LIVRE BLANC

Un accès sécurisé et évolutif pour les technologies industrielles

Favoriser le télétravail et assurer la continuité des opérations métiers

Synthèse

Les technologies industrielles (ou OT pour Operational Technology) permettent aux usines, stations de production et de distribution électrique, transports en commun et acteurs des Utilities de fonctionner. Ces entreprises offrent des services essentiels et il est d'autant plus critique qu'elles disposent d'un plan de continuité de leurs activités.

Fortinet offre une solution intégrée pour un accès distant sécurisé adapté à l'OT. Les pare-feu de nouvelle génération (NGFW) FortiGate permettent de déployer des réseaux privés virtuels (VPN) IPsec, qui permettent aux télétravailleurs de se connecter en toute sécurité au réseau corporate, qu'il s'agisse de réseaux IT ou OT. Avec la protection endpoint offerte par FortiClient et FortiToken, l'authentification multifactorielle (MFA) et l'authentification single sign-on (SSO) de FortiAuthenticator, les entreprises sécurisent le télétravail et assurent la continuité des activités métiers.

9 entreprises OT sur 10 ont subi au moins une intrusion système l'année passée et 63 % d'entre elles en ont subi 3 ou plus.[1]

Pérenniser les opérations grâce au télétravail

Nombre d'acteurs de l'OT jouent un rôle critique en matière de sécurité publique et ils doivent pérenniser leurs activités en cas de situation d'urgence ou de catastrophe naturelle.

Dans un plan de continuité des activités métiers, il est important d'envisager la possibilité de ne plus pouvoir opérer sur site. La capacité à sécuriser le télétravail est essentielle à la continuité des opérations métiers en environnement industriel. Les industriels doivent également sécuriser les accès distants pour pouvoir activer de nouveaux équipements, appliquer des patchs critiques et assurer les opérations de diagnostic et de restauration. De plus, les industriels doivent pouvoir assurer un monitoring à distance ou accéder à des centres opérationnels distants pour piloter des ressources multisites. La sécurité devient critique : un incident en environnement OT peut aboutir à une panne des services avec des impacts potentiellement lourds sur les vies humaines et les infrastructures critiques.

Les solutions Fortinet se déploient facilement sur les lieux distants. Cependant, nombre d'entreprises ont également besoin de ressources sur site ou dans le cloud, à l'intention des télétravailleurs. Dans de nombreux cas, elles disposent déjà de ces ressources qui font partie de leur arsenal de sécurité.

Dans le cas d'une catastrophe naturelle ou de tout autre évènement qui obère une activité métier normale, une entreprise doit être capable de basculer rapidement en mode télétravail. Au-delà de chiffrer les données transitant via un réseau privé virtuel, les solutions Fortinet offrent de nombreuses autres fonctionnalités qui aident les entreprises à sécuriser le travail à distance et l'infrastructure. Parmi ces fonctionnalités :

- **L'authentification multifactorielle (MFA) et le single sign-on (SSO).** FortiToken et FortiAuthenticator offrent une authentification à 2 facteurs, ainsi que le single sign-on à l'intention des collaborateurs distants et des tiers.
- **Pare-feu de nouvelle génération, système de prévention des intrusions, filtrage web et SD-WAN.** FortiGate propose toutes ces fonctionnalités et davantage à partir d'une seule appliance.
- **Connectivité sans fil.** Les points d'accès FortiAP et FortiExtender offrent un accès sans fil, notamment pour les connexions cellulaires 3G/4G LTE/5G sur les lieux de travail distants, avec une intégration étroite et une gestion de la configuration via une interface unique.

Un pare-feu NGFW FortiGate inspecte le trafic en clair et chiffré avec un impact minimal sur les performances. FortiGate intègre également une passerelle VPN qui joue le rôle d'un endpoint pour les communications chiffrées vers les télétravailleurs. Ces plateformes, équipées de FortiOS 7.0, disposent d'une fonction ZTNA (Zero-Trust Network Access) qui permet de contrôler l'accès aux applications, quelle que soit la localisation des applications et des utilisateurs. Le ZTNA, une évolution naturelle du VPN, offre une sécurité renforcée, un contrôle plus précis et une expérience utilisateur renforcée, autant d'avantages à l'intention des équipes distantes.

