und Wartungstool für Netzwerkdesigner. Konfigurationsanpassungen, Firmware-Updates, Monitoring, Rollouts und Fehlerbehebungen nach Ihren Vorgaben werden automatisch und effizient umgesetzt. Rechnen Sie mit einer Zeitersparnis von 75 %.



### Automatisierung mit LANCOM Active Radio Control™ 2.0.

LANCOM Active Radio Control™ 2.0 ist die Antwort auf immer komplexere Netzwerke in Verbindung mit einem zunehmenden Kostendruck und einem Mangel an IT-Fachkräften: Die selbstlernende Automatisierungslösung optimiert WLAN-Installationen auf Basis realer Nutzungsdaten und minimiert den Arbeitsaufwand für IT-Administratoren. Als echte Marktneuheit in der WLAN-Optimierung ist LANCOM Active Radio Control™ 2.0 zum Patent angemeldet und bietet das bestmögliche Nutzererlebnis für jedes Szenario: vom Büro-, Hotel- oder Krankenhaus-WLAN bis hin zu Großinstallationen in Stadien und Veranstaltungsarenen.

### Unmittelbarer Return on Invest.

IT-Administratoren verbringen durchschnittlich 40 Prozent ihrer Arbeitszeit mit Troubleshooting. Gerade bei verteilten Netzen mit vielen Standorten werden mit der LMC wertvolle Ressourcen wie Arbeitskräfte, Zeit und Geld viel effizienter eingesetzt.

Ohne teure Vor-Ort-Einsätze nehmen Sie komplette Standorte in Betrieb, stellen neue Anwendungen bereit oder optimieren auch komplexeste WLAN-Infrastrukturen auf Basis der realen Nutzungsdaten per Mausclick. Die LMC hilft, die laufenden Kosten im Griff zu behalten und Unternehmen schlank und nachhaltig für die Zukunft aufzustellen.

# SICHERE UND ZUVERLÄSSIGE STANDORTVERNETZUNG

Eine Verbindung weit über das Netzwerk hinaus

Professionelle Standortvernetzung zielt auf reibungslose Arbeitsabläufe und eine klare, flüssige Kommunikation ab – ob es um Daten und Signale oder um Menschen geht. Beides sollte im Fluss sein und das Unternehmen stetig voranbringen. Hier ist ein ganzheitliches Konzept mit aufeinander abgestimmten WAN-, LAN-, WLAN-, Security- und Remote-Access-Lösungen gefragt.



## Standortunabhängige Vernetzung mit SD-WAN und SD-Branch

Ein Software-defined Wide Area Network (SD-WAN) ersetzt traditionelle, statische und manuell konfigurierte Netzwerkinfrastrukturen. Gleichzeitig ermöglicht es ein SD-WAN, die datenintensive Vernetzung von verteilten Unternehmensstandorten zu skalieren und unter höchsten Datenschutzanforderungen für standortübergreifendes Arbeiten zu implementieren. Ihr Vorteil: Der Vor-Ort-Einsatz von qualifizierten Technikern an den jeweiligen Unternehmensstandorten entfällt und ein reibungsloser Netzwerkbetrieb wird zur „neuen Normalität“.

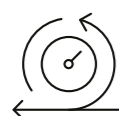
## Sicherer Netzwerkzugang mit cleveren Fernzugriffslösungen

LANCOM Remote & Mobile Access-Lösungen ermöglichen Mitarbeitenden im Büro, zu Hause oder unterwegs einen sicheren und skalierbaren Zugriff auf Unternehmensanwendungen und schützen so das moderne hybride Arbeiten von überall und zu jeder Zeit. Die einzige Voraussetzung ist ein Software-Client auf dem Laptop oder PC. Ist der Zugang einmal konfiguriert, wird mit nur einem Klick eine hochverschlüsselte Verbindung aufgebaut. Ob als klassischer VPN-Client, als Cloud-managed VPN-Client oder nach dem Zero-Trust-Prinzip mit granularen Zugriffsrechten auf bestimmte Anwendungen für einzelne Nutzergruppen: LANCOM Remote & Mobile Access-Lösungen skalieren sowohl für kleine Unternehmen als auch für sehr große Netzwerke mit mehreren tausend Nutzern.

 LANCOM Trusted Access



Automatisierung



Leistung



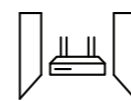
Sicherheit



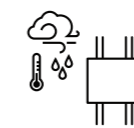
Vertrauen

## Besten Empfang mit professionellen WLAN-Lösungen

Ob Wireless LAN im Außenbereich z. B. in Form von WLAN-Lösungen für Campingplätze, im Innenbereich als klassisches Unternehmens-WLAN, als Gäste-Hotspot oder als besonders belastbares WLAN in Industrie- oder High-Density-Umgebungen benötigt wird: Die Planung einer optimalen WLAN-Abdeckung ist ein Muss.



