Cybersécurité industrielle

Solutions sûres, rapides et fiables

PHOENIX CONTACT
INSPIRING INNOVATIONS

Cybersécurité Industrielle
La confiance est la base

Nous vivons une époque où le développement des technologies de communication permet à des millions d'appareils de partager et d'échanger des informations dans le monde entier, en particulier dans les usines de fabrication (Industrie 4.0 et Internet des Objets). Naît ainsi la nécessité d'une stratégie pour la sécurité des réseaux et la disponibilité des installations. Selon le rapport Unicri d'Interpol en 2014 (Institut de recherche criminelle des Nations Unies et de la justice), le coût de la criminalité IT en Europe est estimé à 750 milliards d'euros et globalement une perte de 150 000 emplois en Europe. La valeur des dommages découlant de la cybercriminalité avoisine ainsi 0,6% du PIB national.

C'est avec cette prise de conscience que Phoenix Contact développe des propositions pour protéger les systèmes de l'entreprise, la sauvegarde du savoir-faire et de tous les actifs de données sensibles constituant le métier ou le processus de production. Phoenix Contact offre ainsi une sélection riche et variée de solutions permettant d'assurer la sécurité des réseaux de communication industriels. Protéger efficacement les différents sites de production, tel est l'objectif principal de nos solutions.

Savoir-faire :
Phoenix Contact a des années d'expérience dans l'automatisation et depuis la dernière décennie dans les réseaux Ethernet industriels. Nous sommes conscients des attentes et comprenons les besoins qui se posent dans le monde de l'automatisation.

Expert chez les fabricants de machines :
Phoenix Contact est étroitement liée à l'industrie, en particulier dans le monde des constructeurs de machines. Phoenix Contact construit des machines pour son usage interne et comprend donc pleinement les défis quotidiens de ses clients. Machine Building est le nom du département dédié à ce secteur d'activité. Il se trouve au sein même de l'usine principale à Blomberg en Allemagne et compte 180 employés.

Conseil et support :
Un réseau de vente avec plus de 45 filiales et plus de 30 partenaires d'affaires partout dans le monde, assure la proximité et le service à la clientèle en temps réel et directement sur site.

La sécurité dans le domaine automobile

Dans les usines de production du Groupe Volkswagen AG ont été installés des routeurs pare-feu industriels de la famille mGuard de Phoenix Contact pour séparer le réseau complet en 15 sous-réseaux. Chaque sous-réseau est conçu avec des règles de pare-feu afin de fournir une plus grande protection contre les accès non autorisés.

Grâce au logiciel gestionnaire de périphériques MDM, il a été possible de contrôler les différents routeurs pare-feu dans le système de production, en évitant les problèmes de mise à jour de chaque appareil et de transférer des informations sur une mauvaise localisation. Cela a permis une plus grande sécurité de transmission des données dans le réseau et une réduction drastique des erreurs techniques durant les assistances.

Maintenance sécurisée dans l'industrie agro-alimentaire

Un important fabricant international de machines dans l'industrie alimentaire, a choisi le pare-feu / routeur FL mGuard de Phoenix Contact pour assurer une maintenance prédictive efficace. Grâce à sa configuration flexible, le client a pu installer celui-ci dans une de ses machines.
Ce système permet un contrôle constant de l'ensemble de la ligne de production et empêche tout arrêt; certains composants de la machine sont soumis à une usure plus importante que les autres, et il était donc nécessaire de contrôler les machines avec une plus grande attention, et de mettre en place une surveillance continue des entraînements asservis. Les capteurs enregistrent divers paramètres, y compris la température des moteurs d'asservissement, et les données résultantes sont transmises en temps réel au constructeur de la machine.
En cas de dépassement des tolérances prescrites, le système peut envoyer automatiquement une alerte et informer votre équipe support afin de démarrer une intervention précoce pour éviter les temps d'arrêt importants.

La transmission des données à la hausse
Propagation mondiale du réseau industriel

Nous constatons une augmentation des télé-services, utiles pour réduire les coûts des interventions lors du traitement d'une problématique. L'Industrie 4.0, l'Internet des Objets et Smart Grid représentent ainsi la situation d'aujourd'hui. L'Industrie 4.0 est nécessaire pour l'analyse en temps réel de la production avec des transferts massifs de données sur l'Internet. Dans l'Internet des Objets, nous sommes témoin d'une prolifération de nœuds de réseau, augmentant les cibles potentielles.

Il est donc essentiel d'adopter une stratégie efficace pour la sécurité des réseaux industriels. Cette mise en réseau a d'énormes avantages, mais en même temps, augmente les risques. Vous pouvez, par exemple, propager rapidement un malware à travers ses nouvelles interfaces et initier des menaces (par exemple : un cheval de Troie se propageant depuis une clé USB) causant de graves dommages à la production.

Vous ne pouvez pas toujours installer un antivirus à bord des PC industriels, en particulier dans la production, où des ralentissements causés par ces antivirus risqueraient de compromettre les performances des installations. Phoenix Contact, grâce à son expérience en tant que fabricant de machines et à l'expertise de ses experts Innominate® (Phoenix Contact Cybersecurity) offre une gamme de systèmes et de solutions qui sont en mesure de protéger les réseaux des dangers de sources internes et/ou externes.

Augmentation du nombre de noeuds

Big data

Industrie 4.0

Internet des Objets

Les risques de sécurité dans la production
Les cas les plus courants

Je n'ai pas de pare-feu ou de VPN. il y a un risque de véhiculer des virus ou des logiciels malveillants

Je crains que les exploitants d'installations entrent une clé USB infectée dans un PC de production

Les vieux PC de production avec le système d'exploitation XP **ne sont plus en sécurité** parce qu'il n'est plus supporté par Microsoft

Je ne peux pas utiliser d'antivirus sur la production, car il reduirait les performances du PC et parce qu'il est incompatible avec le système de contrôle

Mes données sont transférées de manière transparente et clairement lisibles

Mon système est toujours connecté à l'Internet 24 heures par jour et les pirates ont tout le temps de **pénétrer** dans mon système de contrôle

Le PC portable du technicien de service peut être infecté, ce qui pourrait constituer une menace pour la sécurité de mon réseau

Maximiser le nombre d'accès à distance sur les machines installées dans l'usine multiplie les risques ; il est alors plus facile de répandre des logiciels malveillants et de s'exposer à un vol de données

Les informations d'identification du technicien sur le PC support pour l'accès à distance à mes machines ont été volées

Les risques pour votre entreprise

On procède en général à une analyse du site et des process afin d'estimer les risques relatifs sur le système industriel ainsi que son interaction avec le système d'information de l'usine. Celle-ci précède la phase de mise en service de contre-mesures adaptées.

L'absence de mesure appropriée pour la sécurité peut devenir très coûteuse.

Perte de données :

Soudain, toutes les données sont perdues. Quel serait le coût de la reconstruction de ces données ?