Le NGFW FortiGate s'intègre également avec les composantes classiques des infrastructures IT : services d'annuaire corporate (Microsoft Active Directory) et les solutions MFA et SSO. FortiAuthenticator propose un point d'intégration centralisé et unique pour les solutions d'authentification. La solution est compatible avec FortiToken qui offre des tokens matériels, logiciels et par email. Les tokens logiciels sont compatibles avec de nombreux smartphones et dispositifs mobiles.

L'appliance virtuelle FortiGate-VM propose des performances de 20 Gbps sur AWS et d'autres services cloud. Elle peut, à ce titre, prendre en charge de milliers d'utilisateurs distants, que ces derniers utilisent FortiClient ou d'autres clients VPN tiers. De nombreux sites font appel à FortiGate VM pour se connecter en toute sécurité à des services de sécurité cloud et accéder à des applications hébergées dans le cloud. L'accès à des applications sur site est également possible via la région cloud la plus proche et vers les data centers privés, ce qui permet des transferts à très haut débit entre le cloud et les data centers.

Les pare-feu NGFW FortiGate et les point d'accès sans fil FortiAP bénéficient d'un provisioning automatisé. Ces solutions peuvent être configurées en usine pour une installation automatique sur site.

Sécuriser les télétravailleurs avec les pare-feu NGFW FortiGate

Les VPN IPsec et SSL à haut débit et le ZTNA intégré dans chaque pare-feu FortiGate offrent un modèle de déploiement flexible pour les entreprises IT et OT. Les télétravailleurs peuvent tirer parti d'un ZTNA ou d'un VPN sans client, ou obtenir un accès à des fonctionnalités supplémentaires via un VPN ou ZTNA basé sur un client, grâce à la solution de sécurité endpoint FortiClient. Les collaborateurs et les partenaires externes peuvent également tirer parti du déploiement de points d'accès FortiAP, ou de l'outil d'extension WAN FortiExtender, associés au pare-feu FortiGate, pour assurer une connectivité sans fil.

Les solutions Fortinet sont simples à utiliser. FortiGate et FortiAP peuvent ainsi faire l'objet d'un provisioning automatique. D'autre part, les appliances déployées sur les sites distants peuvent être pré-configurées avant livraison pour s'installer automatiquement sur site. Cette automatisation encourage la continuité métier et facilite le télétravail : aucune intervention sur site n'est requise pour configurer le matériel. Il suffit de le brancher et de le connecter au réseau. Le pare-feu FortiGate est disponible aux formats physiques et virtuels, tandis que la version virtuelle peut être hébergée dans un cloud public ou privé.

La Fortinet Security Fabric tire parti du système d'exploitation FortiOS et d'interfaces API pour créer une architecture de sécurité élargie, intégrée et automatisée. Avec la Fortinet Security Fabric, tous les dispositifs d'une entreprise, et notamment ceux déployés à distance pour permettre le télétravail, peuvent être surveillés et gérés à partir d'une plateforme de gestion centralisée. Les équipes de sécurité disposent d'une visibilité et d'un contrôle total sur l'ensemble des dispositifs connectés, où qu'ils soient déployés, à partir d'un pare-feu FortiGate en local ou de la plateforme de gestion centralisée FortiManager.

Cas d'usage des produits Fortinet pour l'accès sécurisé

Les télétravailleurs dans une entreprise ne requièrent pas tous le même niveau d'accès aux ressources d'entreprise. D'autre part, les partenaires externes ne peuvent être tous autorisés à accéder librement aux systèmes critiques et aux réseaux d'une entreprise. Fortinet offre des solutions sur mesure selon le profil de chaque entité distante.

