PRÉSENTATION DE SOLUTION

Fortinet OT Security Platform : la solution sécurité pour les systèmes cyberphysiques

Avant-propos

De plus en plus, les systèmes cyberphysiques des acteurs de l'industrie et de l'énergie deviennent la cible d'attaques pouvant interrompre leurs opérations, voire paralyser totalement leur appareil productif. Pour répondre à ce risque accru, la sécurité des technologies opérationnelles (OT) s'invite aujourd'hui à la table des discussions dans les Comex et conseils d'administration. Pour les RSSI, il est en effet urgent d'assurer ou, tout du moins, de renforcer la sécurité d'infrastructures OT autrefois isolées physiquement des autres systèmes, mais aujourd'hui connectées aux environnements IT[1].

C'est là que Fortinet OT Security Platform entre en jeu avec un système complet optimisé pour la sécurité des environnements OT. Au menu de la plateforme : sécurité réseau, modèle Zero Trust, solutions SecOps, Threat Intelligence dédiée et réseau vaste et inclusif de partenaires technologiques. Entièrement intégrées, toutes ces solutions permettent de consolider les différents produits de sécurité et d'en centraliser la gestion. Simplification des opérations, renforcement de la sécurité réseau, réduction du coût total de possession (TCO)… les industriels et compagnies d'énergie sont gagnants sur toute la ligne.

OT

Fortinet OT Security Platform est la seule solution classée Leader du Westlands Advisory Navigator 2023 des plateformes de protection réseau IT/OT[2].

L'importance de solutions OT dédiées

Dans le cadre de leurs missions de pilotage et de sécurisation des environnements OT, les RSSI et les équipes de sécurité doivent relever plusieurs défis de taille, y compris la sélection et la gestion d'un nombre souvent considérable de fournisseurs. Protéger des environnements aussi complexes tout en respectant les priorités opérationnelles (sécurité des équipes, fiabilité de la production, etc.) peut s'avérer difficile. C'est pourquoi beaucoup d'entreprises cherchent désormais à consolider les produits de différents fournisseurs, à converger leurs solutions IT et OT, et à optimiser l'utilisation d'équipes de cybersécurité en sous-effectif chronique. Pour répondre à ces enjeux, les RSSI ont besoin d'une plateforme de sécurité OT dotée de diverses fonctionnalités capables de s'intégrer en toute simplicité à leurs solutions existantes : connectivité unifiée, segmentation, sécurité Zero Trust et solutions SecOps.

Fortinet OT Security Platform est une suite complète de solutions réseau et de sécurité pour l'industrie, qui va de la connectivité initiale à des solutions SecOps pour l'OT, en passant par un modèle Zero Trust avancé.

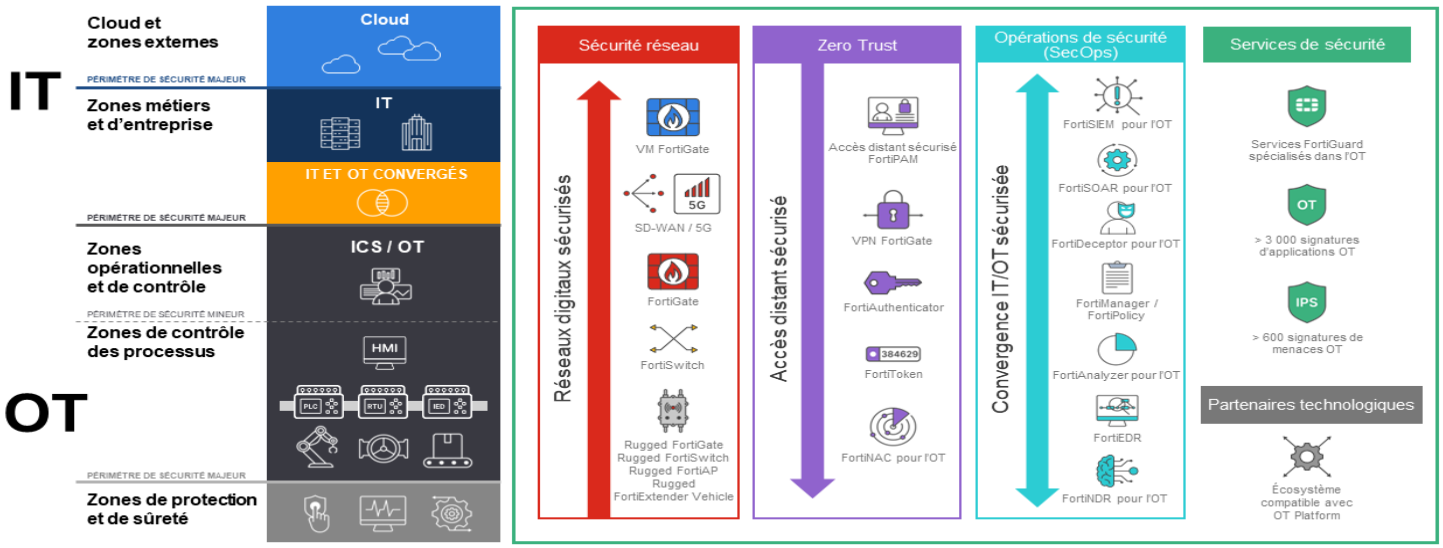

Figure 1. Fortinet OT Security Platform

Un réseau sécurisé garant de la connexion et de la protection des environnements OT