Perte de savoir-faire :

Un concurrent est en mesure d'accéder à vos données sensibles (conception, ingénierie, ...). Pouvez-vous économiquement chiffrer les dégâts ?

Temps d'arrêt de production :

En raison de problèmes liés à la sécurité, la production doit être arrêtée pour quelques heures ou quelques jours, quel est le coût d'un tel manque de production ?

Heures d'employés :

Combien d'heures travaillées par tous les employés seraient nécessaires pour résoudre les dommages causés par un défaut dans vos mesures de sécurité ?

Réputation:

Comment chiffrer les dommages si votre réputation sur la fiabilité et la sécurité des données de votre entreprise était mise en doute chez vos partenaires ?

Ransomware:

Blocage total de la production et des fichiers. Quel serait le coût de la rançon exigée pour réactiver le processus de production ?

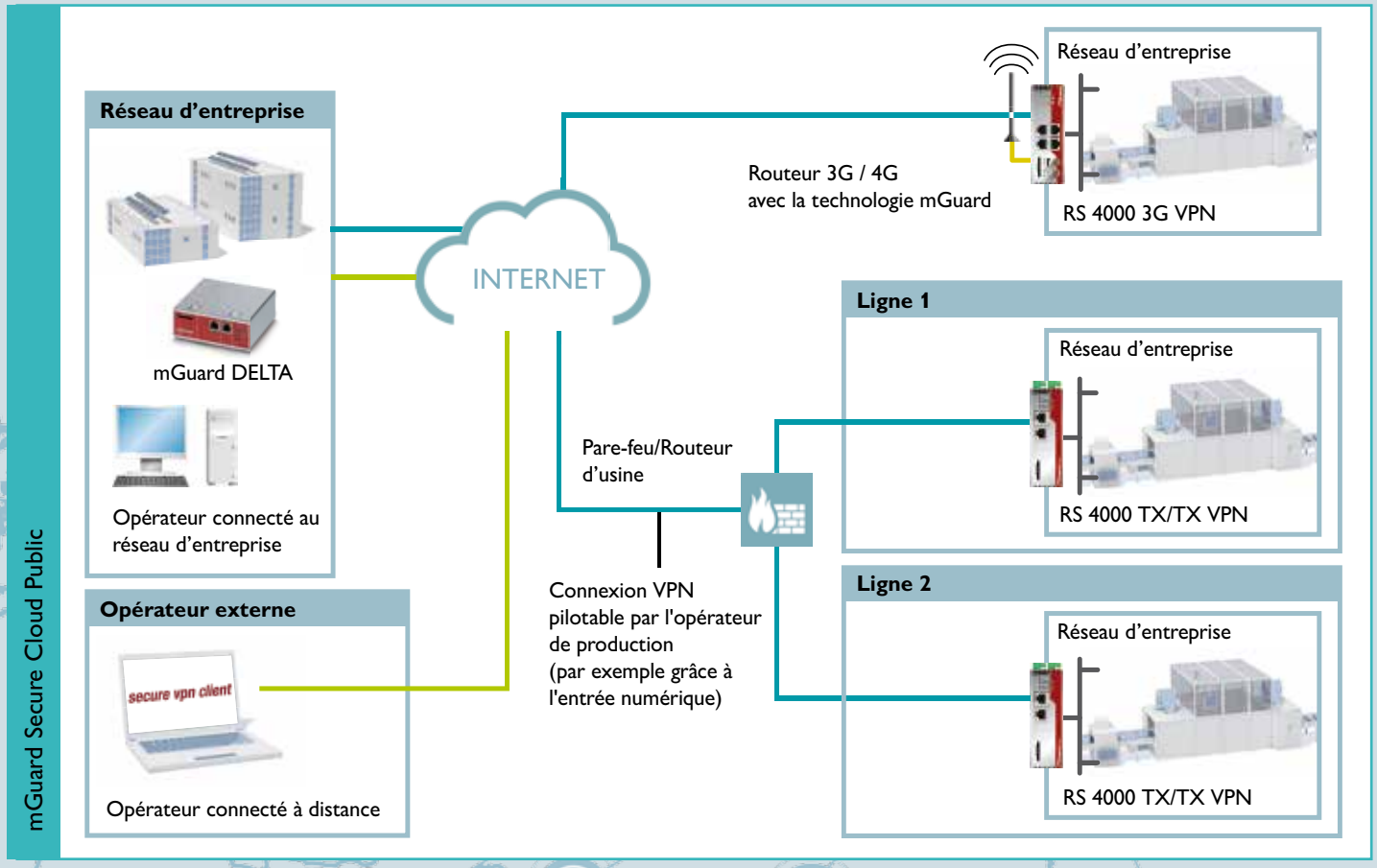
Solution d’assistance à distance Cloud et interne

