LIVRE BLANC

Un accès sécurisé à grande échelle pour les environnements industriels OT

Accompagner le télétravail et assurer la continuité des activités métiers

Synthèse

Les technologies industrielles de type OT (Operational Technology) assurent le bon fonctionnement des usines, sites de production et de transmission d'énergie, réseaux de transport public, sites pétroliers et gaziers et services publics. Ces secteurs d'activité fournissant des produits et des services essentiels, un plan de continuité des activités s'impose.

Fortinet offre une solution intégrée et sécurisée d'accès à distance, parfaitement adaptée aux contingences de l'OT. Les pare-feu FortiGate de nouvelle génération (NGFW) permettent de déployer des réseaux privés virtuels (VPN) sur IPsec, pour que les télétravailleurs se connectent en toute sécurité au réseau de leur entreprise, à partir de sites distants, via des réseaux informatiques classiques (IT) ou des réseaux industriels OT. Grâce à la protection des terminaux assurée par FortiClient et FortiToken, à l'authentification multifactorielle (MFA) et à l'authentification SSO, les entreprises peuvent sécuriser le télétravail et pérenniser leurs activités. FortiPAM propose un coffre-fort pour y stocker les identifiants d'authentification, ainsi qu'un accès zero trust et son monitoring, et un reporting sur les accès des utilisateurs privilégiés aux dispositifs OT les plus critiques de l'entreprise.

Trois acteurs de l'OT sur quatre ont subi au moins une intrusion dans leurs systèmes au cours de l'année écoulée.[1]

Pérenniser l'activité métier grâce au travail à distance

Nombre d'industriels disposant d'environnements OT ont un rôle majeur en matière de sécurité publique. Ils doivent donc s'assurer de pouvoir mener leurs activités en environnement hostile et dans les situations d'urgence, qu'il s'agisse d'épidémies, de maladies, d'inondations, d'ouragans ou de pannes électriques.

En élaborant un plan de continuité des activités, il est important de tenir compte de l'hypothèse qu'une entreprise est susceptible de ne plus pouvoir mener ses activités normales sur site suite à un sinistre. Accompagner les collaborateurs qui basculent vers le télétravail est essentiel à la continuité des activités OT. Les professionnels de l'OT doivent également disposer d'un accès à distance sécurisé. Ils sont en effet amenés à mettre en service de nouveaux équipements, à appliquer des correctifs critiques ou à intervenir à distance à des fins de dépannage. En outre, ils doivent être outillés pour mener des contrôles et des diagnostics à distance ou faire appel à des centres opérationnels distants pour intervenir sur des ressources disséminées géographiquement. La sécurité est essentielle, car une vulnérabilité au sein d'un environnement OT peut entraîner des arrêts de services, endommager des infrastructures critiques, voire mettre en péril des vies humaines.

Les solutions Fortinet se déploient de manière simple sur les sites de travail distants. Cependant, de nombreuses entreprises ont également besoin de ressources sur site ou dans le cloud pour accompagner en toute sécurité les télétravailleurs. Dans de nombreux cas, elles disposent déjà de ces ressources qui font partie de leur infrastructure de sécurité existante. En cas de catastrophe naturelle ou d'événements perturbant l'activité normale d'une entreprise, celle-ci doit être en mesure de basculer rapidement vers le télétravail. Au-delà de chiffrer les données qui transitent via réseau privé virtuel (VPN), Fortinet propose d'autres fonctionnalités qui aident une entreprise à sécuriser ses collaborateurs et son infrastructure hybrides.

Parmi ces fonctionnalités :

- **MFA et SSO :** FortiToken et FortiAuthenticator permettent une authentification à deux facteurs et l'authentification SSO (Single Sign-On) pour les collaborateurs et les tiers.
- **Pare-feu NGFW, système de prévention des intrusions, antivirus, filtrage web et réseau étendu SD-WAN :** FortiGate offre toutes ces fonctionnalités et davantage, à partir d'une seule appliance.
- **Connectivité sans fil :** FortiAP et FortiExtender fournissent un accès sans fil sécurisé, notamment via des connexions cellulaires 3G, 4G LTE et 5G sur les sites de travail distants, avec une gestion des configurations à partir d'une interface unique.
- **Accès des utilisateurs privilégiés :** FortiPAM offre des fonctionnalités de coffre-fort pour les identifiants et de modification de mots de passe, ainsi que le zero trust, une validation de la posture de sécurité et un monitoring des accès des utilisateurs privilégiés aux systèmes OT critiques.