1 L'accès sécurisé des tiers à des fins de maintenance à distance, de monitoring ou de diagnostic (FortiClient, FortiToken, FortiAP, FortiGate)

Les utilisateurs tiers distants sont, par exemple, des ingénieurs de maintenance externes qui s'occupent des équipements industriels. Ils ont besoin d'un niveau supérieur d'accès à distance pour dépanner ou opérer les systèmes de contrôle industriels. Au sein d'un environnement OT, ils doivent accéder à des automates programmables (PLC) et à des télé-terminaux (RTU), et pouvoir intervenir dans de multiples environnements IT parallèles. Les intégrateurs systèmes, les équipements OEM, les fournisseurs et les opérateurs comptent parmi ces utilisateurs externes distants.

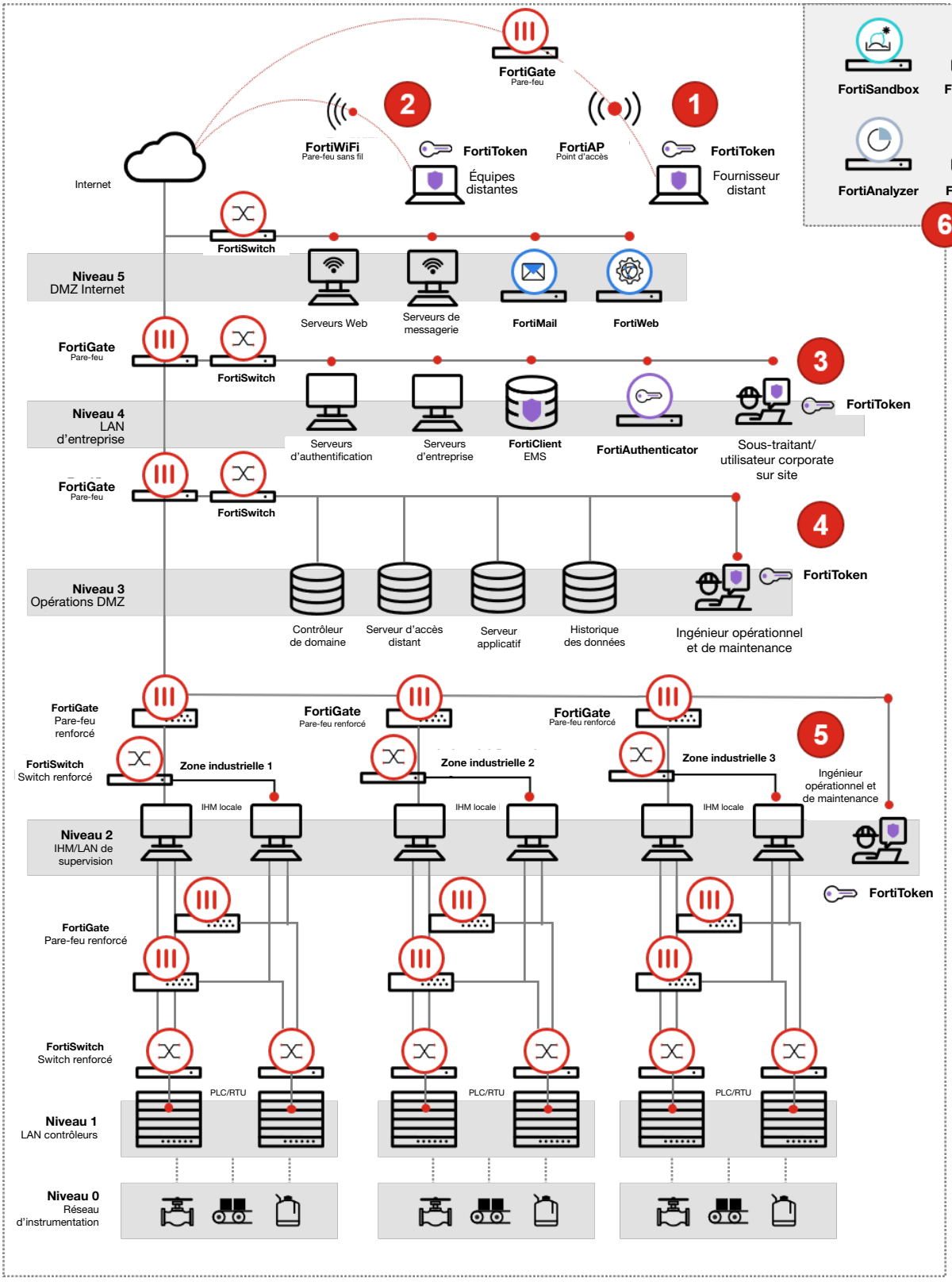

Schéma 1 : accès sécurisé à l'aide de solutions Fortinet sur une infrastructure IT et OT connectée.

