



NETWORKS & CYBERSECURITY

L'innovation au service de réseaux efficaces
et modernes et d'une sécurité effective

ROHDE & SCHWARZ
Make ideas real



À LA RECHERCHE D'UN MONDE SÛR ET CONNECTÉ

Rohde & Schwarz permet aux entreprises et aux États de définir et de maintenir leur souveraineté numérique sur le plan technologique.

L'innovation fait partie intégrante de Rohde & Schwarz depuis ses débuts. Lothar Rohde et Hermann Schwarz, les fondateurs de l'entreprise, étaient des pionniers en matière de technologie. C'est avec un esprit d'entreprise à toute épreuve que ces deux camarades d'études se sont lancés dans le monde de l'ingénierie haute fréquence, encore inexploré à l'époque. Quatre-vingt-dix ans plus tard, cette entreprise privée basée à Munich emploie quelque 13 800 personnes dans le monde, qui ont réalisé un chiffre d'affaires total de 2,78 milliards d'euros au cours de l'exercice 2022/2023.

Dans ses divisions Test et Measurement, Technology Systems et Networks et Cybersecurity, Rohde & Schwarz réalise dès aujourd'hui les innovations de demain. L'expertise de pointe de ce groupe technologique mondial en matière de produits et de solutions permet à ses clients issus des secteurs de l'industrie, de l'administration et de l'armée de façonner leur autodétermination technologique et leur souveraineté numérique.

Grâce à ses solutions réseau, de sécurité et de cryptage, Rohde & Schwarz protège les informations numériques et les processus commerciaux des entreprises et des institutions publiques contre les effets des cyberattaques.

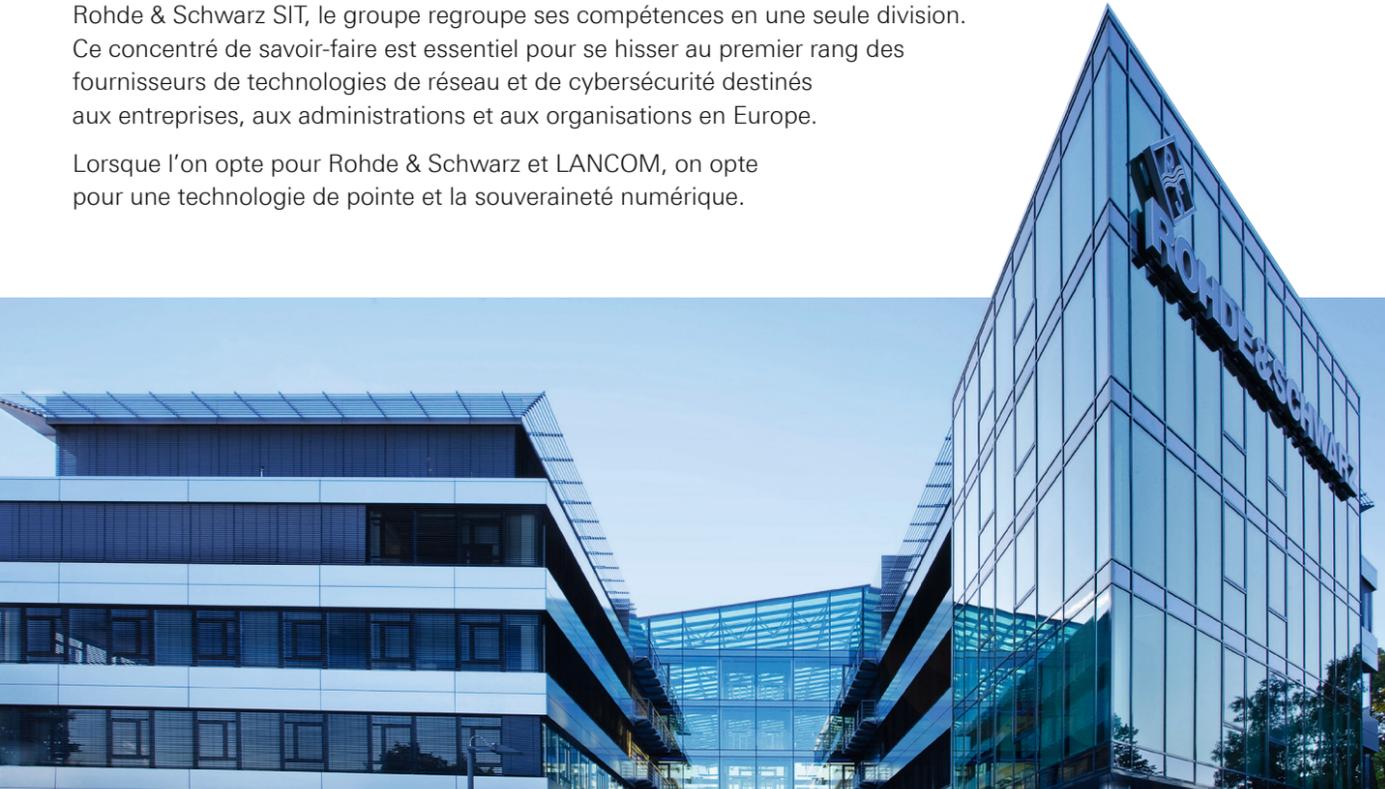
Le volume de données augmente de manière exponentielle. Dans le même temps, les menaces potentielles qui pèsent sur les entreprises, les autorités et les infrastructures critiques augmentent. Selon les estimations d'organisations sérieuses, les cyberattaques, comme le vol de propriété intellectuelle, coûtent chaque année des centaines de milliards d'euros à l'économie mondiale. Mais les valeurs immatérielles ne sont pas les seules à devoir être protégées. Il convient également de protéger les grandes quantités de données sensibles du secteur public ainsi que les données à caractère personnel générées par le secteur privé.

Avec ses filiales LANCOM Systems, Rohde & Schwarz Cybersecurity et Rohde & Schwarz SIT, le groupe regroupe ses compétences en une seule division. Ce concentré de savoir-faire est essentiel pour se hisser au premier rang des fournisseurs de technologies de réseau et de cybersécurité destinés aux entreprises, aux administrations et aux organisations en Europe.

Lorsque l'on opte pour Rohde & Schwarz et LANCOM, on opte pour une technologie de pointe et la souveraineté numérique.

Secur|Ty
made
in
EU

Trust Seal
www.teletrust.de/itsmie



Nos solutions réseau et de cybersécurité renforcent la souveraineté numérique pour les clients publics et commerciaux. Nous assurons la sécurité des appareils mobiles, des ordinateurs portables et des PC grâce à un portfolio complet de solutions de cryptage à haut débit pour centres de données, de solutions VPN pour les réseaux sécurisés des organisations réparties sur plusieurs sites, de passerelles SD-WAN et de firewalls UTM pour la sécurisation des périmètres informatiques, ainsi que de solutions de gestion de réseau basées sur le cloud.



Ralf Koenzen
Vice-président exécutif Networks & Cybersecurity

Contenu

- 02 Introduction
- 03 Contenu
- 04 Rohde & Schwarz, Networks & Cybersecurity
- 06 La souveraineté numérique en tant que tâche stratégique et politique visant à renforcer les compétences
- 08 L'innovation au service de réseaux efficaces et modernes et d'une sécurité effective
- 10 Des solutions réseau fiables pour les entreprises et les États
- 11 Produits de cybersécurité pour les clients des secteurs public et privé
- 12 Communiquer de manière hautement sécurisée avec l'iPhone et l'iPad – R&S®ComSec supporting indigo
- 14 Chiffrement du réseau – R&S®SITLine
- 16 Contrôle de sécurité centralisé – R&S®Trusted Object Manager
- 18 Chiffrement complet du disque dur – R&S®Trusted Disk Solution
- 20 Le navigateur de confiance R&S®, un gage de sécurité pour l'application la plus importante au sein de l'entreprise
- 22 R&S®ELCRODAT, une solution cryptographique de qualité supérieure
- 24 Sécurité du réseau
- 26 Le firewall Unified en rack, un gage de sécurité du réseau pour les grandes entreprises réparties sur plusieurs sites
- 28 Excellente gestion du réseau – LANCOM Management Cloud
- 30 Interconnexion sûre et fiable des sites
- 32 Compétence en matière de connectivité sur site
- 34 Cas d'utilisation – SD-WAN agile pour ATU et cryptage hautement sécurisé pour les autorités

ROHDE & SCHWARZ, NETWORKS & CYBERSECURITY

La division Networks & Cybersecurity de Rohde & Schwarz offre la sécurité des terminaux, des réseaux sécurisés et une cryptographie de qualité supérieure. Avec des produits « Engineered in Germany », nous assurons une transmission de données fiable et sécurisée et sommes spécialisés dans les secteurs du service public, des infrastructures critiques, de la défense, de la santé, du commerce de détail et des PME. Nous sommes un fournisseur de choix offrant un soutien durable aux organisations, aux gouvernements et aux forces armées en matière de planification, de déploiement, d'exploitation et d'optimisation de leurs défis liés au réseau et à la cybersécurité.



