

Fortinet apporte la visibilité et la protection de la Security Fabric à l'IIoT industriel

Fortinet renforce la sécurité de l'Internet des objets (IIoT) et dépose de nouveaux brevets dans le cadre de sa politique d'innovation

John Maddison, Senior Vice President en charge des produits et solutions chez Fortinet

“Les attaques visant l'Internet des objets démontrent à quel point des milliards de dispositifs connectés peuvent être utilisés en tant qu'arme pour lourdement peser sur les économies digitales mondiales, les infrastructures critiques et des millions d'utilisateurs. La sécurité du périmètre particulièrement large de l'IIoT passe par une architecture qui se dimensionne à l'ensemble de l'infrastructure. Cette sécurité doit offrir une visibilité complète, une fonction de segmentation et une protection de bout en bout. La Security Fabric de Fortinet protège les multiples vecteurs d'attaque de l'IIoT, en offrant les performances et la veille sur les menaces nécessaires pour identifier, segmenter et donc protéger ces multiples vecteurs d'attaques issus de l'IIoT”

L'essentiel

Fortinet® (NASDAQ: FTNT), le leader mondial des solutions de cybersécurité hautes performances, annonce FortiGuard Industrial Security Service, une nouvelle offre dont l'ambition est d'apporter la visibilité, le contrôle et la protection de la Security Fabric de Fortinet à l'IIoT des objets industriels. (IIoT)

- [FortiGuard Industrial Security Service](#) (ISS) capitalise sur les services de veille sur les menaces de FortiGuard Labs et offre un contrôle applicatif et des outils de défense conçus pour les infrastructures critiques et les organisations industrielles (utilities, pétrole et gaz, transports et production notamment).
- Nombre de clients dans le monde, issus de secteurs aussi variés que la production, les ressources naturelles, l'aviation ou encore les services publics, retiennent les solutions de sécurité de l'IIoT proposées par Fortinet pour protéger leurs réseaux industriels et leurs endpoints.
- Fortinet renouvelle son engagement à protéger l'IIoT avec de nouveaux brevets dédiés.

La veille sur les menaces FortiGuard protège l'IIoT industriel

La demande de la part des entreprises et du grand public est à l'origine d'une véritable explosion du nombre d'objets intelligents connectés aux réseaux mondiaux. [McKinsey estime](#) à 20 à 30 milliards le nombre d'objets connectés à l'horizon 2020, contre 10 à 15 milliards en 2015. Cependant, cette prolifération d'équipements s'accompagne de risques de sécurité qui progressent également.

Traditionnellement, les réseaux commerciaux et industriels et leurs objets connectés ont fonctionné de manière cloisonnée, mais l'émergence des villes intelligentes et des maisons connectées incite à intégrer les objets connectés au sein d'infrastructures locales, nationales ou mondiales. Les organisations doivent donc repenser la sécurité de leurs réseaux et équipements informatiques, opérationnels et IIoT. L'intégration d'outils de sécurité distincts au sein d'une architecture de sécurité unifiée (Security Fabric) aide les organisations à recueillir et corréliser les informations sur les menaces, pour identifier tout comportement suspect et orchestrer automatiquement les actions nécessaires à la protection des différents vecteurs d'attaque de l'IIoT. FortiGuard ISS protège les systèmes de contrôle industriels les plus courants, ainsi que les applications et dispositifs SCADA (Supervisory Control And Data Acquisition). Ce nouveau service reçoit des informations temps-réel sur les menaces pour se protéger des vulnérabilités et déployer une visibilité et un contrôle précis sur les systèmes industriels et SCADA. Les

organisations peuvent ainsi gérer l'accès vers leurs infrastructures IIoT tout en sécurisant les vecteurs d'attaque. FortiGuard ISS vient au renfort des [appliances de sécurité de qualité industrielle de Fortinet](#), conçus pour fonctionner au sein d'environnements complexes et rigoureux.

Des organisations mondiales sécurisent leur IoT grâce à Fortinet

Nombre d'organisations, de taille et de métiers différents, ont adopté la Security Fabric de Fortinet pour relever les défis qu'elles rencontrent :