Fortinet OT Security Platform assure la connectivité initiale des systèmes cyberphysiques à l'aide des pare-feux nouvelle génération (NGFW) FortiGate, avant sur les commutateurs FortiSwitch de Fortinet ne prennent le relais pour segmenter le réseau. Ces solutions de connectivité critiques sont spécialement conçues pour les rigueurs opérationnelles des environnements OT, notamment grâce à leurs matériels résistants et à des services de sécurité OT avancés.

La plateforme de sécurité OT résout d'autres problématiques propres aux équipes de sécurité. Bien souvent, les systèmes et équipements OT sont en retard de correctifs, soit parce qu'ils sont en fin de support, soit parce que l'impératif de production l'emporte sur tout le reste. Pour y remédier, Fortinet OT Security Platform prend des mesures de sécurité proactives à plusieurs niveaux : contrôles de sécurité pour les applications et protocoles OT, segmentation réseau et microsegmentation des réseaux OT, et virtual patching pour la protection des équipements vulnérables au niveau du réseau.

En plus d'assurer la visibilité sur les ressources et les réseaux, la plateforme inclut Fortinet OT Security Service pour vous protéger contre les vulnérabilités des applications et protocoles OT des principaux fabricants de systèmes de contrôle industriel (ICS). Grâce aux signatures actualisées et aux données de protection contre les vulnérabilités, le pare-feu nouvelle génération FortiGate détecte les tentatives d'exploitation de vulnérabilités connues sur les systèmes OT. Fortinet OT Security Service couvre plus de 70 protocoles d'automatismes et de systèmes de contrôle industriels. Il s'appuie sur une liste de plus de 19 000 signatures de vulnérabilités, dont plus de 600 sont axées sur la sécurité OT et pilotées par le moteur de détection des intrusions de FortiGate.

En l'absence de correctifs sur la majorité des équipements et systèmes OT, le virtual patching (ou vulnerability shielding) s'avère essentiel pour détecter les exploits et prévenir les attaques. Fortinet OT Security Platform apporte les fonctionnalités suivantes :

- Contrôle de la sécurité et application des politiques via le pare-feu nouvelle génération FortiGate
- Visibilité et contrôle sur les utilisateurs et les équipements connectés, et microsegmentation du réseau grâce à FortiSwitch
- Monitoring, journalisation et reporting centralisés pour les appliances FortiGate déployées dans les environnements IT et OT grâce à FortiAnalyzer
- Gestion unifiée des équipements et implémentation centralisée des politiques de sécurité pour les appliances FortiGate sur l'écosystème IT et OT avec FortiManager
- Informations à jour exploitables en temps réel et mesures de réduction des menaces, vulnérabilités et exploits zero-day via les FortiGuard Labs