Ces utilisateurs ont parfois besoin d'un accès administrateur aux réseaux et ressources industrielles pour mettre en route les équipements, assurer les opérations de dépannage (mises à jour logicielles et matérielles) et prendre en charge les incidents (analyses post-incident, activités de gestion des risques, etc.).

Les travailleurs distants peuvent se connecter aux systèmes OT et aux services IT corporate à l'aide du logiciel client de VPN intégré ou le ZTNA de FortiClient, et ainsi vérifier leur identité en utilisant FortiToken pour une authentification à 2 facteurs.

2 L'accès sécurisé pour les télétravailleurs à domicile et autres équipes distantes (FortiClient, FortiToken, FortiWiFi)

Les télétravailleurs doivent pouvoir accéder à leurs systèmes d'entreprise pour assurer leurs tâches quotidiennes. L'accès distant permet d'utiliser les ressources IT d'entreprise, comme l'email, Internet, la téléconférence, le partage de fichiers ou des outils propres à des fonctions (Finances, RH, etc.). Dans le cas des infrastructures OT, certains collaborateurs accèdent à des systèmes OT pour récupérer des données et enregistrements, voire réaliser des diagnostics et opérations de maintenance. Les collaborateurs responsables du bon fonctionnement de l'infrastructure OT doivent être capables de surveiller la disponibilité des ressources OT ou assurer des opérations basiques de dépannage en cas de dysfonctionnement.

Les travailleurs distants peuvent se connecter aux systèmes OT et aux services IT corporate à l'aide du logiciel client de VPN intégré ou le ZTNA de FortiClient, et ainsi vérifier leur identité en utilisant FortiToken pour une authentification à 2 facteurs.

3 Accès sécurisé pour les partenaires présents sur site ou les utilisateurs d'entreprise qui veulent accéder à des systèmes OT à partir de réseaux IT (FortiClient, FortiToken, FortiGate, FortiClient EMS, FortiAuthenticator)

Comme dans les cas d'utilisation 1 et 2, les partenaires sur site et les utilisateurs d'entreprise peuvent vouloir accéder à des systèmes OT à partir de réseaux IT, pour collecter des données ou en assurer la maintenance. Cependant, les systèmes OT peuvent être situés au sein de réseaux OT couvrant différents sites disséminés. Dans certains cas, les réseaux OT sont sur des sites distants sans accès physique, pour cause de restrictions dans les déplacements ou de conditions hostiles.

Les réseaux corporate IT peuvent, à partir d'un site centralisé, se connecter à des réseaux OT distants. L'accès vers ces réseaux OT à partir du réseau IT central doit être sécurisé pour les sous-traitants présents sur site et les utilisateurs d'entreprise. Le lieu central peut également héberger des technologies centralisées pour gérer l'accès à distance sécurisé (autorisations centralisées, monitoring des connexions d'accès distants).

Pour tenir les contraintes réglementaires, un accès sécurisé du réseau corporate IT vers les réseaux OT peut être requis à des fins d'audit et de conformité. Les collaborateurs ont parfois besoin d'accéder aux réseaux OT pour recueillir des informations OT qui seront ensuite mises à disposition des instances réglementaires à l'image des CERT ou encore de l'ENISA (le cas d'utilisation 6 fournit davantage d'informations sur le reporting et la gestion centralisés).