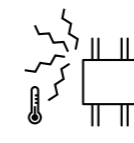
Indoor



Outdoor



High-density



Industrie



Erleben Sie die Zukunft der drahtlosen Konnektivität

LANCOM Wi-Fi 7 Access Points bieten beeindruckende Geschwindigkeiten und extrem niedrige Latenzen. Doch diese Access Points bieten nicht nur die nächste Generation von WLAN, sondern auch ein einzigartiges Angebot für mehr Sicherheit, Nachhaltigkeit und Automatisierung. Erfahren Sie jetzt mehr und stärken Sie bewusst Ihre Digitale Souveränität mit LANCOM Wi-Fi 7!

# KOMPETENZ IN STANDORTVERNETZUNG

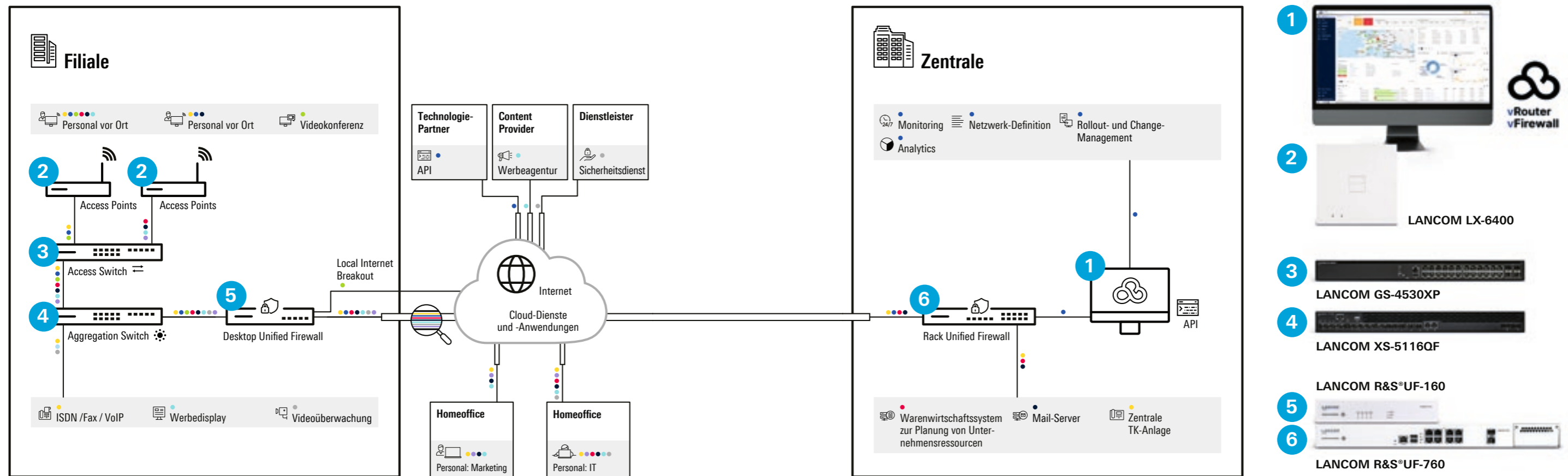
Für Unternehmen, die über mehrere Standorte hinweg arbeiten, ist eine effiziente und sichere Datenkommunikation entscheidend. Als Komplettanbieter garantieren wir mit unseren ganzheitlichen Lösungen beste Netzwerksicherheit und optimierte Verbindungen innerhalb und zwischen den Niederlassungen – ob im Wide Area Network (WAN), Local Area Network (LAN), Wireless Network (WLAN) oder für Remote & Mobile Access-Verbindungen.

Moderne SD-WAN- und SD-Branch-Lösungen spielen dabei eine zentrale Rolle, indem sie die Komplexität des Netzwerks reduzieren und eine einheitliche Verwaltung und einen reibungslosen Betrieb ermöglichen. Basierend auf einem zentralen Netzwerkmanagement über die LANCOM Management Cloud werden Netzwerke konzipiert, automatisch ausgerollt, zuverlässig betrieben und optimiert. Compliance-Anforderungen werden umgesetzt und Anforderungen an Bandbreite, Verbindungsqualität und Anwendungsverfügbarkeit an allen Standorten sichergestellt.

Das Ergebnis ist ein ganzheitliches Management aller Netzwerkprozesse, eine sichere Anbindung aller Standorte und externen Dienstleister sowie eine sichere Netztrennung der verschiedenen digitalen Anwendungen – 100 % DSGVO-konform für Ihre Digitale Souveränität.