Secteur public, infrastructures critiques (KRITIS)

Économie

Machines et Équipements Électriques

- 4 millions de périphériques réseau installés
- 100 000 sites connectés
- >500 produits
- Cryptographie hautement sécurisée pour la défense
- Souveraineté numérique

LA SOUVERAINETÉ NUMÉRIQUE EN TANT QUE TÂCHE STRATÉGIQUE ET POLITIQUE POUR RENFORCER LES COMPÉTENCES

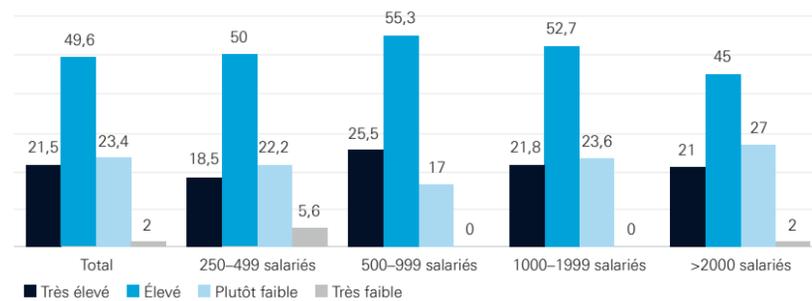
Selon le ministère fédéral allemand de l'Économie et de la Protection du climat (BMWK), la souveraineté numérique « est un sujet d'une grande importance. Les pénuries d'approvisionnement en puces informatiques ont montré à quel point la dépendance vis-à-vis de producteurs non européens peut rapidement freiner des secteurs économiques importants comme l'industrie automobile. »

Nous aussi, nous voyons la numérisation comme une opportunité pour l'Europe de renforcer ses propres compétences et coopérations. Car ce n'est qu'ainsi que nous pourrions consolider notre position dans les domaines des technologies. Le BMWK considère clairement qu'il est nécessaire d'agir dans le domaine des « technologies numériques clés (par ex. technologies de réseau, microélectronique, technologies de sécurité, technologies quantiques, blockchain) ». Les compétences européennes doivent être préservées et développées ici.

Par souveraineté numérique, nous entendons la capacité de décider nous-mêmes de ce que nous faisons. Il s'agit notamment de la compétence décisionnelle, de la compétence d'action et de la capacité à évaluer le risque lié aux dépendances. Une entreprise souveraine sur le plan numérique peut, selon la définition de bitkom, « choisir de manière autonome et en toute confiance entre des alternatives de partenaires performants et dignes de confiance ».

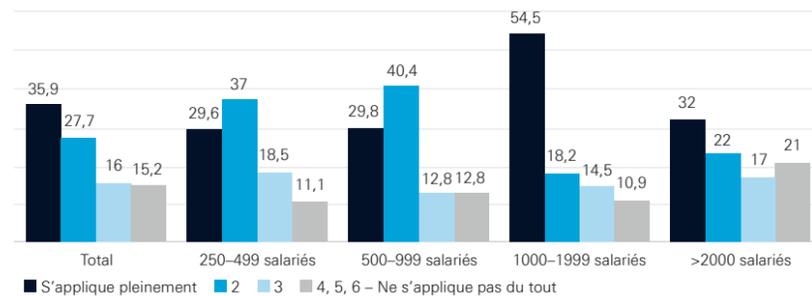
La souveraineté numérique se distingue ainsi de la dépendance numérique – un état qui n'est probablement souhaitable pour aucune entreprise – et de l'autarcie numérique. Ce dernier point n'est généralement pas réalisable dans notre monde globalisé.

Quelle importance accordez-vous actuellement au thème de la souveraineté numérique dans votre entreprise ?



Source : étude du Handelsblatt, 032023, données en %, échelle à 4 points, N/A non incluse dans le graphique

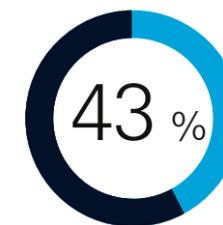
Lorsque nous envisageons d'acheter/d'intégrer des composants de fabricants non européens, nous évaluons les opportunités et les risques que cela implique.



Source : étude du Handelsblatt, 032023, données en %, échelle à 6 points, N/A non incluse dans le graphique

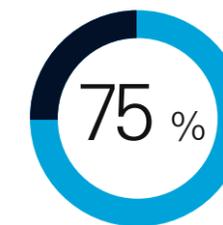


« Le matériel que nous utilisons provient de fabricants de l'UE. »



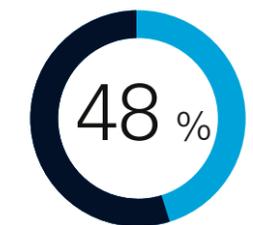
Le matériel informatique est généralement acheté auprès de fabricants situés en dehors de l'UE.
(■ = 3-6/ne s'applique pas du tout)

« En cas de panne, nous pouvons rétablir nos processus de manière autonome ou avec l'aide de partenaires de confiance. »



La capacité à rétablir de manière autonome les processus informatiques en cas de panne est de 75 %, ce qui est considéré comme élevé.
(■ = 1-2/s'applique pleinement)

« Nous n'avons pas besoin de recourir à une aide extérieure pour mettre en œuvre des mesures suffisantes en termes de dispositions de sécurité informatique, de transfert de compétences et de gestion de crise. »



Dépendance à vis-à-vis d'une aide extérieure pour les mesures de sécurité, les compétences, la gestion de crise.
(■ = 3-6/ne s'applique pas du tout)

Source : étude du Handelsblatt, 032023, données en %, échelle à 4 points, N/A non incluse dans le graphique, normalisée à 100 %



L'INNOVATION POUR DES RÉSEAUX EFFICACES ET MODERNES ET UNE SÉCURITÉ EFFECTIVE



LANCOM MANAGEMENT CLOUD

Un réseau qui fonctionne bien est le nerf de la guerre de toutes les entreprises. Cependant, installer et contrôler un tel réseau peut prendre beaucoup de temps et être source d'erreurs. Dans un monde informatique de plus en plus complexe et où la pénurie de personnel qualifié se généralise, vous avez donc besoin d'un centre de contrôle fiable pour votre réseau. Gérez l'ensemble de vos opérations réseau WAN, LAN, Wi-Fi et de sécurité de manière dynamique à partir d'une plateforme unique basée sur le cloud, de manière aussi automatisée que vous le souhaitez.



INTERCONNEXION DE SITES SÉCURISÉE POUR LES SCÉNARIOS SD-WAN DE GRANDE ENVERGURE

Les très grands réseaux IP multi-services ont besoin de hautes performances et d'une fiabilité élevée sur le site central. Une passerelle multi-gigabit comme le LANCOM ISG-8000 constitue le noyau sécurisé et hautement performant de votre SD-WAN. Grâce à une plateforme performante dotée des technologies de cryptage les plus modernes, d'un VPN à haute évolutivité et de fonctions de redondance étendues, vous disposez d'un réseau étendu défini par logiciel (SD-WAN) qui facilite grandement vos tâches administratives.



CHIFFREMENT DE RÉSEAU POUR UNE COMMUNICATION NUMÉRIQUE HAUTEMENT SÉCURISÉE

Nos crypteurs de réseau R&S®SITLine protègent les clients du secteur public et commercial contre l'espionnage et la manipulation des données transmises par Ethernet via le réseau fixe, les fréquences hertziennes ou les satellites. Ils répondent aux multiples exigences des institutions publiques, des entreprises et des infrastructures critiques, qui peuvent compter sur des solutions conçues et adaptées spécialement à leurs besoins.



COMMUNICATION HAUTEMENT SÉCURISÉE AVEC L'IPHONE ET L'IPAD

La solution R&S®ComSec basée sur Indigo allie confort et sécurité dans le cadre du travail avec des données sensibles sur iPhone et iPad selon la norme s'appliquant aux informations classifiées comme étant à diffusion restreinte (diffusion restreinte - réservé à un usage professionnel) et facilite le travail quotidien des utilisateurs travaillant au sein d'administrations et dans des environnements sensibles en termes de sécurité. La solution R&S®ComSec offre des avantages considérables aux organisations et aux entreprises qui préfèrent recourir à une communication mobile sécurisée via des terminaux mobiles qui répondent aux exigences de sécurité les plus élevées pour effectuer leurs tâches quotidiennes, sans pour autant renoncer à leur confort.

DES SOLUTIONS RÉSEAU FIABLES POUR LES ENTREPRISES ET LES ÉTATS

Le développement de logiciels et de matériel ainsi que la fabrication ont lieu principalement en Allemagne, tout comme l'hébergement de la gestion de réseau (LANCOM Management Cloud). Une attention particulière est accordée à la fourniture de solutions fiables avec d'excellentes caractéristiques de sécurité. De plus, l'absence de portes dérobées est une caractéristique de protection essentielle des produits. Le label de confiance « IT-Security Made in Germany » et une certification du bureau fédéral allemand pour la sécurité de l'information (BSI) confirment la fiabilité et le niveau exceptionnel en matière de sécurité.

DES PRODUITS DE CYBERSÉCURITÉ POUR LES CLIENTS DES SECTEURS PUBLIC ET PRIVÉ

Les produits de Rohde & Schwarz Cybersecurity protègent les clients du secteur public et du secteur privé ayant des exigences particulières en matière de sécurité et de certification contre les cybermenaces en constante évolution. Nous développons et produisons un chiffrement réseau à haut débit et une sécurité des points d'accès basée sur le principe Zero-Trust. La plupart de ces produits primés sont approuvés par le bureau fédéral allemand pour la sécurité de l'information (BSI) en tant que dispositifs de sécurisation des données classifiées comme étant à diffusion restreinte. Ces solutions de sécurité de confiance aident les utilisateurs à évoluer vers un monde numérique plus sûr.