4 Accès sécurisé pour les opérateurs et les ingénieurs de maintenance devant accéder aux systèmes ICS à partir des réseaux OT (FortiClient, FortiToken, FortiGate)

Les ingénieurs d'exploitation et de maintenance basés dans les centres de contrôle doivent accéder aux ressources ICS pour réaliser leurs tâches quotidiennes de monitoring, de diagnostic et de maintenance des ressources ICS. Le centre de contrôle peut être situé sur le site ICS ou à distance. La connexion réseau entre le centre de contrôle et le site ICS peut être un réseau local filaire ou sans fil, ou encore un WAN. La sécurité des accès et des communications entre le centre de contrôle et les sites ICS devient essentielle pour prévenir les attaques réseau de type man-in-the-middle ou le détournement de communication. Pour améliorer les mesures de sécurité pour ces accès et réseaux, dans le cadre de la mise en œuvre de l'accès distant, l'authentification multifactorielle des accès peut être déployée, tout comme le chiffrement des liens réseau. Des fonctionnalités comme le SD-WAN peuvent jouer un rôle majeur si le centre de contrôle et les sites ICS sont connectés à l'aide de multiples lignes de communication. La haute disponibilité de ces liens doit être assurée de manière économique.

5 Accès sécurisé pour les opérateurs et les ingénieurs de maintenance qui ont besoin d'un accès local aux ICS (FortiClient, FortiToken, FortiGate)

L'accès sécurisé aux ressources ICS ne doit pas forcément s'effectuer à partir d'un site distant. Dans certains cas, l'accès sécurisé peut être requis pour les opérationnels ou les ingénieurs au niveau des sites industriels, pour ainsi sécuriser l'accès aux ressources ICS. Ce type d'accès aux systèmes industriels doit être encadré par une authentification multifactorielle et des capacités AAA (authentication, authorization et accounting). D'autre part, le chiffrement au sein des réseaux ICS peut être déployé lorsque nécessaire.

6 Traitement analytique, reporting & gestion centralisés et protection contre les menaces évoluées (FortiAnalyzer, FortiManager, FortiSandbox, FortiDeceptor)

Que l'accès sécurisé soit appliqué aux sites locaux ou distants, la centralisation des logs, du monitoring, du reporting et de la gestion permet de recueillir des informations de valeur et gérer efficacement l'infrastructure d'accès sécurisée. Cette centralisation peut être réalisée sous la forme d'un centre opérationnel réseau (NOC) ou un centre opérationnel de sécurité (SOC).

Pour des accès sécurisés à grande échelle, une centralisation des capacités de gestion facilite la gestion de multiples technologies, ainsi que les tâches de maintenance et de mise à jour logicielle ou firmware pour de multiples technologies.

Dans certains cas, un reporting centralisé peut être exigé à des fins de conformité en interne et pour assurer le reporting d'informations vers les équipes de sécurité internes ou les dirigeants. Parfois, cette information devient critique pour la conformité réglementaire et peut être partagée avec des instances externes comme les CERT.

Pour des accès sécurisés à grande échelle, une centralisation des capacités de gestion facilite la gestion de multiples technologies, ainsi que les tâches de maintenance et de mise à jour logicielle ou firmware pour de multiples technologies.

De plus, pour lutter contre les menaces émergentes, des technologies de protection contre les menaces avancées (outils de sandboxing comme FortiSandbox) et de honeypot (comme FortiDeceptor) peuvent être déployés de manière centralisée pour identifier les menaces internes et externes et en maîtriser les risques.

Une sécurité étroitement intégrée grâce aux solutions Fortinet

Pour gérer des collaborateurs distants ou multisites, une visibilité centralisée et la gestion de l'infrastructure de sécurité s'imposent. Toutes les solutions Fortinet peuvent être intégrées à l'aide de la Fortinet Security Fabric, une plateforme unifiée pour la visibilité et les opérations de configuration et de monitoring. Les connecteurs Fabric (API ouvertes), le support à la communauté DevOps et un écosystème étendu de la Security Fabric assurent une intégration avec plus de 250 solutions externes.

Lorsqu'une entreprise prépare un plan de continuité métier, la visibilité et la gestion sur l'ensemble de l'architecture de sécurité de l'entreprise deviennent essentielles. En effet, l'entreprise est susceptible de devoir basculer vers un télétravail complet, en un temps très court. La prise en charge du télétravail ne doit pas mettre la cybersécurité de l'entreprise en péril.