Un pare-feu NGFW FortiGate inspecte le trafic chiffré et en clair à l'échelle d'une entreprise, sans freiner les performances. Les NGFW FortiGate proposent également une passerelle VPN intégrée qui permet des connexions chiffrées avec les travailleurs distants. Les NGFW FortiGate fonctionnant sous FortiOS 7.0 déploient un ZTNA (accès réseau zero trust) qui contrôle les accès aux applications, quelle que soit la localisation des utilisateurs ou des applications. Le ZTNA, une évolution naturelle du VPN, améliore le niveau de sécurité, offre un contrôle plus granulaire et optimise l'expérience utilisateur. Cette approche est donc indiquée pour connecter les télétravailleurs en toute sécurité.

Notons également que le NGFW FortiGate s'intègre avec les composantes classiques d'une infrastructure IT, qu'il s'agisse de services d'annuaire d'entreprise comme Microsoft Active Directory (AD), ou de processus MFA et SSO. FortiAuthenticator constitue un point d'intégration unique et centralisé pour les solutions d'authentification. La solution est compatible avec des outils tiers ainsi qu'avec FortiToken, la solution de Fortinet qui gère les jetons d'authentification matériels, logiciels ou envoyés par email. Les jetons logiciels sont compatibles avec de nombreux smartphones et dispositifs mobiles.

L'appliance virtuelle FortiGate VM fonctionne avec des performances à 20 Gbps sur AWS et d'autres services cloud : elle peut donc prendre en charge des milliers d'utilisateurs distants équipés de FortiClient ou d'autres clients VPN. De nombreux sites utilisent FortiGate VM pour se connecter en toute sécurité à un hub de services de sécurité basé dans le cloud public, pour ainsi accéder aux applications hébergées dans le cloud. L'accès aux applications sur site est également possible via la région cloud la plus proche et jusqu'au data center privé. Ceci permet d'une prise en charge continue des transferts de données à grande vitesse entre le cloud et les data centers et vice versa.

Les NGFW FortiGate et les points d'accès sans fil FortiAP bénéficient d'un provisioning « zero touch » : ils sont préconfigurés avant expédition et s'installent de manière automatisée sur site.

Sécuriser les équipes à distance avec les NGFW FortiGate

Les VPN IPsec et SSL (Secure Sockets Layer) haute performance et le ZTNA intégrés dans chaque FortiGate NGFW offrent un modèle de déploiement flexible pour l'IT et l'OT. Les utilisateurs distants peuvent faire appel au ZTNA ou à un VPN sans client, ou accéder à des fonctionnalités supplémentaires par le biais d'un VPN ou d'un ZTNA basé sur un client, comme c'est le cas avec FortiClient, la solution de sécurité des terminaux de Fortinet. Les collaborateurs et les fournisseurs externes peuvent bénéficier du déploiement d'un point d'accès sans fil FortiAP ou de FortiExtender (extension du WAN en mode sans fil) associé à un FortiGate NGFW pour déployer un réseau sans fil.

Les solutions Fortinet sont conçues pour être faciles à utiliser, de leur achat initial à leur fin de vie. Les NGFW FortiGate et les FortiAP bénéficient tous deux d'un provisioning automatisé. Les dispositifs déployés sur des sites distants peuvent être préconfigurés avant expédition pour une installation automatique sur site. Ce provisioning de type « zero touch » assure la continuité des activités et la prise en charge du travail à distance, car aucune configuration supplémentaire n'est exigée sur site, au-delà de brancher l'appareil et les câbles réseau. Les NGFW FortiGate sont disponibles sous forme d'appliances physiques et virtuelles. Les appliances virtuelles FortiGate peuvent être hébergées dans des clouds publics et privés.

La Security Fabric capitalise sur le système d'exploitation FortiOS et sur une API ouverte pour définir une architecture de sécurité étendue, intégrée et automatisée. Avec cette Security Fabric, parfaitement adaptée à l'OT, tous les dispositifs d'une entreprise, y compris ceux déployés à distance dans un contexte de travail hybride, peuvent être surveillés et gérés à partir d'une plateforme de gestion centralisée. Les équipes de sécurité bénéficient d'une visibilité et d'un contrôle complets de tous les appareils connectés, quelle que soit leur localisation, soit en local à partir d'un FortiGate NGFW, soit de manière centralisée à partir d'une plateforme de gestion centralisée intégrée FortiManager, déployée au niveau du siège de l'entreprise.