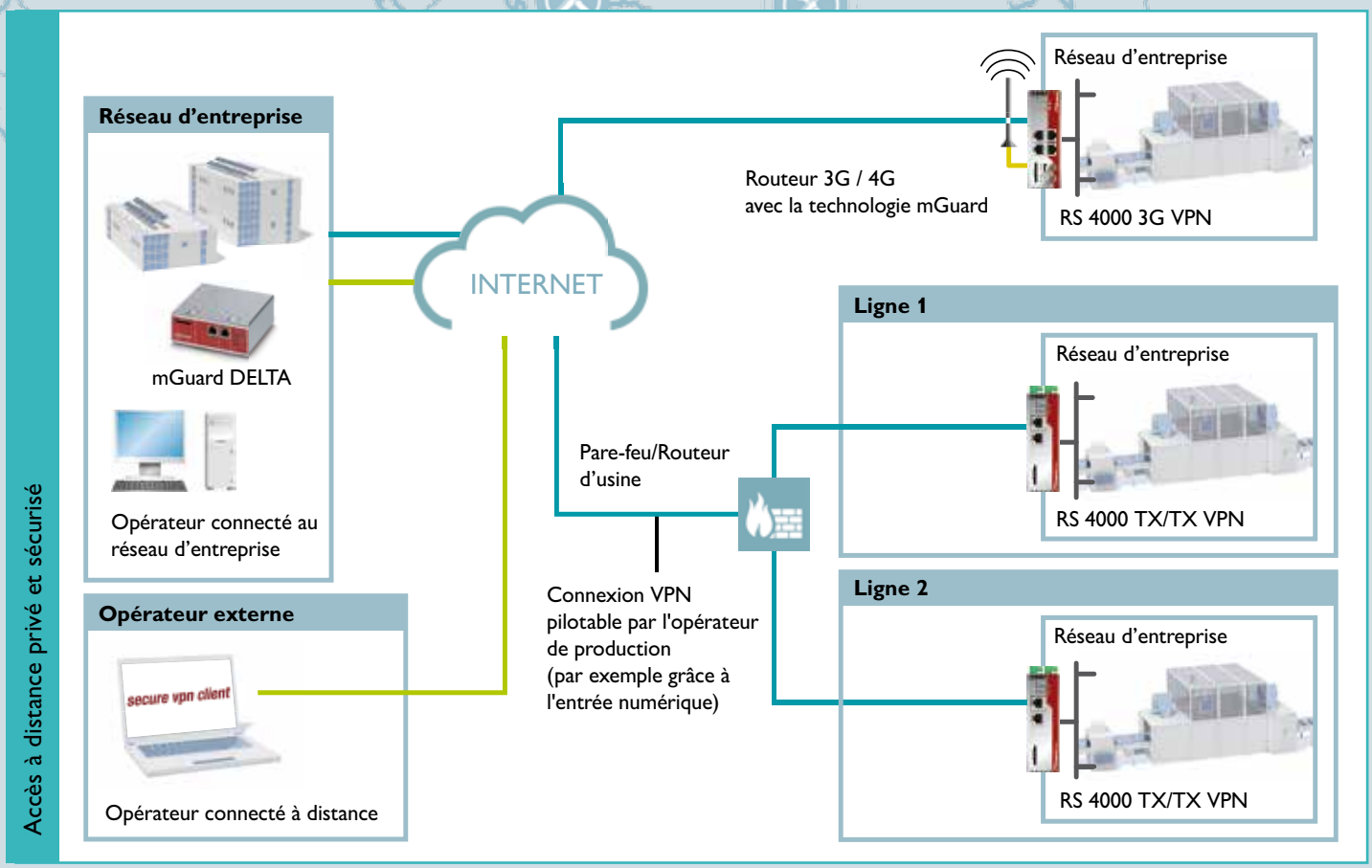
mGuard Secure Cloud Public

L’accès distant sécurisé à une ou plusieurs machines peut être réalisé avec différentes solutions technologiques. La solution mGuard Secure Cloud permet à quiconque de gérer des connexions distantes basées sur le Web, et cela, sans opération invasive sur le domaine informatique du client final. En effet, le pare-feu routeur mGuard génère toujours une communication chiffrée en sortie, qui peut être conditionnée par un contact d’entrée physique sur le mGuard et donc autorisée par le client final sur le site. Une fois authentifié sur le site sécurisé mGuard Secure Cloud, on peut atteindre la machine ou les installations distantes (avec accès aux zones ou aux données opérationnelles). Cette solution est gratuite pour une connexion et nécessite un abonnement annuel pour plusieurs connexions simultanées.

Accès à distance sécurisé privé

La solution InHouse utilise des composants matériels dédiés qui agissent en tant que communication d’infrastructure centralisée. Elle est constituée par un mGuard centerport2 (format 19 pouces 3U), intégrant dans un seul appareil un pare-feu industriel et une gestion de tunnels VPN. Ce dispositif, permet la connexion à un grand nombre de systèmes, de machines ou de techniciens, gère jusqu’à 3000 tunnels VPN simultanément. Cette solution ne nécessite pas d’abonnement annuel.


mGuard Secure Cloud Public
Réseau d'entreprise
mGuard DELTA
Opérateur connecté au réseau d'entreprise
Opérateur externe
secure vpn client
Opérateur connecté à distance
INTERNET
Routeur 3G / 4G avec la technologie mGuard
Réseau d'entreprise
RS 4000 3G VPN
Pare-feu/Routeur d'usine
Connexion VPN pilotable par l'opérateur de production (par exemple grâce à l'entrée numérique)
Ligne 1
Réseau d'entreprise
RS 4000 TX/TX VPN
Ligne 2
Réseau d'entreprise
RS 4000 TX/TX VPN


Accès à distance privé et sécurisé
Réseau d'entreprise
mGuard DELTA
Opérateur connecté au réseau d'entreprise
Opérateur externe
secure vpn client
Opérateur connecté à distance
INTERNET
Routeur 3G / 4G avec la technologie mGuard
Réseau d'entreprise
RS 4000 3G VPN
Pare-feu/Routeur d'usine
Connexion VPN pilotable par l'opérateur de production (par exemple grâce à l'entrée numérique)
Ligne 1
Réseau d'entreprise
RS 4000 TX/TX VPN
Ligne 2
Réseau d'entreprise
RS 4000 TX/TX VPN

Les solutions de sécurité mGuard

Application de routage NAT

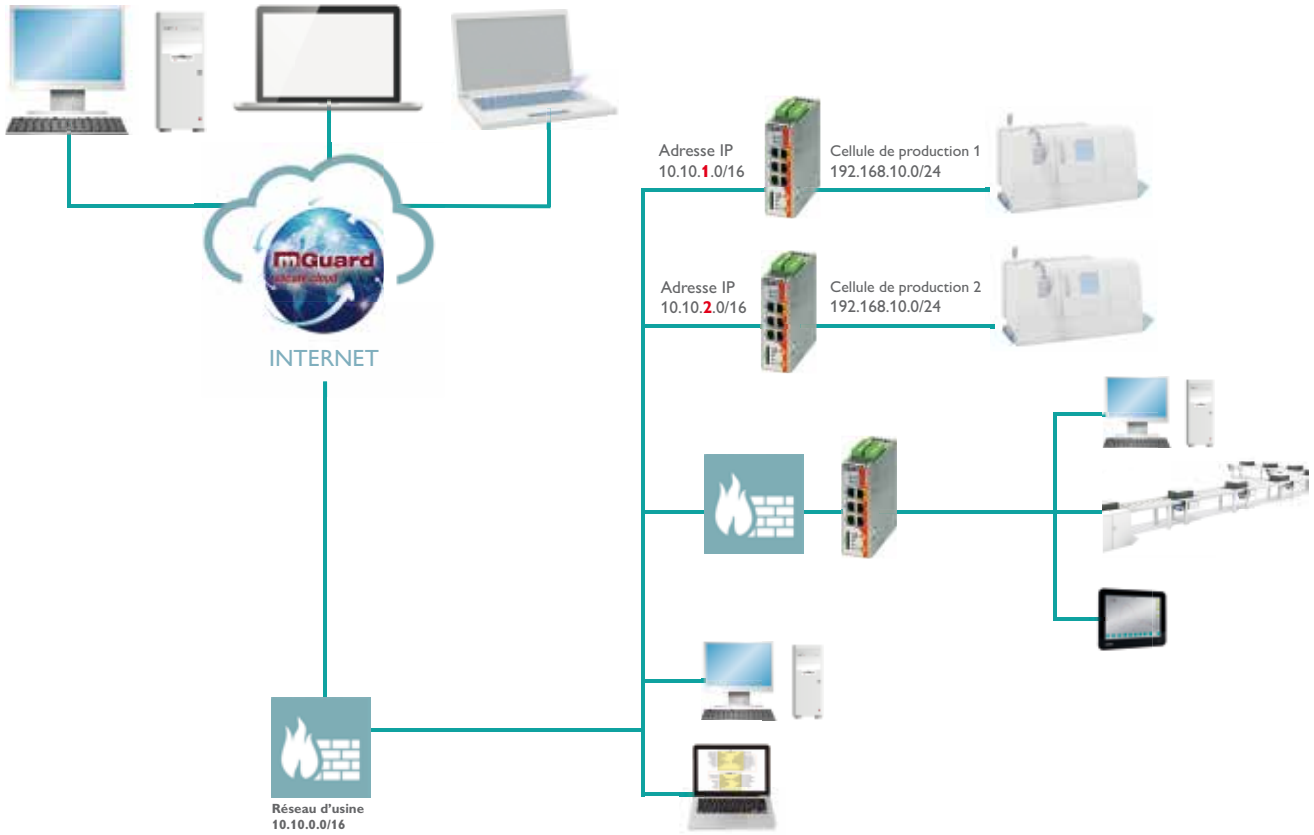
Placé en interface du réseau de l'usine, vous pouvez aussi utiliser le routeur de sécurité mGuard pour la gestion du NAT (Network Address Translation). Grâce à cela, l'ensemble du réseau machine est vu du réseau supérieur comme un seul élément réduisant la possibilité de duplication d'adresses IP sur le réseau. En incluant une configuration de règles de pare-feu appropriées, vous pouvez éviter la contamination entre les réseaux mutualisés. Une sécurité supplémentaire vous est offerte grâce à la gestion des tunnels VPN (Virtual Private Network).