Switchs LANCOM

Le portfolio de switchs Gigabit Ethernet de LANCOM est la base des infrastructures réseau modernes dans tous les secteurs et domaines d'application. Il existe des variantes parfaitement adaptées avec Power over Ethernet (PoE) et un nombre variable de ports pour différents débits et applications (1G, 2,5G, 10G, 25G, 40G, 50G, 100G).



Routeurs LANCOM et SD-WAN

Les passerelles de site central SD-WAN garantissent des performances et une fiabilité élevées au niveau du site central. Les routeurs VPN LANCOM garantissent des bandes passantes élevées, une communication sécurisée et la confidentialité des échanges de données sur les réseaux professionnels.



Points d'accès LANCOM

Les points d'accès LANCOM permettent d'accéder au réseau sans fil dans tous les environnements imaginables - à l'extérieur, en intérieur ou dans des environnements industriels difficiles. Ils répondent aussi bien aux exigences les plus élevées en termes de qualité du matériel (durée de vie, évolution de la température, etc.) qu'en termes de flexibilité et de sécurité du logiciel sur lequel ils reposent.



Crypteur de réseau R&S

Nos crypteurs de réseau protègent les clients du secteur public et commercial contre l'espionnage et la manipulation des données transmises par Ethernet via le réseau fixe, les fréquences hertziennes ou les satellites. Ils répondent aux multiples exigences des institutions publiques, des entreprises et des infrastructures critiques, qui peuvent compter sur des solutions conçues et adaptées spécialement à leurs besoins.



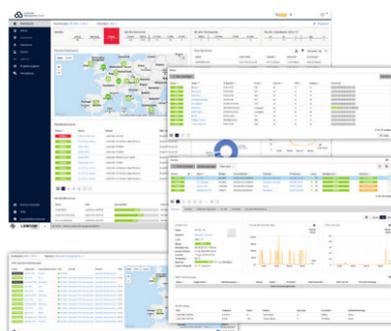
Gestion centralisée de la sécurité R&S

Un niveau de sécurité fiable nécessite un contrôle simple et centralisé. C'est précisément la raison pour laquelle le R&S®Trusted Objects Manager a été conçu. Il permet de configurer et de gérer facilement les produits de sécurité spécialisés. Il offre une interface utilisateur intuitive. Les utilisateurs peuvent facilement gérer la configuration, le déploiement et la surveillance. Une API REST moderne dans le backend permet d'intégrer facilement et rapidement vos systèmes centraux de surveillance et de reporting.



Accès à distance et mobile LANCOM

Offrez à vos collaborateurs un accès sécurisé et extensible aux applications d'entreprise, qu'ils soient au bureau, à domicile ou en déplacement, et protégez ainsi le travail hybride moderne, partout et à tout moment.



LANCOM Management Cloud

Contrôle, optimise et automatise l'ensemble de vos opérations réseau, simplifiant et rationalisant considérablement les flux de travail en éliminant les configurations manuelles individuelles des appareils.



Firewall LANCOM R&S® Unified

Une gestion unifiée des menaces (Unified Threat Management - UTM) complète, associée à l'apprentissage automatique, offre la meilleure protection contre les nouveaux types de virus et de logiciels malveillants. Ces puissants firewalls et accessoires appropriés vous permettent d'étendre votre infrastructure réseau de confiance, basée sur la nouvelle génération de moteur d'inspection profonde des paquets.



R&S® ComSec

R&S®ComSec allie confort et sécurité dans le cadre du travail avec des données sensibles sur iPhone et iPad, selon la norme s'appliquant aux informations classifiées dans la catégorie à diffusion restreinte, ce qui facilite le travail quotidien des utilisateurs travaillant au sein des administrations et dans des environnements où la sécurité est primordiale.



Sécurité des terminaux R&S

Le processus de cryptage transparent en temps réel garantit une sécurité maximale – sans aucune restriction de productivité. Le cryptage intégral des disques durs pour systèmes Windows et les supports de données externes protège les données utilisateur classifiées dans la catégorie à diffusion restreinte, les fichiers temporaires et l'ensemble du système d'exploitation, notamment contre les vols ou les sabotages.



Dispositifs cryptographiques R&S

Le R&S®ELCRODAT 7-MC est un dispositif de cryptographie tactique robuste permettant de crypter et de décrypter les communications vocales et de données pour les classifications de sécurité allemandes, de l'UE et de l'OTAN jusqu'à SECRET.

COMMUNIQUER DE MANIÈRE HAUTEMENT SÉCURISÉE AVEC L'IPHONE ET L'IPAD

Solution R&S®ComSec utilisant indigo

La solution R&S®ComSec utilisant indigo allie confort et sécurité dans le cadre du travail avec des données sensibles sur iPhone et iPad selon la norme s'appliquant aux informations classifiées dans la catégorie à diffusion restreinte et facilite le travail quotidien des collaborateurs travaillant dans des administrations ou dans des environnements où la sécurité est primordiale.

Avec la solution R&S®ComSec utilisant indigo, les organisations et les entreprises qui préfèrent opter pour une communication mobile sécurisée via des terminaux mobiles qui répondent aux exigences de sécurité les plus élevées pour effectuer leurs tâches quotidiennes, font un grand pas en avant.

CARACTÉRISTIQUES PARTICULIÈRES DE LA SOLUTION R&S®COMSEC SUPPORTING INDIGO

Appareils standard et mises à jour garanties

Les smartphones et les tablettes standard peuvent être utilisés. Le fournisseur garantit des mises à jour gratuites pendant au moins 5 ans. Il est possible de les revendre lorsqu'ils ne sont plus utilisés, et il est fort probable que les prix de revente soient élevés.

Un seul appareil – pour une utilisation professionnelle privée et sécurisée

Un seul appareil mobile permet de remplir deux fonctions : l'utilisation privée et l'utilisation protégée, le tout sans négliger le respect des directives s'appliquant aux informations classifiées dans la catégorie à diffusion restreinte. E-mail, calendrier, contacts et, en option, Messenger ; les navigateurs Intranet peuvent être utilisés comme applications standard préinstallées dans le domaine hautement sécurisé – ce n'est pas une solution conteneur.

La solution R&S®ComSec utilisant indigo a été approuvée par le BSI

La plateforme indigo a été approuvée par le bureau fédéral allemand pour la sécurité de l'information (BSI) en octobre 2022. En raison de la confirmation de la sécurité de la plateforme par le BSI, aucune carte à puce ou carte SD supplémentaire n'est nécessaire pour assurer la sécurité.

Composants diffusion restreinte

La solution utilise trois composants principaux : un smartphone ou une tablette en tant que terminal, une passerelle VPN respectant les directives s'appliquant aux informations classifiées dans la catégorie à diffusion restreinte et un MDM.

Une solution – de la planification à l'exploitation

Les deux spécialistes de la sécurité Rohde & Schwarz Cybersecurity et agilimo Consulting proposent une solution complète : backend VPN complet, Mobile Device Management (MDM) et gestion automatisée des certificats.



Ce partenariat spécial entre Rohde & Schwarz Cybersecurity et agilimo Consulting offre aux autorités, aux organisations et aux entreprises une solution sophistiquée, utilisable au quotidien, qui répond aux exigences de sécurité du BSI pour le traitement des données cryptées selon la norme relative à la catégorie à diffusion restreinte. Conçu en Allemagne.

SecurTy
made
in
EU

Trust Seal
www.teletrust.de/itsmie

CRYPTAGE DE RÉSEAU

Avec plus de 30 ans d'expertise en matière de cryptographie, Rohde & Schwarz Cybersecurity fait partie des pionniers dans le domaine du cryptage réseau à haut débit. L'entreprise couvre l'ensemble de la chaîne de valeur et garantit ainsi le plus haut niveau de confiance et de fiabilité qui soit. Nos crypteurs de réseau protègent les autorités publiques et les clients du secteur commercial contre l'espionnage et la manipulation des données transmises par Ethernet via le réseau fixe, les fréquences hertziennes ou les satellites.

Ils répondent aux multiples exigences des institutions publiques, des entreprises et des infrastructures critiques, qui peuvent compter sur des solutions conçues et adaptées spécialement à leurs besoins.

Avantages de nos crypteurs de réseau

- ▶ « La sécurité informatique made in Germany » – plus de 30 ans de compétence en matière de cryptographie
- ▶ Du matériel et des logiciels spécialement conçus pour des performances de cryptage de pointe
- ▶ Des méthodes et des normes cryptographiques de pointe
- ▶ Grande facilité d'utilisation grâce au système central de gestion de la sécurité
- ▶ Approuvé par le BSI :

VS-NfD (RESTRICTED), EU & NATO RESTRICTED

R&S®SITLine ETH

Disponible dans différentes classes de performance, cette architecture matérielle et logicielle moderne, combinée au dernier cri en matière de cryptographie, offre une sécurité durable et à long terme pour votre infrastructure. Ce nouvel appareil haute performance a un débit de 2 x 100 Gbit/s.



UN TRANSFERT DE DONNÉES PERFORMANT ET SÉCURISÉ

L'intégration de solutions de cybersécurité dans les entreprises est un investissement dans la pérennité et la résilience de votre organisation. Chez Rohde & Schwarz Cybersecurity, nous pensons que la sécurité informatique fait partie intégrante de la chaîne de valeur. Cette approche nous permet de proposer des solutions de sécurité qui non seulement protègent contre les cyberattaques, mais qui soutiennent également le fonctionnement sans interruption de vos processus commerciaux, assurant ainsi la continuité de vos activités commerciales.