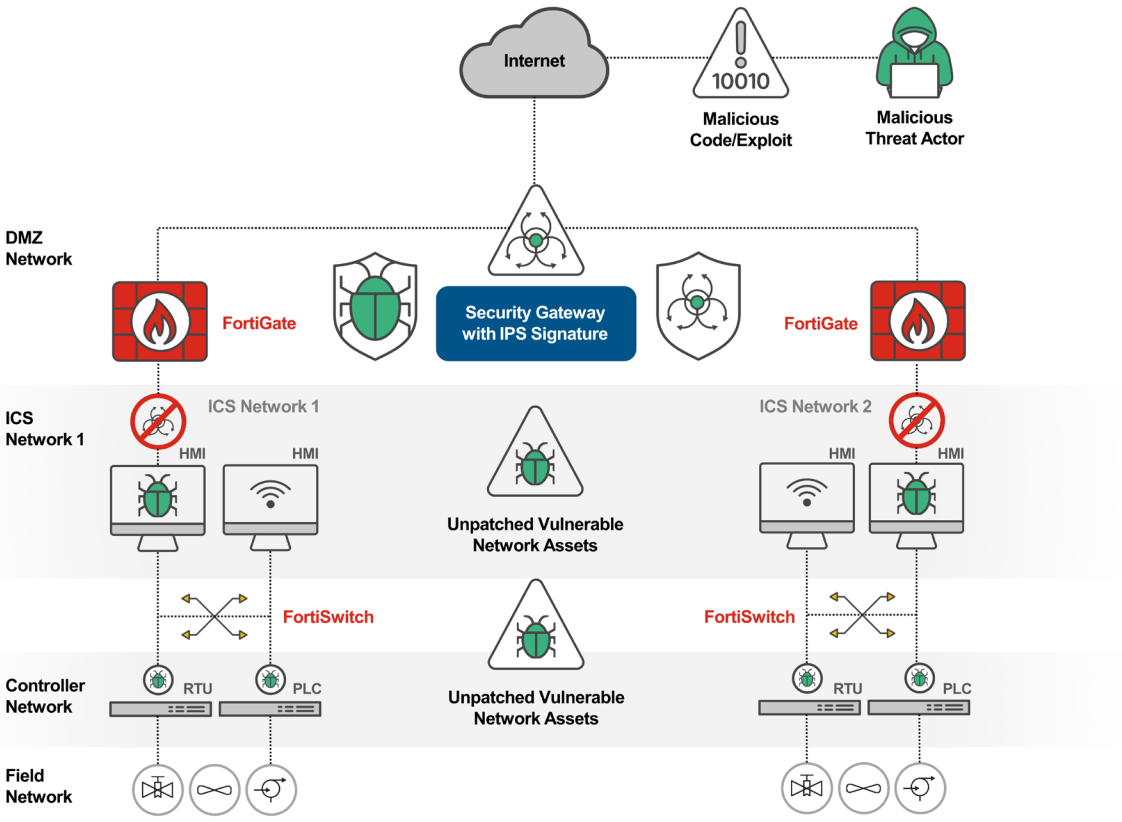

Figure 2. Virtual patching sur les réseaux ICS/OT

Solutions Zero Trust pour les technologies opérationnelles

Appliquer une stratégie Zero Trust aux réseaux OT n'est pas chose aisée. Primauté de l'opérationnel sur la sécurité, caractère sensible des réseaux et équipements ICS critiques, manque de solutions Zero Trust propres à l'OT… les obstacles sont nombreux. Pour résoudre ces problématiques, OT Security Platform embarque trois fonctionnalités majeures : la sécurisation des accès distants (SRA), la gestion des privilèges d'accès (PAM) et le contrôle d'accès au réseau (NAC).

Très efficaces individuellement, ces solutions fonctionnent également en parfaite synergie pour authentifier les utilisateurs et les entités qui se connectent au réseau OT. Elles limitent ainsi l'accès aux seules ressources correspondant aux rôles de l'équipement ou de l'utilisateur en question. Quant aux solutions Zero Trust de Fortinet, elles connectent en toute sécurité les utilisateurs aux applications, peu importe où ils se trouvent et où l'application est hébergée.

Le NAC autorise les accès d'utilisateurs spécifiques aux applications, et identifie et sécurise les parcs IT, OT et IIoT (Internet des objets industriels). Pour les opérateurs et les responsables de ressources (asset owners), cela se traduit par une visibilité totale et un contrôle renforcé sur tout élément connecté au réseau. FortiPAM, FortiAuthenticator et FortiToken sont des solutions de gestion des identités et des accès. Ensemble, elles permettent de restreindre l'accès aux seuls utilisateurs approuvés. En parallèle, la segmentation FortiGate renforce les accès Zero Trust en subdivisant les réseaux IT/OT selon les besoins métiers. L'architecture Zero Trust de Fortinet s'articule autour de plusieurs solutions :

- FortiGate est un pare-feu nouvelle génération qui assure les contrôles de sécurité et l'application des politiques.
- FortiNAC offre visibilité, contrôle et réponse automatisée pour tous les éléments connectés au réseau.
- FortiToken permet l'authentification à deux facteurs avec mot de passe à usage unique (OTP), notifications push ou jeton OTP matériel éphémère.
- FortiAuthenticator procède 1) à l'authentification unique (SSO) et à l'autorisation des utilisateurs, 2) au contrôle des autorisations d'accès des systèmes tiers et 3) à l'envoi de demandes d'accès au pare-feu nouvelle génération FortiGate pour implémenter des politiques de sécurité basées sur les identités.
- FortiPAM gère les identités et les privilèges d'accès et veille à l'implémentation d'une sécurité Zero Trust sur les ressources critiques. L'outil contrôle les accès aux applications et systèmes vitaux, suit et surveille l'activité utilisateur, et sécurise les accès distants aux ressources critiques.