Les solutions suivantes font partie de Fortinet Security Fabric et sécurisent le télétravail :

- **FortiClient** propose des indicateurs endpoints, la gestion des vulnérabilités, la prévention des malware, un pare-feu d'application web, un client VPN, le ZTNA et le MFA.
- **FortiClient EMS** permet de configurer le client VPN et de gérer des règles de sécurité endpoint. Ce connecteur de la Security Fabric assure un déploiement et une gestion centralisée des clients.
- **FortiAP** offre une connexion sécurisée avec un contrôleur sans fil et étend le réseau aux utilisateurs distants. Ceci élimine le besoin de clients VPN logiciel et permet un provisioning automatisé.
- **FortiExtender** offre une connectivité hybride WAN-LAN, une connectivité WAN sans fil et la compatibilité avec les réseaux 3G/4G LTE/5G. La solution est parfaitement indiquée pour les sites mobiles, les flottes de véhicules et les équipes sur le terrain.

- **FortiWiFi/FortiGate** est un contrôleur sans fil sécurisé avec des services VPN et ZTNA multifonctions : contrôle d'admission, pare-feu NGFW et de prévention d'intrusion nouvelle-génération, connecteurs Security Fabric, règles de sécurité dynamiques, SD-WAN et provisioning automatisé.
- **FortiToken** confirme l'identité des utilisateurs à l'aide de tokens d'authentification matériels et logiciels. La solution s'intègre en toute transparence avec FortiGate et/ou FortiAuthenticator, à l'aide de jetons logiciels disponibles pour iOS/Android, ainsi qu'une activation sécurisée en ligne avec les services de sécurité FortiGuard.
- **FortiAuthenticator** assure une gestion des authentifications par LDAP/RADIUS/SAML, la gestion du MFA et des jetons, la gestion des tokens matériels et logiciels, ainsi que les certificats de sécurité.
- **FortiAnalyzer** centralise les logs et le reporting, ainsi que la visibilité sur les ressources et le réseau, ce qui permet de gérer les évènements et les incidents. La solution offre un traitement analytique des données NOC/SOC et se déploie sous forme d'une appliance matérielle ou de machine virtuelle.
- **FortiManager** offre une gestion et un monitoring centralisés, une automatisation de la sécurité. La solution, qui s'intègre avec les environnements multitenant, propose une administration fondée sur les rôles, un provisioning sécurisé du SD-WAN, ainsi qu'un déploiement sous forme d'appliance matérielle ou de machine virtuelle.
- **FortiSandbox** permet de détecter et de répondre aux malware, ainsi qu'une protection automatisée contre les piratages via une analyse basée sur le framework MITRE ATT&CK. La solution s'intègre en toute transparence avec FortiGate et la Security Fabric, tout en prenant en charge les applications et les protocoles ICS/OT. Elle se déploie en mode autonome ou de manière centralisée, dans un format matériel ou de machine virtuelle.
- **FortiDeceptor** déploie des leurres pour neutraliser les cybermenaces en amont. La solution émule des environnements Windows, Linux, de VPN, et de télé-terminaux industriels et s'intègre en toute transparence avec FortiGate et la Security Fabric. Elle est parfaitement compatible aux applications et protocoles ICS/OT. Le déploiement s'effectue en mode autonome ou centralisé, dans un format d'appliance matérielle ou de machine virtuelle.

Des fondamentaux de sécurité pour assurer la continuité des activités

Pour les acteurs de l'IT comme de l'OT, se préparer à la continuité métier et à la reprise sur sinistre est essentiel. En concevant leur plan de continuité, les entreprises doivent d'assurer de disposer des bonnes ressources pour sécuriser leurs télétravailleurs, favoriser des opérations IT et OT sans dysfonctionnement en local et à distance, et optimiser la posture de sécurité. Les solutions Fortinet se déploient et se configurent de manière simple. Les acteurs de l'IT et de l'OT bénéficient ainsi d'une visibilité à 360° et d'un contrôle sur leurs ressources digitales, quel que soit l'environnement de déploiement.

[1] "2021 State of Operational Technology and Cybersecurity Report," Fortinet, 26 mai 2021.

www.fortinet.com/fr

15 février, 2022

950814-0-1-FR