## LEISTUNGSSTARKE SD-BRANCH-ORCHESTRIERUNG



# AGILES SD-WAN FÜR ATU

Modernes Netzwerkmanagement für Deutschlands größte Autowerkstattkette mit heute mehr als 500 Filialen

Das SD-WAN ist die Basis für das gesamte ATU-Filialnetz. Es bildet damit das Rückgrat für die Digitalisierung aller Standorte und deren Anbindung an die Unternehmenszentrale. Auch an den lokalen Standorten setzt ATU auf ein umfassendes digitales Netz. Alle Komponenten – von den Filialroutern, Access Points und Switches bis hin zu den Multi-Gigabit-Gateways in der Zentrale – werden über eine zentrale Instanz, die LANCOM Management Cloud (LMC), verwaltet. Zahlreiche automatisierte Prozesse sorgen für ein effizientes und sicheres Management aus der Cloud. Insbesondere beim Rollout und Netzwerkausbau profitiert ATU von Funktionen wie der automatischen Provisionierung aller Geräte.

Redundanz und Zuverlässigkeit spielen bei ATU eine wichtige Rolle. Denn der Ausfall eines Filialrouters oder eines zentralen Gateways kostet nicht nur Nerven, sondern auch Zeit und Geld. ATU setzt vier zentrale Gateways ein, die jeweils in einem eigenen Rechenzentrum an zwei verschiedenen, georedundanten Standorten stehen. Die Filialen verfügen zudem über Backup-Szenarien via Mobilfunk, um eine maximale Verfügbarkeit zu gewährleisten.



Wir wollten eine alternative Lösung zu MPLS umsetzen: eine attraktivere und flexiblere Art der Standortvernetzung. Standard-Breitbandzugang, hohe Zuverlässigkeit, Leistung und eine sichere Verbindung waren die Hauptanforderungen für unsere Standortanbindung.



Volker Hermann  
Teamleiter im Bereich „Communication & Collaboration“ bei der ATU



# HOCHSICHERE VERSCHLÜSSELUNG FÜR BEHÖRDEN

Als erstes Bundesland in Deutschland hat das Saarland eine moderne, flexible und umfassende Verschlüsselung eingeführt

Das Saarland verwendet eine Mehrpunkt-zu-Mehrpunkt-Verschlüsselung inklusive einer modernen Layer-2-Verschlüsselungslösung, die die strengen BSI-Anforderungen für die Übertragung von VS-NfD-Daten erfüllt. Der Ethernet-Verschlüsseler R&S®SITLine ETH verhindert effektiv, dass ausgetauschte Dokumente, Datenströme oder E-Mails von Außenstehenden gelesen werden können. Dieses Konzept wurde im Saarland zweimal separat umgesetzt: einmal für die Polizei und einmal für das IT-Dienstleistungszentrum mit den angeschlossenen Landesbehörden.

Unser Partner T-Systems hat die Detailplanung des Konzepts einschließlich des Rollouts durchgeführt und die Sicherheitslösung implementiert. Dabei wurde nicht nur die Inbetriebnahme der Hardware-Boxen vorbereitet und begleitet, sondern auch die Anpassung an die spezifischen Anforderungen des Landesdatennetzes und der Behörden vorgenommen. Dank der in den Verschlüsselerboxen integrierten Hardware erfahren die User keine Leistungseinbußen.



Die Behörde entschied sich, die bestehende IPsec-basierte Verschlüsselung auf ein neues Niveau zu heben und durch die leistungsfähige Verschlüsselungslösung von Rohde & Schwarz Cybersecurity zu ersetzen.



Marian Rachow  
CEO Rohde & Schwarz Cybersecurity





## Rohde & Schwarz

Rohde & Schwarz setzt sich mit seinen Geschäftsbereichen Test & Measurement, Technology Systems und Networks & Cybersecurity für eine sicherere und vernetzte Welt ein. Seit 90 Jahren setzt der globale Technologiekonzern mit der Entwicklung von Spitzentechnologien neue Maßstäbe. Die führenden Produkte und Lösungen des Unternehmens ermöglichen es Kunden aus Industrie, Behörden und Regierungen, technologische Unabhängigkeit und Digitale Souveränität zu erlangen. Das inhabergeführte Unternehmen mit Sitz in München kann unabhängig, langfristig und nachhaltig agieren.

[www.rohde-schwarz.com](http://www.rohde-schwarz.com)

### Nachhaltiges Produktdesign

Umweltverträglichkeit und ökologischer Fußabdruck  
Energieeffizienz und geringe Emissionen  
Langlebigkeit und optimierte Gesamtbetriebskosten

Certified Quality Management

ISO 9001

Certified Environmental Management

ISO 14001

### Rohde & Schwarz Training

[www.training.rohde-schwarz.com](http://www.training.rohde-schwarz.com)

### Rohde & Schwarz Kundenbetreuung

[www.rohde-schwarz.com/support](http://www.rohde-schwarz.com/support)