Applications CIM

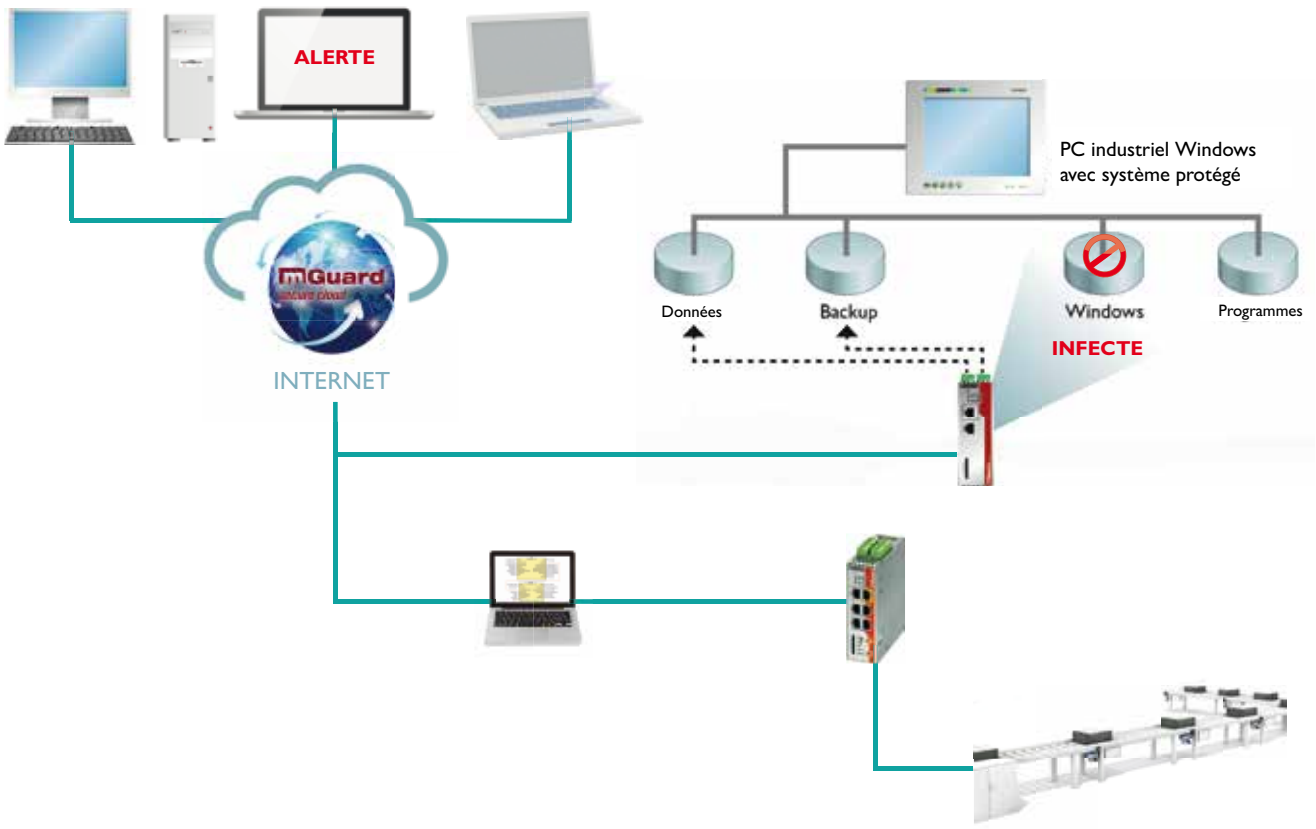
L'utilisation de la technologie CIM (CIFS Integrity Monitoring) disponible en option sur les routeurs de sécurité mGuard permet un contrôle de l'intégrité du système en continu. Il n'est donc plus nécessaire d'installer sur les PC industriels des logiciels anti-virus peu compatibles avec les besoins de la production et d'un réseau industriel.

Grâce à cette technologie de systèmes de fichiers CIFS, les PC industriels du réseau sont surveillés de façon à ce que tout changement (ajout ou modification de programmes, de DLLs ou un autre fichier exécutable) puisse être reconnu et qu'une alerte soit envoyée à la supervision avant propagation d'une éventuelle anomalie.

Application de routage NAT



Application CIM (CIFS Integrity Monitoring)