Cas d'utilisation pour les produits Fortinet adaptés à l'accès sécurisé

Les collaborateurs distants n'ont pas tous besoin d'un même niveau d'accès aux ressources de leur entreprise. Par ailleurs, tous les fournisseurs externes ne devraient pas être autorisés à accéder aux systèmes et réseaux critiques d'une entreprise sans une autorisation formelle de demande d'accès à distance et un contrôle des connexions à distance. Fortinet propose des solutions sur mesure pour différents profils de collaborateurs.

1 Accès sécurisé pour les prestataires distants, dans le cadre de la maintenance, de la surveillance et des diagnostics à distance (FortiClient, FortiToken, FortiAP, FortiGate, FortiPAM)

Des techniciens extérieurs sont susceptibles d'intervenir à distance pour assurer la maintenance des équipements industriels d'une entreprise. Parfois, ils nécessitent des privilèges d'accès plus élevés pour dépanner, opérer ou gérer des systèmes de contrôle industriel (ICS) à distance. Dans l'environnement OT, ils peuvent avoir besoin d'accéder à des automates programmables (PLC) et à des unités de télégestion (RTU). Ils sont également susceptibles d'intervenir dans des environnements informatiques multiples et parallèles. Dans certains cas, les utilisateurs tiers distants sont des intégrateurs systèmes, des fabricants d'équipement d'origine (OEM), des fournisseurs de technologies et des opérateurs.