D'après Gartner : « À l'heure où les entreprises cherchent à simplifier leurs opérations, les fournisseurs consolident leurs plateformes autour d'un ou de plusieurs domaines clés de la cybersécurité. Par exemple, une plateforme commune peut offrir des services de sécurité des identités et, en même temps, régir la gouvernance, les privilèges d'accès et la gestion des accès. Les responsables sécurité et de la gestion du risque doivent constamment inventorier leurs contrôles de sécurité pour identifier les doublons et limiter les redondances grâce à des plateformes consolidées[3]. »

Des SecOps pensés pour la sécurité OT

Grâce à une plateforme conçue spécialement pour l'OT, vous pouvez intégrer de multiples sources de données pour accélérer les détections et automatiser les réponses aux événements de sécurité. Les solutions SecOps de Fortinet répondent spécifiquement aux exigences de sécurité OT. Ainsi, elles assurent l'identification des ressources et la communication réseau avec une carte topologique alignée sur le modèle Purdue, MITRE ATT&CK pour la matrice ICS et le reporting de risque et de conformité.

Les équipes IT et OT doivent également trouver un juste équilibre entre les impératifs de sécurité et les priorités opérationnelles. D'où l'importance de pouvoir déléguer certaines actions de remédiation aux équipes opérationnelles et de sécurité OT, car elles sauront trouver le juste équilibre entre réduction du risque et continuité de la production et des services. Le but ultime : créer et optimiser un SOC convergé IT/OT qui rassemble Threat Intelligence, analytique, détection des menaces, leurres ou honeypots, réponse à incident, threat hunting, gouvernance et conformité, sans jamais déstabiliser l'environnement OT. Pour ce faire, les solutions SecOps de Fortinet incluent des outils indispensables :

- FortiGate est un pare-feu nouvelle génération qui assure les contrôles de sécurité et l'application des politiques.
- FortiEDR opère une détection et une protection automatiques et en temps réel contre les menaces sur les terminaux, l'orchestration de la réponse à incident et les analyses forensiques.

- FortiSIEM ingère et analyse les données de journaux des systèmes IT et OT, puis corrèle les comportements suspects transverses aux deux environnements. Cet outil affiche également les activités malveillantes répertoriées dans le framework MITRE ATT&CK pour les environnements IT et ICS d'entreprise.
- FortiSOAR est une plateforme SecOps personnalisable qui fournit des playbooks automatisés, trie les incidents et les résout en temps réel. Elle permet ainsi aux entreprises d'identifier les attaques et d'organiser la riposte.
- FortiDeceptor gère le déploiement d'honeypots afin de leurrer, d'exposer et d'éliminer les menaces internes et externes avant qu'elles ne provoquent des dommages.
- FortiNDR apporte des fonctions de détection et de réponse sur le réseau (NDR) pilotées par IA et par des réseaux de neurones artificiels, pour des investigations effectuées en moins d'une seconde. Grâce au deep learning, cet outil agit en appui des analystes SOC pour répondre automatiquement à différents types d'attaques. Pour ce faire, FortiNDR intègre un analyste de sécurité virtuel qui identifie puis classe les menaces pour y répondre rapidement.
- SOCaaS (Security Operations Center-as-a-Service) est un service cloud managé de surveillance de la sécurité. Sa mission : analyser les événements générés par les pare-feux nouvelle génération FortiGate et d'autres produits de sécurité. Il procède ainsi au tri des alertes et signale les menaces avérées.
- FortiRecon est un service SaaS qui assure une protection contre les risques digitaux grâce à trois modules performants : gestion de la surface d'attaque externe, protection de la marque et Threat Intelligence spécifique aux différents groupes cyber connus. La solution vous montre ce que vos adversaires peuvent voir, ce qu'ils font et ce qu'ils planifient. Vous pouvez ainsi les contrer dès la phase de reconnaissance et réduire considérablement le risque, la durée et les coûts par rapport à une résolution plus tardive.

Cap sur la consolidation et la convergence avec OT Security Platform

Comme nous l'avons évoqué plus haut, la sécurisation des systèmes cyberphysiques est un défi technique complexe, car souvent en conflit avec les priorités opérationnelles. La sécurité des environnements OT passe d'abord par la connexion sécurisée des réseaux OT au reste de l'entreprise, parfois même pour la première fois. Ceci est la base pour implémenter un SOC OT 100 % opérationnel. En outre, beaucoup d'entreprises cherchent à optimiser leurs opérations en consolidant leurs solutions et en convergeant leurs ressources IT et OT. C'est là que Fortinet OT Security Platform intervient grâce à sa connectivité réseau dédiée à l'OT, à son modèle Zero Trust et à ses solutions SecOps. Pour les RSSI chargés de la sécurité OT, la plateforme Fortinet apporte toute la flexibilité et les solutions indispensables pour sécuriser leurs environnements industriels.

[1] Fortinet 2023 State of OT and Cybersecurity Report.

[2] Fortinet Named Sole Leader in 2023 IT/OT Network Protection Platforms Navigator™ Report, 27 juillet 2023.

[3] Gartner, Gartner Identifies the Top Cybersecurity Trends for 2023, 12 avril 2023.

FORTINET

www.fortinet.com/fr

26 février 2024 17:38
2436831-0-0-FR