Solution optimale pour la disponibilité de vos données

Application sécurisée avec DMZ

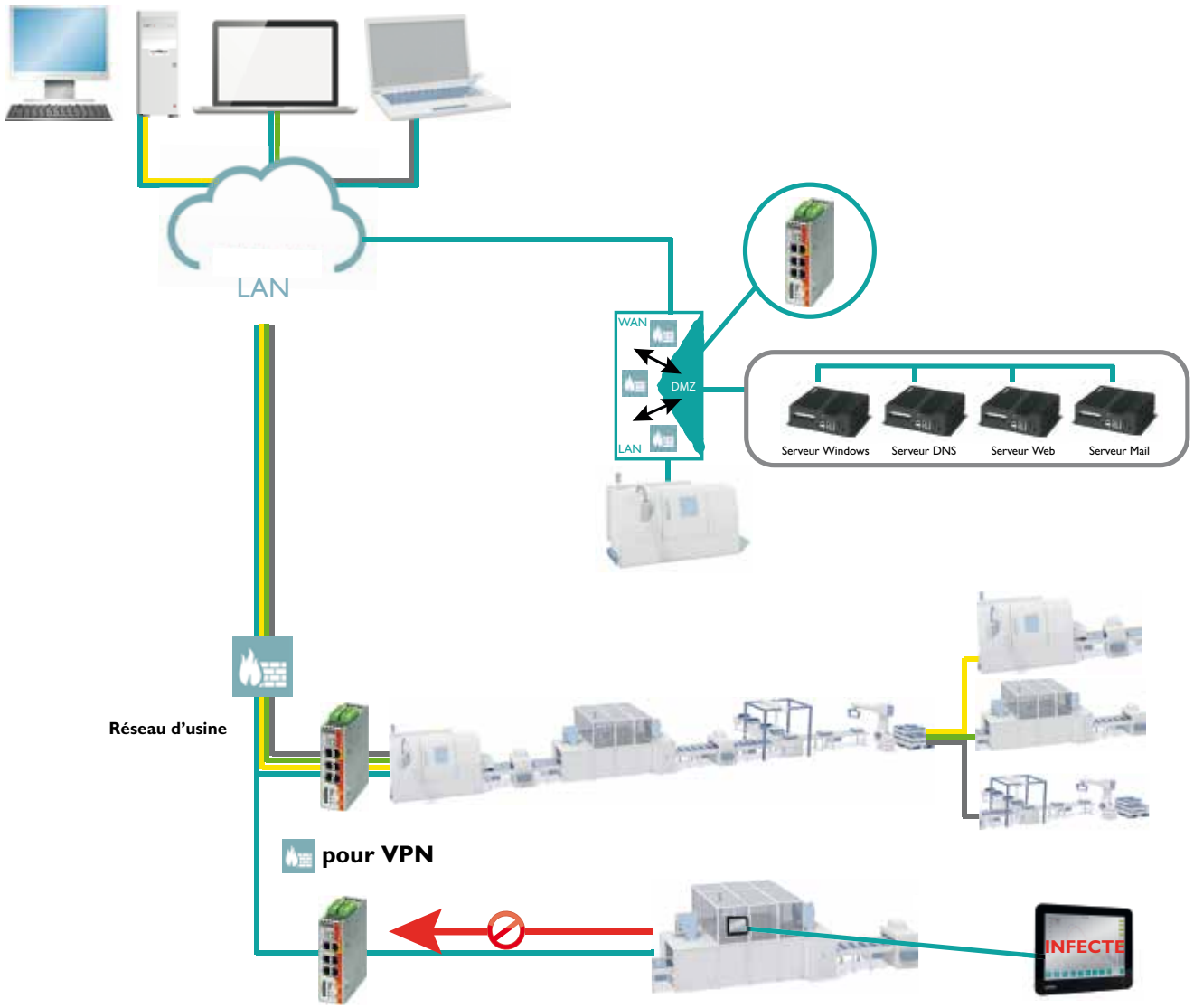
L'utilisation de routeur de sécurité avec port DMZ permet une utilisation plus efficace de la technologie de pare-feu. La zone du serveur est limitée et protégée par des pare-feu permettant de sécuriser l'accès, aussi bien du côté du réseau supérieur que du réseau local. Dans la partie inférieure de l'architecture, vous pouvez aussi découvrir une solution redondante (routeur et connexion VPN).

Licences DPI mGuard

La licence FL MGUARD LIC MODBUS INSPECTEUR permet d'effectuer l'inspection approfondie des paquets pour le protocole Modbus TCP. Cette licence supplémentaire permet de définir quel code de fonction et adresses sont autorisées en communication entre deux noeuds en s'assurant, par exemple, qu'une communication entre un écran et un PLC peut être en lecture seule et non en écriture.

La licence FL MGUARD LIC OPC INSP, permet l'inspection approfondie des paquets pour le protocole OPC DA. Avec cette licence, le mGuard est capable d'intercepter la communication OPC et créer une règle dynamique pour verrouiller le port négocié assurant ainsi une protection fiable.