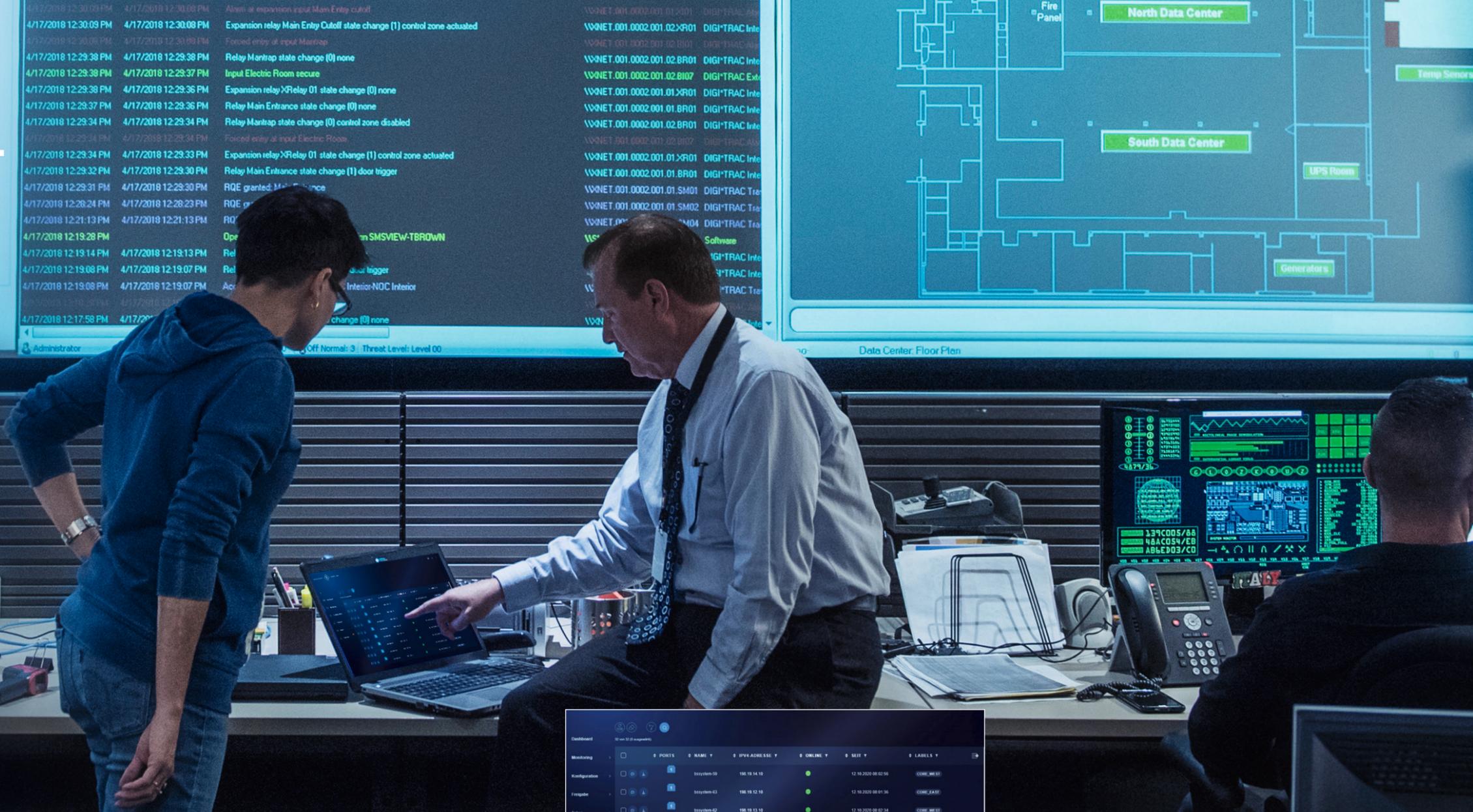
Nos solutions se caractérisent par des performances de pointe associées à un temps de réaction rapide. Nos clients bénéficient à la fois d'une technologie de sécurité de pointe et de la certitude de pouvoir compter sur le service compétent et fiable de Rohde & Schwarz en cas d'incident affectant la sécurité ou de besoin d'assistance technique. La confiance dans la marque Rohde & Schwarz repose sur des décennies d'expérience et sur une compréhension approfondie des exigences de différents secteurs en matière de cybersécurité.

En fin de compte, en investissant dans les solutions de cybersécurité de Rohde & Schwarz, vous êtes non seulement sûr d'être protégé contre les menaces de plus en plus complexes du cyberspace, mais vous vous assurez également l'intégrité et la disponibilité de vos données et systèmes critiques. Votre entreprise est ainsi assurée de pouvoir continuer à fonctionner avec succès et en toute sécurité dans un monde de plus en plus interconnecté et numérisé.

CONTRÔLE DE SÉCURITÉ CENTRAL

R&S®Trusted Objects Manager

Un niveau de sécurité fiable nécessite un contrôle simple et centralisé. C'est précisément cette fonction que remplit le R&S®Trusted Objects Manager. Il permet de configurer et de gérer facilement les produits de sécurité spécialisés. Ce système permet aux administrateurs informatiques d'accéder à et de contrôler des applications telles que R&S®Trusted VPN, R&S®Trusted Disk, R&S®Trusted Identity Manager et R&S®Trusted VPN Client. En installant une seule instance du R&S®Trusted Objects Manager, les utilisateurs peuvent gérer tous ces produits sans interruption, ce qui permet d'atteindre jusqu'à 50 000 clients. La compatibilité avec différents services d'annuaire LDAP, notamment Microsoft Active Directory, Lotus Domino et Novell eDirectory et OpenLDAP, garantit une intégration sans interruption dans des environnements réseau de différentes tailles. Les utilisateurs et les groupes d'utilisateurs peuvent être facilement importés à partir des structures LDAP existantes. Afin d'augmenter la fiabilité et la résilience, il est possible d'intégrer des R&S®Trusted Objects Manager supplémentaires en tant qu'instances de veille. Il s'agit d'une option de mise à l'échelle en fonction du niveau d'extension requis.



LES PROPRIÉTÉS SPÉCIALES DE LA COMMANDE CENTRALISÉE AVEC LE R&S®TRUSTED OBJECT MANAGER :

Utilisation intuitive du Manager

Le R&S®Trusted Objects Manager se caractérise par un guidage de l'utilisateur orienté processus offrant une expérience utilisateur intuitive, ainsi que par sa flexibilité en matière de gestion des utilisateurs et des droits. Un administrateur informatique peut gérer l'ensemble du cycle de fonctionnement des composants de cybersécurité de Rohde & Schwarz via une interface Web sécurisée. En outre, l'infrastructure à clé publique (PKI) intégrée en option présente l'avantage de pouvoir être exploitée de manière autonome et indépendamment de fournisseurs tiers.

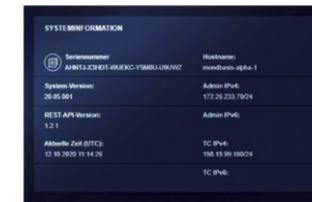
Sécurité maximale grâce à une infrastructure à clé publique (PKI) disponible en option

Il est également possible d'intégrer en option une infrastructure à clé publique (PKI) via le R&S®Trusted Objects Manager – un composant de sécurité assurant une plus grande confidentialité, intégrité et authenticité des données. L'infrastructure à clé publique (PKI) peut être mise en place et exploitée de manière autonome, sans l'intervention de tiers. R&S Cybersecurity vous assiste lors de la configuration.



VS-NfD-, EU & NATO RESTRICTED-ready

Les R&S®Trusted Objects Manager sont certifiés par le bureau fédéral allemand pour la sécurité de l'information (BSI) et autorisés à traiter les données classifiées VS-NfD, EU & NATO RESTRICTED. Les institutions publiques et les entreprises privées peuvent ainsi sécuriser leurs postes de travail et leurs appareils de stockage portables de manière à pouvoir stocker et traiter des informations classifiées comme étant à diffusion restreinte.



L'effet protecteur d'un environnement sécurisé dépend directement de l'efficacité avec laquelle le contrôle des composants respectifs est intégré dans les processus. Les R&S®Trusted Objects Manager sont des assistants numériques employés au quotidien pour gérer les composants de sécurité R&S de manière simple et sûre. En partant du processus d'exploitation, l'accent est mis sur l'utilisation intuitive de l'unité de commande centrale. En particulier lorsqu'il s'agit de réduire considérablement la complexité des processus et d'éliminer les sources d'erreur.

Engineered in Germany

CRYPTAGE INTÉGRAL DU DISQUE DUR

Solution R&S®Trusted-Disk

Le processus de cryptage transparent en temps réel garantit une sécurité maximale sans aucune restriction de productivité. Le cryptage intégral des disques durs pour systèmes Windows et supports de données externes protège les données utilisateur classifiées dans la catégorie à diffusion restreinte, les fichiers temporaires et l'ensemble du système d'exploitation sur tous les disques durs internes de vos ordinateurs, les supports de données externes USB et Thunderbolt, notamment contre les vols ou les sabotages. La solution R&S®Trusted-Disk garantit la productivité illimitée de tous les ordinateurs (portables, ordinateurs de bureau, systèmes de serveurs) grâce à un cryptage transparent en temps réel – basé sur une certification du bureau fédéral allemand pour la sécurité de l'information (BSI) assortie d'une approbation VS-NfD (diffusion restreinte). Pour bénéficier d'un accès sécurisé, il faut par exemple utiliser des cartes à puce comme les badges électroniques de service et militaires. Ainsi, même en cas de vol de supports de données portables ou d'ordinateurs portables, vos données sont protégées de manière sûre contre la perte de données sensibles.