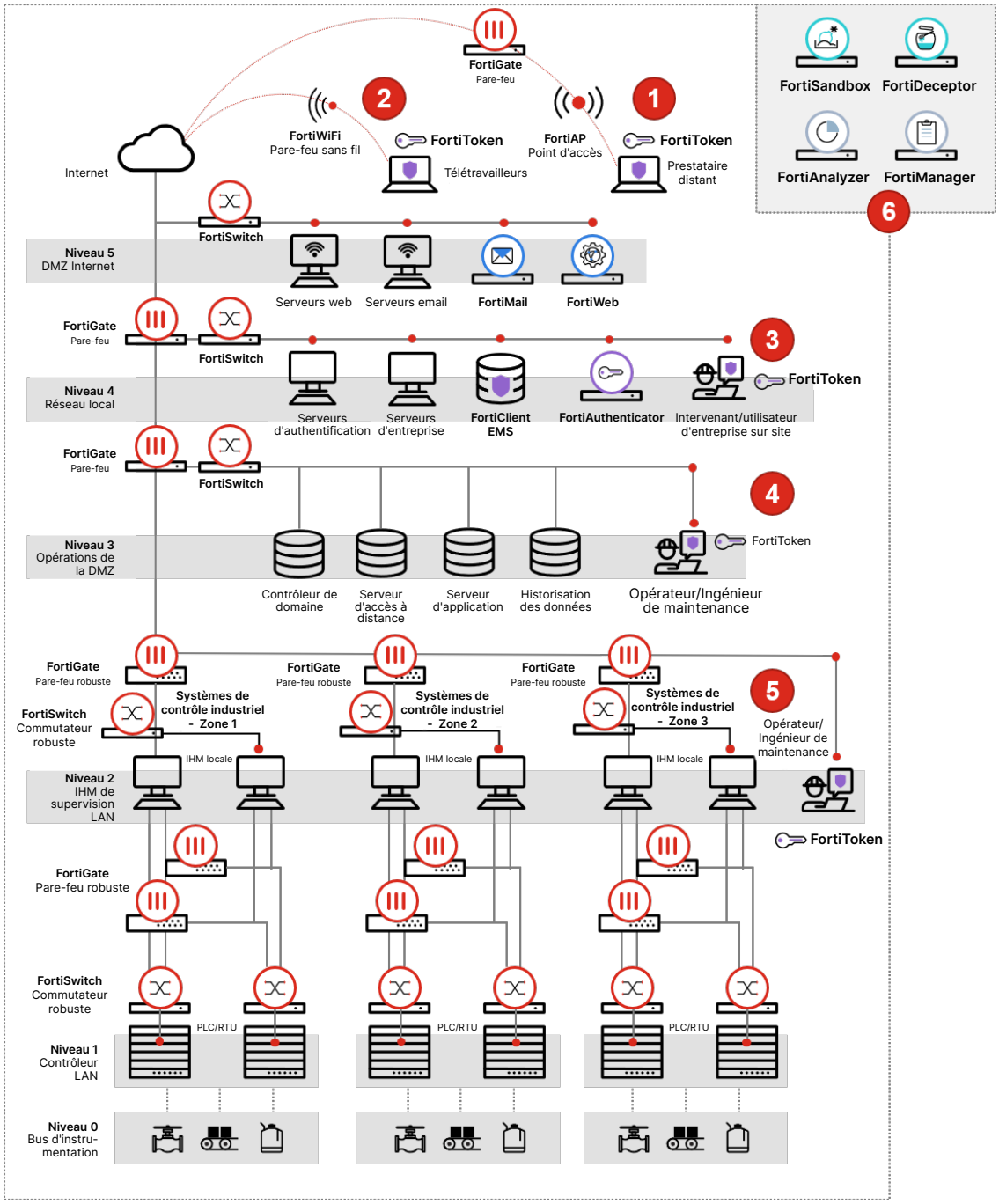


Schéma 1 : Accès sécurisé avec des solutions Fortinet sur l'ensemble d'une infrastructure IT et OT connectée

2 Accès sécurisé pour les équipes distantes, et notamment les collaborateurs utilisant le WFA (FortiClient, FortiToken, FortiWiFi, FortiPAM)

Les collaborateurs distants ont besoin d'accéder aux systèmes de leur entreprise dans le cadre de leurs tâches quotidiennes. L'accès à distance fait parfois appel à des fonctionnalités informatiques de l'entreprise (email, internet, vidéoconférence, partage de fichiers, etc.) ou demande un accès à des fonctions métiers spécifiques (finances, RH, etc.) Chez les opérateurs d'infrastructures OT, des techniciens doivent pouvoir accéder aux systèmes OT pour consulter des fichiers et données spécifiques ou effectuer des opérations de maintenance et de diagnostic. Les collaborateurs chargés de l'entretien de l'infrastructure d'OT doivent être en mesure de contrôler à distance la disponibilité des ressources OT et procéder à un dépannage de base en cas de dysfonctionnement.

Les télétravailleurs se connectent aux systèmes OT et aux services informatiques de l'entreprise en utilisant le client VPN ou la fonction ZTNA intégrés à FortiClient. Leur identité est validée à l'aide d'un jeton FortiToken qui assure une authentification MFA.

3 Accès sécurisé pour le personnel externe sur site ou les utilisateurs d'entreprise accédant à l'OT à partir des réseaux IT (FortiClient, FortiToken, FortiGate, FortiClient EMS, FortiAuthenticator, FortiPAM)

Comme dans les cas d'utilisation 1 et 2, les intervenants externes opérant sur site et les utilisateurs d'entreprise peuvent avoir besoin d'accéder aux systèmes OT à partir du réseau IT corporate, à des fins de recueil de données et de maintenance. Cependant, les systèmes OT peuvent être situés dans des réseaux OT disséminés sur de nombreux sites géographiques. Dans certains cas, les réseaux OT couvrent des sites éloignés, ce qui ne simplifie en rien les interventions physiques, en raison, par exemple, de restrictions sur les déplacements ou de conditions extrêmes.

Le réseau IT d'entreprise centralisé peut se connecter aux réseaux OT sur différents sites. Dans de cas, la mise en place d'un accès sécurisé aux différents réseaux OT à partir de ce réseau IT central permet à tous les utilisateurs (personnel externe présent sur site ou collaborateurs d'entreprise) d'accéder à distance et en toute sécurité aux ressources OT. Le site central peut également héberger des technologies de gestion des accès à distance, pour notamment autoriser et surveiller les connexions d'accès à distance de manière centralisée.

Tout assurant sa conformité, un accès sécurisé du réseau IT d'entreprise vers les réseaux OT peut être nécessaire à des fins d'audit et de conformité. Certains collaborateurs doivent accéder aux réseaux OT pour récupérer des informations liées à l'infrastructure OT et les mettre à disposition d'instances de réglementation : CERT, le NERC et la FERC (dans le cadre de la norme NERC CIP), ainsi que l'ENISA et le CSIRT (dans le cadre du NIS-D). Le cas d'utilisation n°6 ci-dessous offre davantage de détails sur le reporting et la gestion centralisés.