Application de sécurité pour zone DMZ

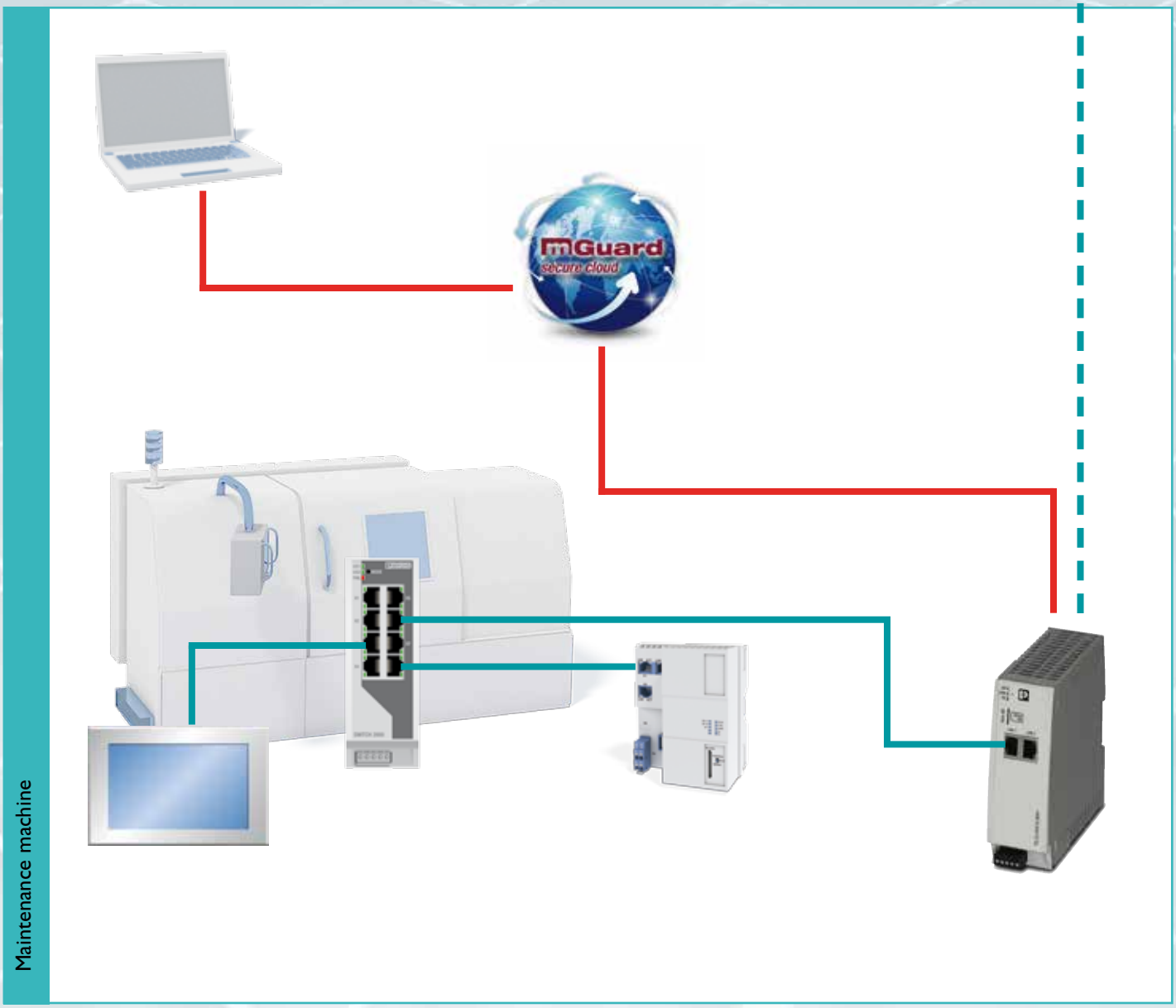


Accès à distance pour les machines

Cas 1 - Machine simple

- Petit réseau sur la machine
- Service distant automate et IHM
- Analyse des défauts
- Mise à jour du programme
- Assistance au démarrage sur nouvelle machine

Votre solution : Ref. 2702885
TC CLOUD CLIENT 1002-TX/TX

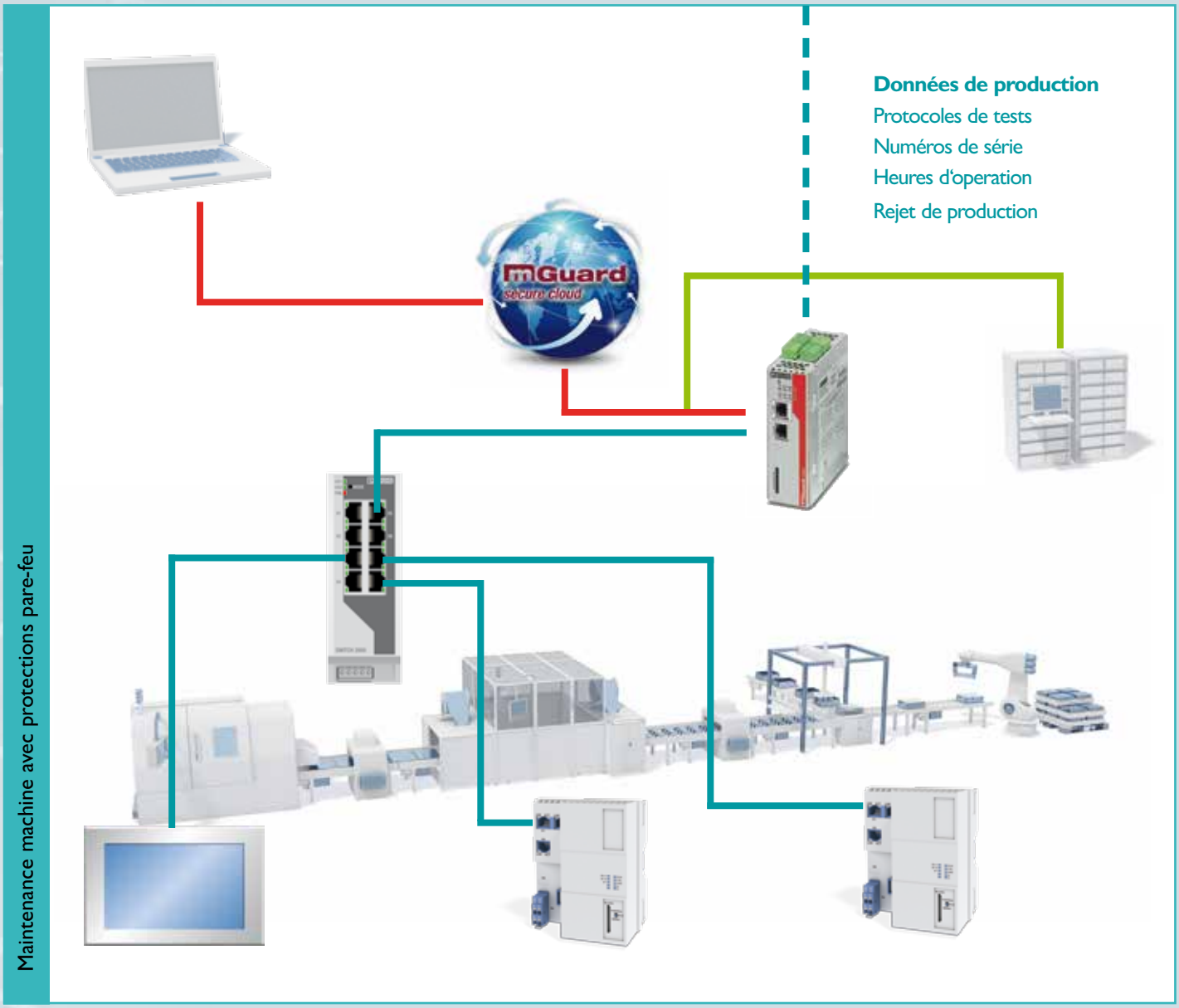


Accès à distance pour les machines

Cas 2

- Petit réseau sur la machine
- Service distant automate et IHM
- Analyse des défauts
- Mise à jour du programme
- Assistance au démarrage sur nouvelle machine
- Service distant et intégration dans le réseau de production