- **Gibsons Energy** – Cet acteur majeur du pétrole et du gaz, spécialisé dans les opérations intermédiaires entre l'extraction et la distribution, dispose d'une infrastructure multisite de grande envergure et souhaite mieux sécuriser sa migration vers le cloud et la gestion de ses dispositifs IoT sur le terrain. " Nos objets connectés se comptent par milliers et nous devons, jusqu'à présent, les gérer manuellement. Désormais, nous envisageons de les connecter au cloud pour analyser nos opérations de manière pertinente", explique Richard Hannah, Vice-président en charge des services d'informations chez Gibson Energy. "En collaborant avec Fortinet, nos équipes d'exploitation pilotent ces dispositifs en temps réel, avec, à la clé, des économies évaluées à plusieurs milliers d'heures-hommes et une sécurité optimale de nos infrastructures. "
- **Ville de Mumbai** – Le gouvernement de l'état indien du Maharashtra a retenu Fortinet dans le cadre du projet Mumbai WiFi. L'équipementier contribue à déployer un accès Internet sans fil sur les principaux quartiers de la ville, via des hotspots Wi-Fi à disposition des citoyens et d'applications de parking et de transports intelligents. "Le projet Mumbai WiFi joue un rôle essentiel dans l'apport du digital à nos citoyens. Notre objectif est d'offrir un Wi-Fi public sur toutes nos principales zones urbaines, pour ainsi fournir nombre de services gouvernementaux en ligne », explique Vijay Kumar Gautam, Principal Secretary Information Technology au sein du gouvernement du Maharashtra. "Compte tenu de la nature hyper-connectée de notre infrastructure publique actuelle, un projet aussi ambitieux nécessite une technologie évolutive et flexible, capable de prendre en charge davantage d'utilisateurs, d'équipements et d'applications sur le long terme ».

Une solution intégrée au service de la sécurité de l'IoT

Fortinet sécurise l'IoT grâce à ses solutions intégrées qui sécurisent chaque vecteur d'attaque. La sécurité des objets connectés professionnels nécessite des fonctions d'identification, de segmentation et de protection. Fortinet propose justement des solutions dédiées : [FortiOS](#), [FortiGate](#), [FortiSIEM](#), [Secure Access](#), [FortiGuard Threat Intelligence](#) et [Advanced Threat Protection](#). De plus, l'écosystème [Fabric Ready Partner](#) de Fortinet favorise une intégration évoluée et une protection intégrale via des partenariats technologiques, grâce aux solutions de sécurité endpoint et IoT d'éditeurs tels que [ForeScout](#), [Nozomi Networks](#) et [SentinelOne](#).

Sécurité de l'IoT : à la pointe de l'innovation

Fortinet a toujours misé sur l'innovation et détient aujourd'hui le nombre le plus important de brevets du secteur en matière de sécurité de l'IoT, prenant ainsi le large sur ses concurrents. De tels brevets sont essentiels pour pérenniser le leadership de Fortinet et à la conception de solutions de sécurité novatrices pour l'IoT, dans les domaines suivants :

- Système de gestion et de sécurité de l'Internet des objets
- Détection des intrusions IoT au niveau physique
- Fingerprinting des clients IoT IPv6 pour une autoconfiguration stateless
- Techniques comportementales pour identifier les attaques IoT menées par Wi-Fi.

La politique d'innovation et le savoir-faire de Fortinet ont été récompensés par le marché, comme le souligne la nomination de Fortinet au nouveau palmarès [Fortune Future 50](#) qui liste les

entreprises positionnées pour une forte croissance dans le futur.

Ressources supplémentaires

- Rendez-vous sur la page de [FortiGuard Industrial Security Service](#) pour plus d'informations.
 - Plus d'informations sur les solutions Fortinet dédiées à la sécurité de l'IoT [ici](#).
 - Plus d'informations sur les solutions Fortinet dédiées à la sécurité des systèmes de contrôle industriels et SCADA [ici](#).
- Suivez Fortinet sur [Twitter](#), [LinkedIn](#) et [Facebook](#).
- Rejoignez-nous sur le [blog Fortinet](#).

À propos de Fortinet

Fortinet (NASDAQ: FTNT) assure la sécurité des entreprises, fournisseurs de services et administrations parmi les plus grandes au monde. Fortinet apporte à ses clients une protection intelligente et transparente, véritable ligne de défense d'une surface d'attaque qui s'étend. Cette sécurité affiche des performances pérennes, adaptées à des réseaux décloisonnés. Seule l'architecture Security Fabric de Fortinet est capable de déployer une sécurité sans compromis pour relever les défis de sécurité les plus critiques au sein des environnements réseaux, applicatifs, cloud ou mobiles. Plus de 320 000 clients dans le monde font aujourd'hui confiance à Fortinet pour les protéger. Pour en savoir davantage : <http://www.fortinet.com>, le [blog](#) Fortinet ou [FortiGuard Labs](#).

FTNT-O

Copyright © 2017 Fortinet, Inc. All rights reserved. The symbols ® and ™ denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCloud, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiSIEM, FortiAP, FortiDB, FortiVoice, FortiWeb and FortiCASB.

Fortinet does not independently endorse such statements. Notwithstanding anything to the contrary herein, nothing herein constitutes a warranty, guarantee, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release contains forward-looking statements that involve uncertainties and assumptions, such as statements regarding program, technology and functionality releases and release times. Changes of circumstances, product release delays or product priority or roadmap changes, or other risks as stated in our filings with the Securities and Exchange Commission, located at www.sec.gov, may cause results to differ materially from those expressed or implied in this press release. If the uncertainties materialize or the assumptions prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Fortinet assumes no obligation to update any forward-looking statements, and expressly disclaims any obligation to update these forward-looking statements.