CARACTÉRISTIQUES PARTICULIÈRES DU R&S®TRUSTED DISK :

Sécurité renforcée grâce à une cryptographie haut de gamme

La solution R&S®Trusted-Disk utilise des algorithmes de cryptage hautement sécurisés tels qu'AES-XTS avec une longueur de clé de 512 bits et un système de camouflage RSA. Elle utilise les bibliothèques cryptographiques sécurisées de Botan et permet un effacement sécurisé des données. Elle offre également une authentification utilisateur dans le processus d'authentification avant l'amorçage, basé sur une carte à puce et un code PIN. Cette solution utilise des mécanismes d'amorçage sécurisés et un chargeur d'amorçage SHIM. Cette technologie comprend également la génération de nombres aléatoires actuels et le recalcul flexible des clés de cryptage en fonction du temps et des données écrites.

Protection étendue également pour les supports de données mobiles

De plus, les supports de stockage portables populaires et pratiques tels que les clés USB, les lecteurs Thunderbolt et les disques durs externes peuvent être cryptés et authentifiés en toute sécurité. C'est justement là que cette solution offre une protection des données efficace en cas de vol des supports de données mobiles.

Gestion centralisée des terminaux protégés

La gestion centralisée des droits d'accès des utilisateurs permet d'adapter les installations de manière rapide et flexible. La prise en charge du démarrage sécurisé avec le chargeur d'amorçage SHIM de Microsoft facilite et accélère les déploiements à grande échelle.

VS-NfD, EU & NATO RESTRICTED

Toutes les solutions R&S®Trusted Disk sont certifiées par le bureau fédéral allemand pour la sécurité de l'information (BSI) et autorisées à traiter les données classifiées VS-NfD, EU & NATO RESTRICTED. Les institutions publiques et les entreprises privées peuvent ainsi sécuriser leurs postes de travail et leurs appareils de stockage portables de manière à pouvoir stocker et traiter des informations classifiées comme étant à diffusion restreinte.

Qualification du fabricant pour la procédure d'approbation qualifiée du BSI s'appliquant aux données classifiées comme étant à diffusion restreinte

La protection contre les pertes de données et les cyberattaques constitue un risque pour la continuité des activités des institutions publiques et des entreprises. Selon l'étude TÜV Cybersecurity 2022, une entreprise allemande sur dix a déjà été touchée par une cyberattaque. Les menaces sont donc réelles et les conséquences peuvent être dévastatrices. En effet, le monde du travail et ses processus de travail quotidiens sont plus numériques que jamais, et les données sont la ressource la plus précieuse en matière de création de valeur numérique.

Les solutions R&S®Trusted Disk vous protégeront contre ces menaces. Elles utilisent les technologies de cryptage les plus modernes pour protéger vos données contre les modifications, le sabotage et le vol de supports de données. Ne faites pas de compromis en matière de sécurité. Agissez dès maintenant pour sécuriser vos stocks de données et protéger votre institution ou votre entreprise en ajoutant un élément important supplémentaire pour contrer les menaces croissantes du monde cybernétique.

LA SÉCURITÉ POUR L'APPLICATION LA PLUS IMPORTANTE AU SEIN DE L'ENTREPRISE

R&S®Trusted Browser

Avec R&S®Trusted Browser, vous bénéficiez d'une sécurité native qui protège chaque appareil dans chaque réseau. Cela englobe l'ensemble des menaces basées sur le Web. Protégez vos données grâce à des politiques de données applicables de manière granulaire, qui permettent de déplacer librement les données entre les applications d'entreprise tout en empêchant les fuites de données. R&S®Trusted Browser contrôle de manière fiable les contenus du navigateur.

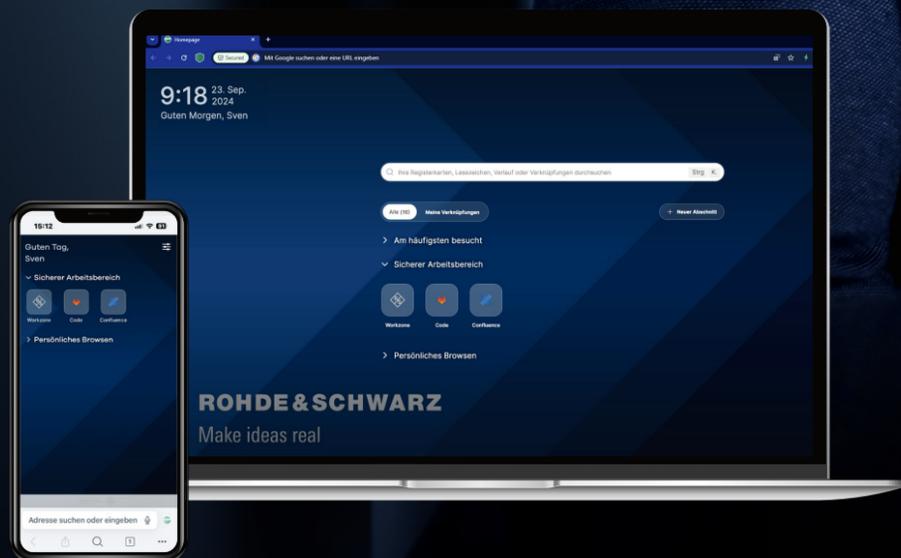
En outre, R&S®Trusted Browser vous permet de contrôler l'accès des utilisateurs aux données, ce qui augmente la sécurité. Les détails des sessions d'application peuvent être consignés en détail.

R&S®Trusted Browser authentifie chaque utilisateur et tout accès qu'il génère, ce qui permet d'atteindre une plus grande transparence. En font notamment partie le contrôle de l'accès aux sites Web, les téléchargements/téléversements, les captures d'écran, le copier/coller de contenus/données et le filtrage des contenus indésirables (p. ex. les pop-ups).

GESTION EFFICACE DES PARAMÈTRES DE SÉCURITÉ POUR LA NAVIGATION

La création de directives exhaustives ainsi qu'une configuration centralisée permettent d'automatiser efficacement les processus de travail courants. Les appareils privés (BYOD) peuvent également être intégrés au service d'entreprise.

R&S®Trusted Browser contribue à améliorer de manière significative la conformité aux cadres de certification courants (par ex. ISO 27000).



CARACTÉRISTIQUES R&S®TRUSTED BROWSER

Séparation entre usage privé et professionnel

Séparation transparente, côté navigateur, des domaines privé et professionnel et contrôle centralisé de l'interaction entre ces deux domaines

Protéger les données sensibles

Possibilités de journalisation (dernier kilomètre) des accès sensibles aux données, y compris des données agrégées sur le comportement des utilisateurs

Navigation sécurisée

Navigation sûre pour l'utilisateur grâce au filtrage des différents sites Web et à la création de catégories de risques. Il est également possible de bloquer des sites Web en fonction de l'endroit où l'utilisateur se trouve.

Prise en charge complète

Rohde & Schwarz Cybersecurity fournit une assistance à la mise en œuvre de politiques et de directives spécifiques, ainsi qu'une assistance à l'intégration, une formation et une assistance.

Conformité BSI et multi-plateforme

Conformité des navigateurs Web aux exigences de sécurité du BSI par rapport aux navigateurs standard

- Communication fiable (certificats et présentation de la forme de communication)
- Protection des données de confiance (transmission des données de télémétrie)
- Compatible avec les ordinateurs de bureau, les tablettes, les appareils mobiles fonctionnant avec Windows et macOS



SOLUTION CRYPTOGRAPHIQUE DE QUALITÉ SUPÉRIEURE

Sécurité robuste HF/VHF/UHF/IP pour la voix et les données

Le R&S®ELCRODAT 7-MC est un dispositif de cryptographie tactique robuste permettant de crypter et de décrypter les communications vocales et de données pour les classifications de sécurité allemandes, de l'UE et de l'OTAN jusqu'à SECRET. Il est résistant à TEMPEST et interopérable avec les fréquences radio HF/VHF/UHF, les communications par satellite, les lignes de télécommunications et l'infrastructure IP. Il est parfait pour une utilisation sur des plateformes fixes et mobiles en terrain accidenté, en mer et dans les airs.

LES FAITS MARQUANTS DE LA SOLUTION

- ▶ Protège les lignes HF/VHF/UHF, les communications par satellite et les lignes de télécommunication
- ▶ Prend en charge les protocoles de cryptage IP tels que NINE et SCIP
- ▶ Débits pouvant atteindre jusqu'à 1 Gbit/s
- ▶ Extrêmement résistant, inviolable, résistant à TEMPEST
- ▶ Opérations stationnaires et mobiles dans tous les domaines militaires (armée de terre, marine, armée de l'air)
- ▶ Idéal pour la manipulation et la gestion par l'utilisateur final grâce à sa petite taille et à sa configuration simplifiée
- ▶ Possibilité de mise à jour grâce au téléchargement sécurisé du logiciel, ce qui permet de relever les défis futurs
- ▶ Matériel pour les applications futures, par exemple la cryptographie post-quantique

Le R&S®ELCRODAT 7-MC est conçu pour remplacer son prédécesseur, le R&S®ELCRODAT 4-2.