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

Les opérateurs ou les ingénieurs de maintenance présents dans des centres et salles de contrôle doivent accéder aux ressources industrielles pour effectuer leurs tâches de monitoring, de diagnostic et de maintenance des systèmes ICS. Le centre de contrôle peut être situé à proximité ou à distance du site industriel supervisé. Le lien réseau entre le centre de contrôle et ce site industriel peut être un LAN ou un WAN, filaire ou sans fil.

La sécurisation des accès et des communications entre le centre de contrôle et les sites ICS est primordiale pour prévenir les attaques de type "man-in-the-middle" ou la mise sur écoute furtive des communications. Pour renforcer la sécurité de ces accès et réseaux, il est recommandé d'appliquer des mesures comme l'authentification des accès par MFA et le chiffrement du trafic réseau. D'autre part, un SD-WAN peut jouer un rôle important si le centre de contrôle et les sites industriels sont connectés à l'aide de plusieurs liens de communication. La haute disponibilité de ces liens doit être assurée de manière économique.

5 Accès sécurisé et en local des opérateurs et ingénieurs de maintenance aux systèmes ICS (FortiClient, FortiToken, FortiGate, FortiPAM)

L'accès sécurisé aux systèmes ICS ne s'effectue pas toujours depuis un site distant. Dans certains cas, un accès sécurisé en local peut être nécessaire pour les opérateurs et ingénieurs présents sur les sites industriels, afin de sécuriser l'accès aux ressources ICS. La mise en œuvre du MFA améliore les processus d'authentification, d'autorisation et de traçabilité (AAA) des accès aux ressources industrielles. En outre, les réseaux industriels peuvent être chiffrés lorsque nécessaire.

Pour les accès sécurisés à grande échelle, la centralisation des opérations de gestion simplifie le pilotage de plusieurs technologies et allège les coûts de maintenance (mise à jour logicielle ou du firmware).

6 Analyses, reporting & gestion centralisés de la sécurité, et protection centralisée contre les menaces avancées (FortiAnalyzer, FortiManager, FortiSandbox, FortiDeceptor)

Que les accès sécurisés concernent des sites locaux ou distants, il est important de centraliser les logs, le monitoring, le reporting et la gestion de l'environnement afin d'obtenir des informations pertinentes et de gérer efficacement l'infrastructure d'accès sécurisé. La centralisation des logs, du monitoring et du reporting peut être réalisée au niveau d'un centre opérationnel réseau (NOC) ou d'un centre opérationnel de sécurité (SOC).

Dans certains cas, un reporting centralisé s'impose à des fins de conformité en interne, avec notamment la mise à disposition d'informations pertinentes aux équipes de sécurité ou aux dirigeants d'entreprise. Ces informations sont essentielles à des fins de conformité réglementaire. L'opérateur ou le propriétaire des ressources peuvent avoir besoin de fournir ces informations aux CERT nationaux ou locaux.

Pour les accès sécurisés à grande échelle, la centralisation des opérations de gestion simplifie le pilotage de plusieurs technologies et allège les coûts de maintenance de ces technologies (mise à jour du logiciel ou du firmware).

De plus, pour suivre le rythme des menaces émergentes, des technologies avancées de protection contre les menaces (sandboxing, honeypots) peuvent être déployées de manière centralisée pour identifier les menaces internes ou externes et maîtriser les risques.

Une sécurité étroitement intégrée avec les solutions Fortinet

La gestion de collaborateurs distants et disséminés impose de centraliser la visibilité et la gestion de l'infrastructure de sécurité. Toutes les solutions Fortinet peuvent être intégrées à l'aide de la Fortinet Security Fabric, pour concrétiser l'idée d'une plateforme unifiée assurant les fonctions de visibilité, de configuration et de monitoring. Les connecteurs Fabric, notre environnement ouvert basé sur des API, l'accompagnement de la communauté DevOps et l'écosystème étendu de la Security Fabric permettent une intégration avec plus de 500 solutions tierces.

Lorsqu'une entreprise élabore son plan de continuité des activités, la visibilité et la gestion sur son architecture de sécurité sont essentielles, pour que cette entreprise puisse, si nécessaire, basculer rapidement vers le télétravail. Le travail à distance ne doit pas mettre en péril la cybersécurité d'une organisation.

Les solutions suivantes, qui font partie de la Security Fabric de Fortinet, permettent de sécuriser le travail et les opérations à distance :

FortiClient propose des indicateurs sur les terminaux, la gestion des vulnérabilités, la prévention des logiciels malveillants, un filtrage web, un pare-feu applicatif, un client VPN, un ZTNA et l'authentification MFA.