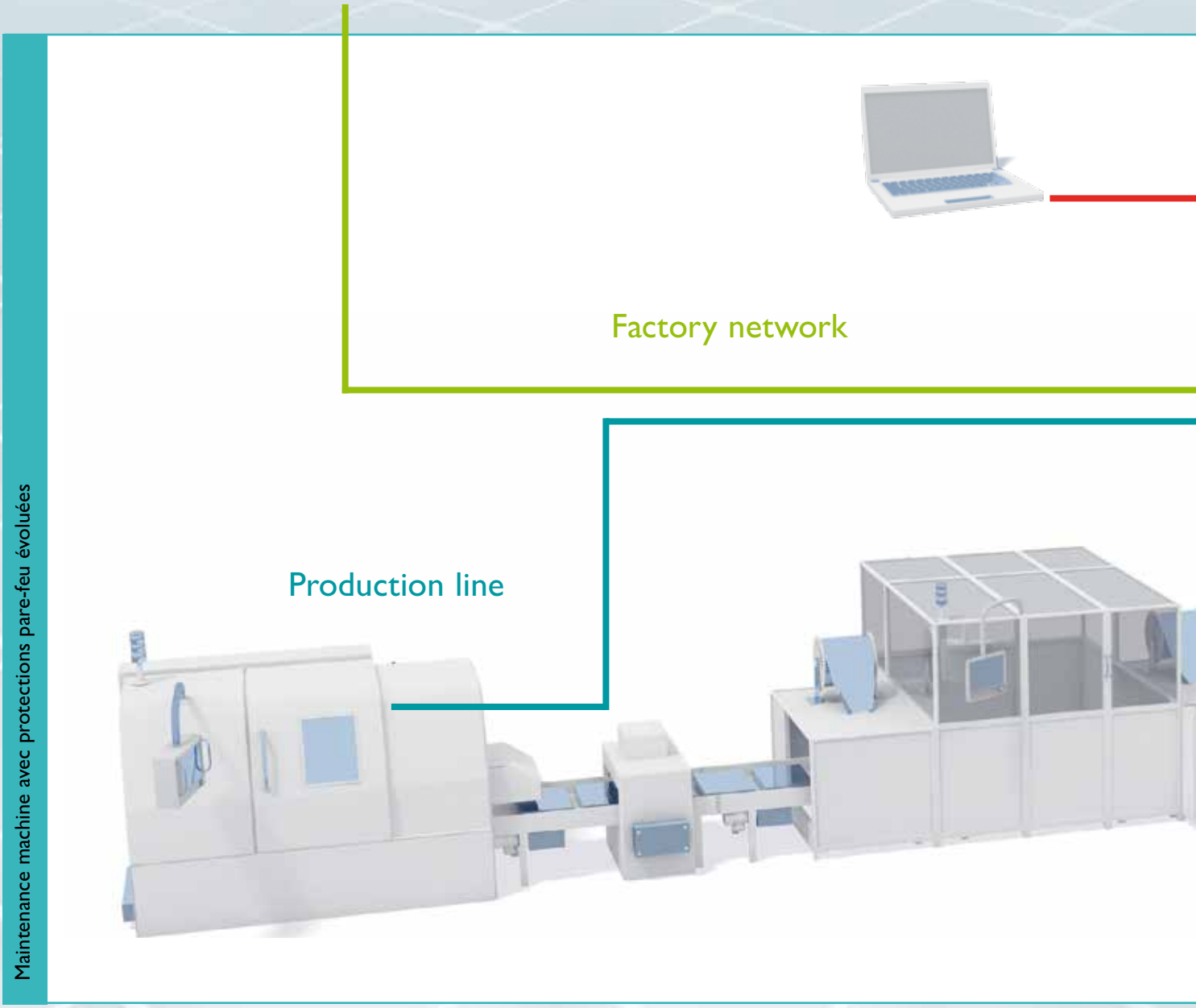
Votre solution : Ref. 2700642
FL MGUARD RS2000 TX/TX VPN



Accès à distance pour les machines

Cas 3

- L'intégration du réseau machine est la première priorité
- Le service à distance est la 2ème priorité
- Exigences de sécurité spéciales
  - Éviter l'accès du réseau d'usine à la machine
  - Supervision de l'accès local
  - Accès au service local limité au réseau de la machine uniquement



Accès à distance pour les machines

Cas 4

- La protection du réseau machine est la 1ère priorité,
- Le service à distance est la 2ème priorité
- Exigences de sécurité spéciales
  - Éviter l'accès du réseau d'usine à la machine
  - Bloquer la charge de trafic lourd du réseau d'usine
  - Accès au service local

Votre solution : Ref. 22701877
FL MGUARD RS4004 TX/DTX VPN

Panorama produits

Pare-feu/Routeur

FL MGUARD RS2000 TX/TX VPN
cod. art. 2700642

FL MGUARD RS4000 TX/TX
cod. art. 2700634

FL MGUARD RS4000 TX/TX VPN
cod. art. 2200515

• 2 ports RJ45, 10/100 Mbit/s

• 1:1-NAT, NAT, port-forwarding, routage standard pare-feu facilement configurable, pare-feu mode "stateful inspection", trafics réseau entrant et sortant séparés

• Jusqu'à 2 tunnels VPN, chiffrement sécuritaire selon les normes IPsec ou Open VPN (RS2000)

• Jusqu'à 250 tunnels VPN, chiffrement sécuritaire selon les normes IPsec ou Open VPN (RS4000)

Pare-feu/Routeur avec Switch non administrable

FL MGUARD RS2005 TX VPN
cod. art. 2701875

• 1 port WAN, 5 ports LAN

• WAN/LAN routeur avec commutateur 5 ports non administrables, pare-feu simplifié, 2 tunnels VPN simultanément actifs

• Jusqu'à 2 tunnels VPN, chiffrement sécuritaire selon les normes IPsec ou Open VPN

Pare-feu/Routeur Gigabit

FL MGUARD GT/GT
cod. art. 2700197

FL MGUARD GT/GT VPN
cod. art. 2700198

• 2 ports RJ45, 10/100/1000 Mbit/s

• 2 ports SFP, 1000 Mbit/s

• 1:1-NAT, NAT, port-forwarding, routage standard pare-feu facilement configurable, pare-feu mode "stateful inspection", trafics réseau entrant et sortant séparés, fibre optique

• Jusqu'à 250 tunnels VPN (par pallier de 10), chiffrement sécuritaire selon les normes IPsec ou Open VPN

Pare-feu/Routeur pour application mobile

FL MGUARD SMART2 VPN
cod. art. 2700639

• Pare-feu/routeur pour le technicien de service

• Version VPN: 10 tunnels parallèles (jusqu'à 250 accéssoires)

• Firewall type"stateful inspection" NAT / 1:1-NAT

• Port-forwarding, routage standard

(Egalement disponible sans version VPN)

Pare-feu/Routeur au format PCI / PCIe

FL MGUARD PCI4000
cod. art. 2701274

FL MGUARD PCI4000 VPN
cod. art. 2701275

FL MGUARD PCIE4000 VPN
cod. art. 2701278

• Routeur avec pare-feu "stateful inspection" pour le PCI

• Version VPN: 10 tunnels parallèles (jusqu'à 250 accéssoires)

• Pare-feu "stateful inspection" NAT / 1:1-NAT

• Port-forwarding, routage standard

mGuard centerport2

FL MGUARD CENTERPORT
cod. art. 2702547

• Pare-feu et gestion VPN haut niveau, format rack 19 pouces (format 1U)

• Idéal pour des solutions de service à distance dans l'infrastructure réseau centralisée

• Jusqu'à 3000 tunnels VPN actifs simultanément

• Processeur basé sur une architecture x86 multicœurs

• Entièrement compatible avec tous les dispositifs mGuard et avec le mGuard Software Central Management (FL mGuard DM)

Pare-feu/Routeur pour atmosphères Ex

FL MGUARD RS4000 TX/TX-P
cod. art. 2702259

- Plage de temperature de -40° C à +70°C
- Certification Atex IECex
- Licence Fonction CIFS
- Licence Fonction Modbus-Inspector
- Licence Fonction OPC-Inspector
- Licence Fonction firewall/routeur en redondance
- Licence Fonction VPN en redondance
- Licence fonction 250 VPN