Avec son architecture matérielle et logicielle moderne, il offre également les capacités nécessaires pour les protocoles de cryptographie modernes, y compris les algorithmes post-quantiques et des débits de données allant jusqu'à 1 Gbit/s. Le R&S®ELCRODAT 7-MC peut être utilisé de manière flexible. Il offre des interfaces en série pouvant être utilisées dans des environnements sans fil et modem traditionnels, ainsi que des interfaces Ethernet pour l'intégration aux réseaux IP. En outre, il peut installer, stocker et exécuter plusieurs applications cryptographiques qui mettent en œuvre différents modes de cryptographie, ce qui permet un déploiement flexible pour différents scénarios nationaux et de coalition. Le R&S®ELCRODAT 7-MC peut être utilisé soit avec un dispositif de commande, soit via une interface Web, soit via le module de bus MIL.

R&S®ELCRODAT 7-FN pour les applications SCIP

Une solution cryptographique pour la communication d'informations confidentielles auprès des autorités et du secteur public : la voix, la vidéo et les données sont cryptées conformément à la norme internationale SCIP et transmises sur des réseaux IP avec l'infrastructure de télécommunication VoIP standard. La solution est homologuée pour la classification jusqu'à SECRET et une homologation pour les normes OTAN et SECRET UE est en cours de planification. Le dispositif cryptographique R&S®ELCRODAT 7-FN convient aussi bien aux environnements de bureau qu'aux conditions environnementales difficiles. Il offre les fonctions habituelles et modernes des systèmes de téléphonie et vidéo. Le cryptage de bout en bout garantit que les informations ne sont jamais disponibles en clair entre la source et la destination (par exemple, dans l'infrastructure de commutation).



SÉCURITÉ DU RÉSEAU

Pour une entreprise, la priorité absolue en matière de sécurité réseau est la protection technique et organisationnelle de son infrastructure informatique interne, avec l'ensemble des données, systèmes, appareils et applications – pour une numérisation souveraine et sûre sur le plan numérique. Rester à jour en matière de sécurité réseau est une tâche sans fin : les entreprises sont confrontées quotidiennement à des formes complexes de cyber-attaques (p.ex. Advanced Persistent Threats) et à de nouvelles directives (par ex. NIS2) qui exigent sans cesse de nouvelles mesures de protection plus sophistiquées.

LA SOLUTION : ADOPTER UNE PROTECTION MULTICOUCHE

Sécurité informatique de base

- Stockage sécurisé des données (« data in rest ») comprenant des paramètres de sécurité pour les fichiers, des droits d'accès et de traitement clairement définis et des sauvegardes de données
- Protection des équipements informatiques physiques, y compris les serveurs et le contrôle d'accès réseau (NAC), contre les accès non autorisés grâce à un système central de gestion unifiée des menaces (UTM) de nouvelle génération (par ex. LANCOM R&S® Unified Firewalls) et à la mise en œuvre des fonctionnalités qui en découlent, telles que les patchs de sécurité à intervalles réguliers, les contrôles fonctionnels, les mises à jour logicielles, la mise en bac à sable avec apprentissage automatique, la segmentation du réseau et la gestion des droits
- Renforcement de la sensibilisation des collaborateurs à la sécurité par des formations et des cours de remise à niveau sur la sécurité informatique et la conformité, des simulations de phishing et des directives de sécurité

La sécurité informatique dans le quotidien professionnel

- Sécurité des terminaux (par ex. appareils mobiles et IoT) grâce à des droits d'accès individuels à fine granularité qui sont octroyés à chaque utilisateur (par ex. LANCOM Trusted Access Client)
- Cryptage des données via des réseaux VPN en utilisant des paramètres et des algorithmes de cryptage conformes à la norme BSI actuelle
- Sécurité des applications grâce à la surveillance/au contrôle des applications et au recours à des normes de sécurité actuelles

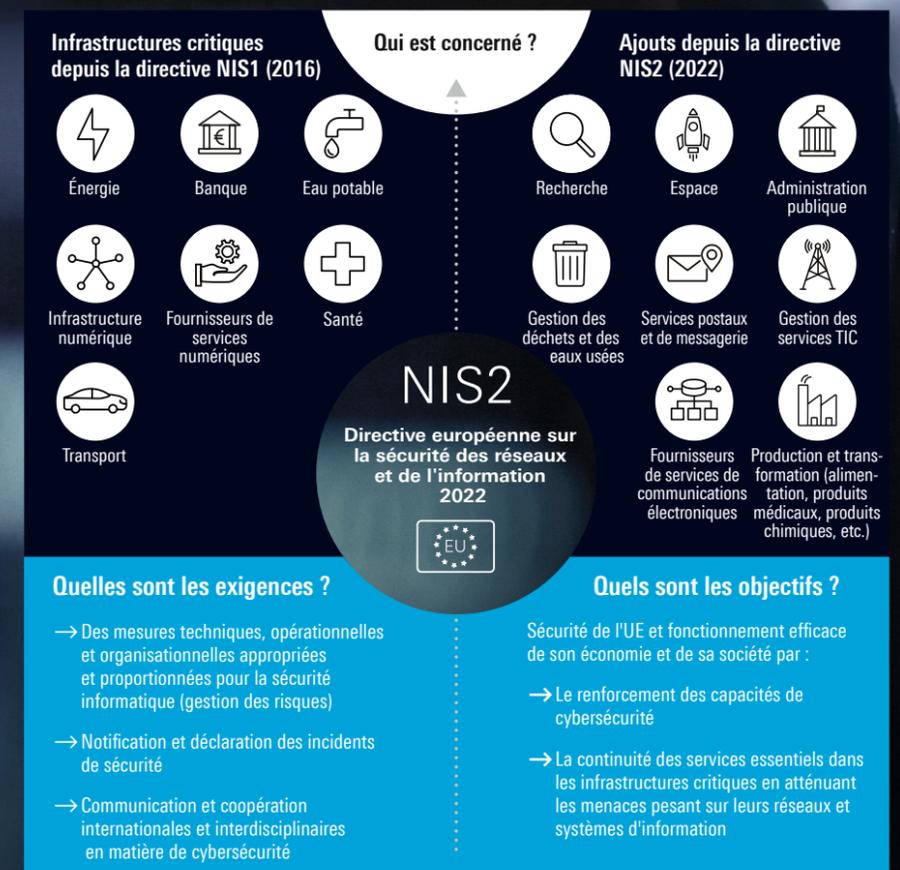
Sécurité de transmission

- Protection latérale de votre propre réseau (« data in motion »), par exemple grâce à la segmentation du réseau (VLAN) et aux routines de mise en cache pour empêcher l'accès public
- Utilisation et traitement des données conformes à la législation avec des applications et des systèmes conformes au RGPD, des composants réseau sans backdoor et des services de cloud hébergés au sein de l'UE
- Sécurité du cloud grâce à la redondance géographique et à l'examen de la sécurité des services cloud externes utilisés

Faites-vous une idée précise des lignes directrices sur la sécurité des réseaux et de l'information (NIS2)

La directive NIS2 est l'instruction publiée en décembre 2022 par la Commission européenne visant à transposer certaines mesures de sécurité des réseaux dans le droit national avant le 17 octobre 2024.

L'objectif explicite est d'améliorer la résilience des infrastructures critiques telles que définies dans le Programme européen pour la protection des infrastructures critiques (PEPIC) – telles que les entreprises du secteur de la santé, de la recherche, des services postaux ou de l'administration publique – et d'augmenter ainsi le niveau général de la cybersécurité au sein de l'UE.



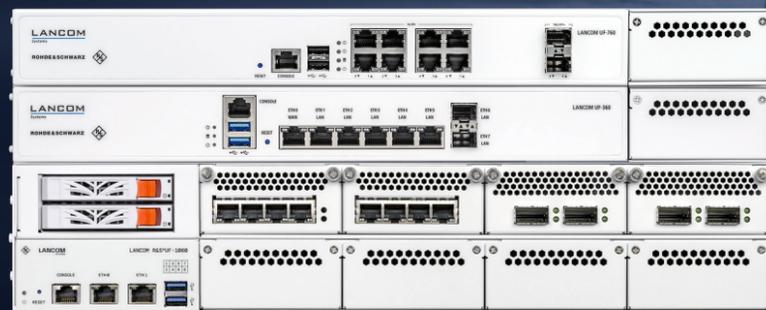
LA SÉCURITÉ DU RÉSEAU POUR LES GRANDES-ENTREPRISES RÉPARTIES SUR PLUSIEURS SITES

Phishing, menaces persistantes avancées, attaques DDoS...

La situation de menace qui pèse sur les entreprises s'aggrave de jour en jour. Les entreprises en pleine croissance, réparties sur plusieurs sites et dotées de réseaux sophistiqués et d'un volume de données important ont particulièrement besoin de technologies performantes en matière de sécurité. Avec les modèles en rack des firewalls de nouvelle génération (NGFW), vous misez sur une solution de sécurité globale grâce à la gestion unifiée des menaces (UTM, Unified Threat Management). Avec le concept « One-Click Security » de LANCOM Management Cloud, des architectures de sécurité adaptées sont mises en place de manière automatisée, transparente et simple. Tous les firewalls LANCOM R&S®Unified sont développés en Allemagne et garantissent l'absence de backdoor.