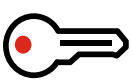
FortiClient EMS assure la configuration des clients VPN, ainsi que la gestion des politiques de sécurité des terminaux et des profils. La solution fait office de connecteur de la Security Fabric qui permet un déploiement et une gestion centralisés des clients.

FortiAP offre une connexion sécurisée avec un contrôleur sans fil et étend les réseaux vers les utilisateurs distants. La solution se déploie automatiquement, sans installation d'un client VPN logiciel.

FortiExtender offre une connectivité hybride WAN-LAN, une connectivité WAN sans fil flexible et est compatible aux réseaux cellulaires 3G, 4G et 5G. La solution est adaptée aux sites mobiles, aux flottes de véhicules et aux collaborateurs œuvrant sur le terrain.

FortiWiFi et **FortiGate** sont des contrôleurs sans fil sécurisés avec des services VPN et ZTNA. De multiples fonctionnalités sont proposées : contrôle d'accès avec application des règles, pare-feu NGFW, prévention des intrusions de nouvelle génération (NGIPS), connecteurs Security Fabric, politiques de sécurité dynamiques, SD-WAN et déploiement automatisé.

FortiToken confirme l'identité des utilisateurs à l'aide de jetons d'authentification matériels et logiciels. La solution s'intègre de manière transparente avec FortiGate et FortiAuthenticator, grâce à des jetons logiciels disponibles pour iOS et Android et une activation en ligne sécurisée avec les services de sécurité FortiGuard.



FortiAuthenticator assure la gestion de l'authentification avec intégration LDAP, RADIUS et SAML, la gestion du MFA et des jetons et la prise en charge des jetons matériels et logiciels. La solution joue le rôle d'autorité de certification.

FortiPAM assure la gestion, le contrôle et la surveillance des accès privilégiés et élevés, ainsi que des processus et systèmes critiques sur l'ensemble de l'environnement OT.

FortiAnalyzer offre une journalisation et un reporting centralisés, une visualisation centralisée des ressources et du réseau, ainsi qu'une gestion centralisée des événements et des incidents. La solution assure le traitement analytique des données réseau et de sécurité et se déploie en tant qu'appliance matérielle ou machine virtuelle (VM).

FortiManager permet une gestion et un monitoring centralisés, une automatisation de la sécurité, une intégration avec l'environnement existant, une administration multitenant fondée sur le rôle et le provisioning du SD-WAN. La solution se déploie sous forme d'appliance matérielle ou de machine virtuelle.

FortiSandbox mise sur l'IA pour détecter et répondre aux logiciels malveillants, tout en assurant une protection automatisée contre les vulnérabilités. Les analyses capitalisent sur le framework MITRE ATT&CK. La solution qui s'intègre avec FortiGate et la Security Fabric de Fortinet, est compatible avec les applications et protocoles ICS/OT. FortiSandbox se déploie en mode autonome ou centralisé, dans un format matériel ou sous forme d'une machine virtuelle.

FortiDeceptor utilise des leurres pour identifier et déjouer les cybermenaces à un stade amont. La solution simule des environnements Wndows, Linux, VPN et ICS. Elle s'intègre de manière transparente avec FortiGate et la Security Fabric de Fortinet. Compatible avec les applications et les protocoles ICS et de l'OT, elle se déploie en mode autonome ou centralisé, dans un format matériel ou en tant que machine virtuelle.

Un socle robuste pour garantir la continuité des activités

Se préparer à la continuité des activités et à la reprise après sinistre est essentiel, tant pour les acteurs de l'OT que pour ceux de l'IT. Lors de l'élaboration d'un plan de continuité des activités, les entreprises doivent s'assurer de disposer des ressources nécessaires pour sécuriser leurs travailleurs distants, permettre un fonctionnement ininterrompu de l'infrastructure OT et IT, en local et à distance, et assurer une posture de sécurité pertinente.

Les solutions Fortinet se déploient et se configurent simplement, pour permettre aux professionnels de l'OT et de l'IT de bénéficier d'une sécurité, d'une visibilité et d'un contrôle de bout en bout sur leurs ressources digitales, quelle que soit leur localisation.

[1] "2023 State of Operational Technology and Cybersecurity Report," Fortinet, 24 mai 2023.

novembre 24, 2023 12:40 PM

950814-A-0-FR