Pare-feu/Routeur avec Switch administrable

FL MGUARD RS4004 TX/DTX
cod. art. 2701876

FL MGUARD RS4004 TX/DTX VPN
cod. art. 2701877

- WAN routeur / LAN avec commutateur 4 ports administrés, port DMZ, plage de température étendue, carte SD, pare-feu prolongé, routeur avec NAT / 1: 1- NAT

- WAN routeur / LAN avec commutateur 4 ports administrés, port DMZ, plage de température étendue, carte SD, pare-feu prolongé, routeur avec NAT / 1: 1- NAT, 10 tunnels VPN actifs simultanément (jusqu'à 250 sous licences)

Routeur avec modem 3G /4G

TC MGUARD RS2000 3G VPN
cod. art. 2903441

TC MGUARD RS2000 4G VPN
cod. art. 2903588

- Routeur avec modem pour applications de sécurité et de télémaintenance
- Jusqu'à 2 tunnels VPN
- Chiffrement sécuritaire selon les normes IPsec
- Mémoire SD de configuration
- VPN via bouton I/O , voyants d'état VPN

Pare-feu / Routeur pour ordinateur bureautique

FL MGUARD DELTA TX/TX
cod. art. 2700967

FL MGUARD DELTA TX/TX VPN
cod. art. 2700968

- Dispositifs de sécurité avec boîtier métallique, pour une utilisation dans des bureaux ou des centres distribution
- Fente pour carte SD
- Routeur avec NAT / 1:1 NAT

Routeur avec modem 3G / 4G

TC MGUARD RS4000 3G VPN
cod. art. 2903440

TC MGUARD RS4000 4G VPN
cod. art. 2903586

- Routeur avec modem pour applications de sécurité et de télémaintenance
- Jusqu'à 10 tunnels VPN
- Chiffrement sécuritaire selon les normes IPsec
- Mémoire SD de configuration
- VPN via bouton I/O , voyants d'état VPN

Modem pour connexion vers le portail

TC CLOUD Client 1002-TX/TX
cod. art. 2702885

TC CLOUD Client 1002-4G
cod. art. 2702886

- Modem transparent pour connexion vers le portail d'accès
- Gestion du tunnel VPN
- Chiffrement sécuritaire selon les normes IPsec
- Configuration automatique depuis le portail

Antennes
- TC ANT Mobile Wall 5M, cod. art. 2702273
- PSI-GSM/UMTS-QB-ANT, cod. art. 2313371
- TC ANT MOBILE/GPS, cod. art. 2903590

Panorama produits

CIFS – Integrity Monitoring

FL MGUARD LIC CIM
cod. art. 2701083

Surveillance CIFS intégrité (CIM),

Capteur type Antivirus de Phoenix Contact pour les applications industrielles. Pas de mise à jour de listes de virus. CIM est en mesure de détecter si les systèmes basés sur Windows, tels que les automates, les unités et les ordinateurs d'exploitation sont manipulés, par exemple, par des logiciels malveillants.

Licence d'inspection de paquet

FL MGUARD LIC OPC INSP
cod. art. 2702191

FL MGUARD LIC MODBUS INSP
cod. art. 2702980

mGuard Inspecteur OPC, en option, permet un firewall stateful inspection sur le protocole OPC DA, en grande partie utilisé dans un environnement industriel.

mGuard Inspecteur Modbus, en option, permet un firewall stateful inspection sur le protocole Modbus TCP. Elle permet de définir quel code de fonction et adresses sont autorisées en communication entre deux noeuds.

LicenceVPN

FL MGUARD LIC VPN-10
cod. art. 2700194

FL MGUARD LIC VPN-100
cod. art. 2702546

FL MGUARD LIC VPN-250
cod. art. 2700193

FL MGUARD LIC FW RD
cod. art. 2701356

FL MGUARD LIC FW/VPN RD
cod. art. 2702193

Licences pour l'activation des solutions MGuard, jusqu'à 250 connexions VPN supplémentaires

mGuard Secure Cloud Public

Licence Premium pour 3 connexions
cod. art. tbd

Licence Premium pour 1 connexion supplémentaire
cod. art. tbd

Portail de connexion à distance, géré Phoenix Contact et à la disposition des fabricants de machines et opérateurs d'installations. En utilisant un navigateur Web standard, le personnel de service peut se connecter au site Web Secure Cloud et, après identification, ouvrir un accès au terrain et gérer les informations associées aux droits d'accès.

https://fr.cloud.mguard.com

Logiciel de gestion centrale

FL MGUARD DM UNLIMITED
cod. art. 2981974

Logiciel illimité pour la gestion centrale des périphériques FL MGUARD.

Ce logiciel facilite la gestion et la configuration des périphériques installés.

Mode démo jusqu'à 10 mguards.

Client VPN sécurisé

secure vpn client

MGUARD SECURE VPN CLIENT LIC
cod. art. 2702579

Logiciel de gestion des connexions VPN sécurisées pour ordinateur portable ou tablette PC.

Système d'exploitation Windows 8.x, Vista et 7

(Article à commander sur le portail de connexion Secure Mguard Cloud)

Service après-vente
Toujours à vos cotés

Service clients

cybersecurite@phoenixcontact.fr

www.phoenixcontact.fr/cybersecurite

Tel : 01.60.17.98.98

Découvrez la gamme de services que

Phoenix Contact est en mesure d'offrir :

- L'analyse et l'évaluation du réseau existant
- Les tests fonctionnels pour une bonne solution de sécurité
- Des conseils pour identifier les technologies les plus adaptées au système
- La conception et le développement de votre solution de sécurité
- L'analyse et réalisation d'une solution de redondance

Phoenix Contact propose des séminaires qui fournissent les bases théoriques et pratiques pour une utilisation optimale des réseaux Ethernet industriels.

Pour plus d'informations ou pour participer à ces séminaires, rendez-vous sur www.phoenixcontact.fr/cybersecurite ou contactez-nous par mail à cybersecurite@phoenixcontact.fr

Aux côtés de nos clients et partenaires dans le monde entier

Phoenix Contact, basée en Allemagne, est une entreprise leader présente dans le monde entier. Le groupe d'entreprises est une référence en matière de composants, de systèmes et de solutions de pointe dans les domaines de l'électrotechnique, l'électronique et de l'automatisation. Fort d'un réseau mondial dans plus de 100 pays et composé de 14 500 collaborateurs, le groupe assure une proximité directe avec sa clientèle.

Grâce à un portefeuille de produits varié et innovant, nous offrons à nos clients des solutions de pointe pour diverses applications et industries. en particulier dans les domaines de l'énergie, de l'infrastructure, des processus et de l'automatisation industrielle.

Notre gamme complète de produits est disponible sur notre site web:
phoenixcontact.fr

PHOENIX CONTACT SAS
52 Bd de Beaubourg · Émerainville
77436 Marne la Vallée Cedex 2
Tél. : 01 60 17 98 98
Fax : 01 60 17 37 97
www.phoenixcontact.fr

MNR 000000000-00-FR

INSPIRING INNOVATIONS