FIREWALL UNIFIED EN RACK

- ▶ Sécurité de nouvelle génération grâce à l'UTM « Engineered in Germany » protégeant contre les spams, les virus et les logiciels malveillants ainsi que les cyberattaques, avec absence de backdoor garantie
- ▶ Techniques de sécurité de pointe telles que l'inspection approfondie des paquets R&S® PACE2 et l'inspection SSL
- ▶ Sécurité préventive contre les menaces encore inconnues grâce à la mise en bac à sable et à l'apprentissage automatique
- ▶ Règles d'application et de filtrage propres via la gestion des applications et les filtres de contenu
- ▶ Gestion pratique des firewalls grâce à une interface Web intuitive, à LANCOM Management Cloud ou à LANCOM R&S®UF Command Center
- ▶ Modules d'extension LANCOM UF pour l'extension de port disponibles séparément pour une flexibilité maximale
- ▶ Également disponible en tant que firewall virtuel basé sur un logiciel (LANCOM vFirewall)
- ▶ Fonctionnement en cluster haute disponibilité (cluster HD) possible sans coûts ni licences supplémentaires
- ▶ Modèle de licence basé sur la durée (1, 3 ou 5 ans)



POINTS FORTS

Notre promesse de sécurité : la sécurité nouvelle génération avec UTM

Face aux menaces croissantes qui pèsent sur le Web, une sécurité digne de confiance est loin d'être un fait acquis. Véritables piliers de la sécurité des réseaux, les firewalls de nouvelle génération (NGFW) combinent des mécanismes de sécurité courants avec des technologies de dernière génération. Dans la triade de la sécurité, de la conformité et de la convivialité, la protection efficace de votre réseau et la prévention maximale contre les menaces encore inconnues sont prioritaires - cette promesse s'applique sans restriction à tous les firewalls Unified LANCOM R&S®, qu'il s'agisse d'un modèle de bureau ou d'un modèle en rack. Tous les firewalls LANCOM R&S®Unified sont développés en Allemagne, sont garantis sans accès cachés (backdoor) et portent donc le label de confiance « IT Security made in Germany ».

Puissant : des firewalls aux performances convaincantes

Tant les grandes entreprises réparties sur plusieurs sites que les campus ont des exigences particulièrement élevées en matière de débit de données pour les firewalls. Nos modèles en rack hautement performants et à l'épreuve du temps séduisent également dans les grandes infrastructures informatiques présentant un volume de données élevé et concentré. L'UF-1060 en particulier, avec ses performances d'interface de 100G et d'UTM de 10G, offre la performance nécessaire pour mettre en œuvre, côté central, des fonctions de sécurité à haut débit pour les infrastructures des succursales. Grâce aux modules d'extension disponibles en option, vous pouvez ajouter des ports supplémentaires aux modèles en rack des firewalls LANCOM R&S®Unified pour une flexibilité de connexion maximale et ainsi les adapter individuellement à vos besoins en matière de réseau.

Clair : convivialité intuitive

C'est surtout dans les grands réseaux d'entreprises et campus, qui comportent de nombreuses règles en matière de firewall, qu'une gestion simple de ces derniers vaut de l'or. C'est pourquoi les firewalls LANCOM R&S®Unified offrent un concept d'utilisation intuitif « easy to use » qui met l'accent sur une représentation graphique claire de vos paramètres. Cela permet non seulement de minimiser les sources d'erreur potentielles, mais aussi de gagner beaucoup de temps lors du dépannage. Les firewalls vous offrent ainsi un quotidien sans stress, vous permettant de vous concentrer entièrement sur votre entreprise, sans vous soucier de la sécurité de votre réseau.

EXCELLENTE GESTION DU RÉSEAU

LANCOM Management Cloud

La gestion de réseau avec LANCOM, c'est la sécurité, le routage, la commutation et le Wi-Fi depuis le cloud ! Le LANCOM Management Cloud (LMC) permet de contrôler l'ensemble de l'infrastructure réseau avec notre portfolio composé de firewalls R&S®Unified, de passerelles SD-WAN, de switches et même de points d'accès via un seul système. C'est vous qui décidez si vous voulez migrer tout de suite l'ensemble de votre réseau vers une gestion innovante du cloud ou si vous voulez le faire étape par étape : une migration successive de certains sites est possible sans problème.



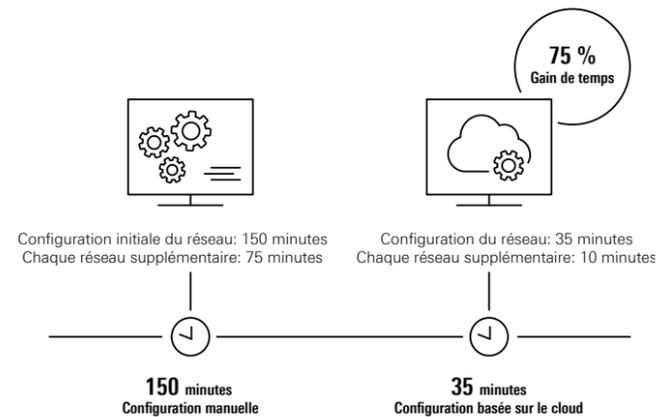
GESTION DE RÉSEAU DANS UNE NOUVELLE ÈRE

Puissance accrue. Sécurité renforcée.

Le succès de votre entreprise dépend en grande partie d'une infrastructure de réseau puissante et sécurisée. Grâce à l'harmonisation optimale de tous les composants impliqués, le LANCOM Management Cloud optimise énormément la vitesse et l'efficacité de votre réseau. Les fonctions d'analyse et d'optimisation du trafic exploitent au mieux la bande passante de votre réseau.

Une productivité maximale.

En tant que centre de contrôle pour votre réseau, le LANCOM Management Cloud est l'outil de déploiement et de maintenance par excellence pour les concepteurs de réseaux. Les ajustements de configuration, les mises à jour de firmware, le monitoring, les déploiements et les corrections d'erreurs selon vos instructions sont réalisés automatiquement et efficacement. Attendez-vous à un gain de temps de 75 %.



Automatisation avec LANCOM Active Radio Control™ 2.0.

LANCOM Active Radio Control™ 2.0 est la réponse à des réseaux de plus en plus complexes en lien avec une pression croissante sur les coûts et une pénurie de spécialistes en informatique : la solution d'automatisation auto-apprenante optimise les installations Wi-Fi sur la base des données d'utilisation réelles et minimise la charge de travail pour les administrateurs informatiques. Véritable nouveauté sur le marché de l'optimisation du réseau Wi-Fi, LANCOM Active Radio Control™ 2.0 est en instance de brevet et offre la meilleure expérience utilisateur possible pour chaque scénario : du Wi-Fi de bureau, d'hôtel ou d'hôpital aux grandes installations dans les stades et les salles de spectacle.

Retour sur investissement immédiat

Les administrateurs informatiques consacrent en moyenne 40 % de leur temps de travail à la résolution de problèmes. Le LMC permet d'utiliser de manière beaucoup plus efficace des ressources précieuses telles que la main-d'œuvre, le temps et l'argent, en particulier lorsqu'il s'agit de réseaux répartis sur de nombreux sites.

Sans intervention coûteuse sur place, vous mettez en service des sites complets, mettez à disposition de nouvelles applications ou optimisez les infrastructures Wi-Fi les plus complexes sur la base des données d'utilisation réelles en un clic de souris. Le LMC aide à maîtriser les dépenses courantes et à mettre en place des entreprises légères et durables pour l'avenir.

INTERCONNEXION SÛRE ET FIABLE DES SITES

Une connexion bien au-delà du réseau

L'interconnexion professionnelle de sites vise à assurer des processus de travail fluides et une communication claire et fluide, qu'il s'agisse de données et de signaux ou de personnes. Les deux éléments doivent être en constante évolution et faire progresser l'entreprise. Il faut ici une approche globale avec des solutions WAN, LAN, Wi-Fi, de sécurité et d'accès à distance harmonisées entre elles.

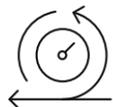


Interconnexion indépendante des sites avec SD-WAN et SD-Branch

Un Software-defined Wide Area Network (SD-WAN, réseau étendu à définition logicielle) remplace les infrastructures réseau traditionnelles, statiques et configurées manuellement. En même temps, un SD-WAN permet de faire évoluer l'interconnexion à forte intensité de données d'entreprises réparties sur plusieurs sites et de la mettre en œuvre en respectant les exigences les plus strictes en matière de protection des données pour un travail sur plusieurs sites. Votre avantage : l'intervention sur place de techniciens qualifiés sur les différents sites de l'entreprise n'est plus nécessaire et un fonctionnement sans interruption du réseau devient la « nouvelle normalité ».



Automatisation



Puissance



Sécurité



Confiance

 LANCOM Trusted Access



Accès réseau sécurisé avec des solutions d'accès à distance intelligentes

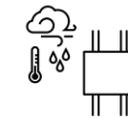
Les solutions d'accès à distance et mobile LANCOM offrent à vos collaborateurs un accès sécurisé et extensible aux applications d'entreprise, qu'ils soient au bureau, à domicile ou en déplacement, et protégez ainsi le travail hybride moderne, partout et à tout moment. La seule condition préalable est d'avoir un logiciel client sur l'ordinateur portable ou le PC. Une fois l'accès configuré, une connexion hautement cryptée est établie en un seul clic. Qu'il s'agisse d'un client VPN classique, d'un client VPN géré dans le cloud ou selon le principe Zero-Trust avec des droits d'accès granulaires à certaines applications pour des groupes d'utilisateurs individuels, les solutions d'accès distant et mobile de LANCOM s'adaptent aussi bien aux petites entreprises qu'aux très grands réseaux comptant plusieurs milliers d'utilisateurs.

Meilleure réception avec des solutions Wi-fi professionnelles

Que vous ayez besoin d'un réseau Wi-Fi à l'extérieur, par exemple sous la forme de solutions Wi-Fi pour les campings, à l'intérieur comme réseau Wi-Fi classique d'entreprise, comme hotspot pour les invités ou comme réseau Wi-Fi particulièrement résistant dans des environnements industriels ou à haute densité, il est indispensable de disposer d'une couverture réseau optimale :



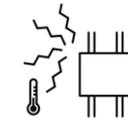
Intérieur



Extérieur



Haute densité



Industrie



Découvrez l'avenir de la connectivité sans fil

Les points d'accès LANCOM Wi-Fi 7 offrent des vitesses impressionnantes et des latences extrêmement faibles. Mais ces points d'accès ne se contentent pas d'offrir la prochaine génération de réseau Wi-Fi, ils proposent également une offre unique pour plus de sécurité, de durabilité et d'automatisation. Apprenez-en plus maintenant et renforcez consciemment votre souveraineté numérique avec LANCOM Wi-Fi 7

COMPÉTENCE EN MATIÈRE D'INTERCONNEXION DES SITES

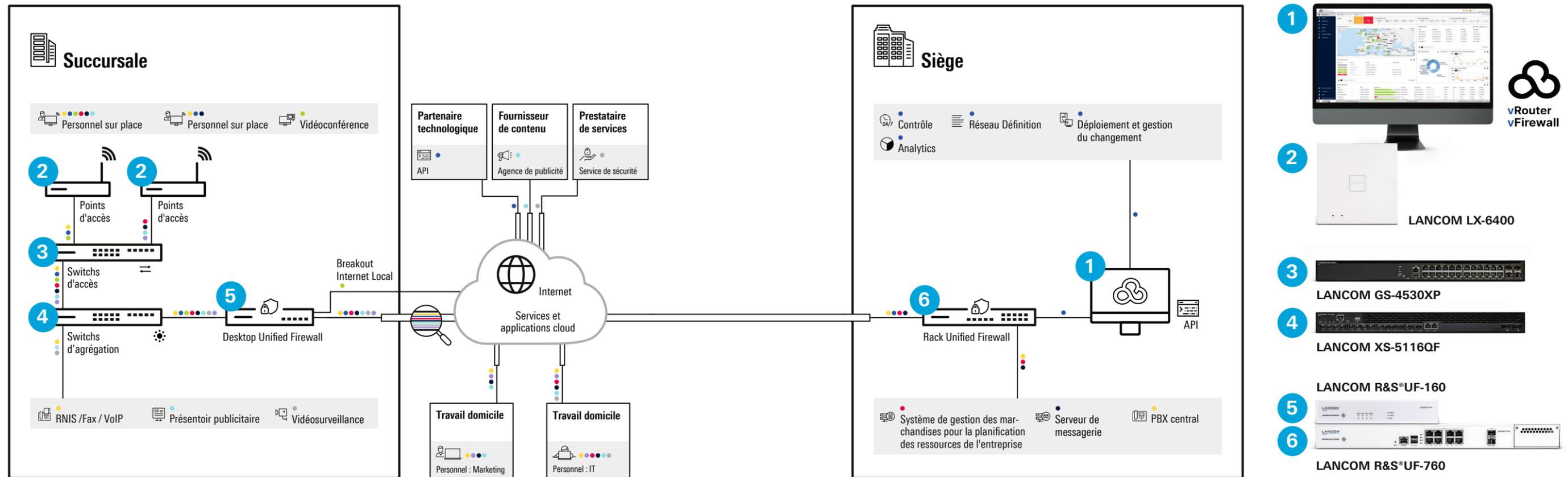
Pour les entreprises qui travaillent sur plusieurs sites, une communication de données efficace et sécurisée est essentielle. En tant que fournisseur de solutions complètes, nous garantissons, grâce à nos solutions globales, la meilleure sécurité réseau et des connexions optimisées au sein des succursales et entre ces dernières – que ce soit sur le Wide Area Network (réseau étendu, WAN), le Local Area Network (réseau local, LAN), le réseau sans fil (Wi-Fi) ou pour les connexions d'accès à distance et mobiles.

En réduisant la complexité du réseau et en permettant une gestion et un fonctionnement sans interruption, les solutions SD-WAN et SD-Branch modernes jouent un rôle central. Sur la base d'une gestion centralisée du réseau via le LANCOM Management Cloud, les réseaux sont conçus, déployés automatiquement, exploités de manière fiable et optimisés. Les exigences en matière de conformité sont mises en œuvre et les exigences en matière de bande passante, de qualité de connexion et de disponibilité des applications sont garanties sur tous les sites.

Il en résulte une gestion globale de tous les processus réseau, une connexion sécurisée de tous les sites et prestataires de services externes ainsi qu'une séparation réseau sécurisée des différentes applications numériques – 100 % conforme au RGPD pour votre souveraineté numérique.



ORCHESTRATION PERFORMANTE DE SD-BRANCH



SD-WAN AGILE POUR ATU

Gestion de réseau moderne pour la plus grande chaîne de garages automobiles d'Allemagne, qui compte aujourd'hui plus de 500 succursales

Le SD-WAN est la base de l'ensemble du réseau de succursales ATU. Il constitue ainsi l'épine dorsale de la numérisation de tous les sites et de leur connexion au siège de l'entreprise. ATU mise également sur un réseau numérique complet sur les sites locaux. Tous les composants sont gérés par une instance centrale, le LANCOM Management Cloud (LMC), depuis les routeurs des succursales jusqu'aux passerelles multi-gigabit de la centrale, en passant par les points d'accès et les switches. De nombreux processus automatisés assurent une gestion efficace et sécurisée à partir du cloud. En particulier lors du déploiement et de l'extension du réseau, ATU profite de fonctions telles que l'auto-provisioning de tous les appareils.

La redondance et la fiabilité jouent un rôle important chez ATU. En effet, non seulement les pannes de routeurs de succursales ou d'une passerelle centrale sont néfastes pour les nerfs, mais elles coûtent aussi beaucoup de temps et d'argent. ATU utilise quatre passerelles centrales, chacune située dans son propre centre de données sur deux sites géo-redondants différents. Les succursales disposent également de scénarios de sauvegarde via la téléphonie mobile pour garantir une disponibilité maximale.



Nous voulions mettre en œuvre une solution alternative à MPLS : un type d'interconnexion des sites plus attrayant et plus flexible. Un accès haut débit standard, une grande fiabilité, des performances élevées et une connexion sécurisée étaient les principales exigences relatives à l'interconnexion de nos sites.



Volker Hermann

Chef d'équipe dans le domaine « Communication & Collaboration » auprès d'ATU



CRYPTAGE HAUTEMENT SÉCURISÉ POUR LES AUTORITÉS

La Sarre a été le premier land allemand à introduire un cryptage moderne, flexible et complet

La Sarre utilise un cryptage multipoint à multipoint, y compris une solution de cryptage moderne de couche 2, qui répond aux exigences strictes du BSI en matière de transmission de données à diffusion restreinte. Le crypteur Ethernet R&S®SITLine ETH permet d'éviter de manière efficace la lecture par des personnes extérieures des documents, flux de données ou e-mails échangés. Ce concept a été mis en œuvre séparément à deux reprises en Sarre : une fois pour le compte de la police et une fois pour le compte du centre de services informatiques et des autorités du land qui y sont rattachées.

Notre partenaire T-Systems a réalisé la planification détaillée du concept, y compris le déploiement, et a mis en œuvre la solution de sécurité. Il s'agissait non seulement de préparer et d'accompagner la mise en service du matériel, mais aussi de l'adapter aux exigences spécifiques du réseau de données du land et des autorités. Grâce au matériel intégré aux boîtiers de cryptage, les utilisateurs ne subissent aucune perte de performance.



Nous avons décidé de porter notre cryptage IP-Sec existant à un niveau supérieur. C'est pourquoi nous avons choisi de le remplacer par la solution de cryptage haute performance de Rohde & Schwarz Cybersecurity.

Ammar Alkassar,

Délégué à l'innovation et à la stratégie et CIO du Land de Sarre



SAARLAND



Rohde & Schwarz

Avec ses divisions Test & Mesure, Technology Systems et Networks & Cybersecurity, Rohde & Schwarz s'engage pour un monde plus sûr et plus interconnecté. Depuis 90 ans, le groupe technologique mondial établit de nouvelles normes en développant des technologies de pointe. Les produits et solutions de pointe de cette entreprise permettent aux clients issus des secteurs de l'industrie, de l'administration et des gouvernements de bénéficier d'une indépendance technologique et d'une souveraineté numérique. Dirigée par ses propriétaires, cette entreprise basée à Munich peut agir de manière indépendante et durable sur le long terme.

www.rohde-schwarz.com

Vers la conception de produits durables

Compatibilité environnementale et empreinte écologique
Efficacité énergétique et faibles émissions
Longévité et total des charges d'exploitation

Certified Quality Management

ISO 9001

Certified Environmental Management

ISO 14001

Formation Rohde & Schwarz

www.training.rohde-schwarz.com

Assistance clientèle de Rohde & Schwarz

www.rohde-schwarz.com/support



R&S® est une marque déposée de Rohde & Schwarz

Les noms propres sont des marques déposées de leurs propriétaires respectifs

PD 3685.0611.63 | Version 01.00 | December 2024 (sj)

Networks & Cybersecurity

Les données sans spécifications de précision

sont sans engagement | Sous réserve de modifications

© 2024 Rohde & Schwarz | 81671 Munich