

## FORTINET, ACTEUR MAJEUR EN MATIÈRE DE CYBERSÉCURITÉ

Entreprise mondiale fondée en 2000 à la croissance très rapide, **Fortinet** est, avec plus de 4800 salariés, une multinationale spécialisée en cybersécurité proposant des solutions uniques pour les organisations de toutes tailles, des PME aux grandes entreprises et aux fournisseurs de services, afin de sécuriser leurs environnements actuels et faire face aux menaces en constante évolution. Éclairages sur ce savoir-faire et cette expertise avec Christophe Auberger, Directeur Technique France, Fortinet.



Christophe Auberger

### Pouvez-vous nous présenter l'entreprise et vos fonctions ?

Fortinet s'emploie à fournir un environnement de sécurité le plus innovant et performant possible pour sécuriser et simplifier les systèmes d'information de nos clients. Nous fournissons des solutions de sécurité à plus de 320 000 clients actifs à travers le monde : des PME aux grandes entreprises, aux fournisseurs de services et instances gouvernementales. Des réseaux sans fil aux plateformes de messagerie, applications Web, cloud, objets connectés, centres de données physiques ou virtuels, entre autres, Fortinet offre des solutions de sécurité adaptées, flexibles et évolutives permettant de protéger les systèmes d'information de nos clients face aux cyberattaques, quel que soit le type d'industrie. En tant que Directeur Technique, mon rôle est de coordonner une

équipe d'ingénieurs experts en cybersécurité qui vont aider les clients à bénéficier de solutions de sécurité adaptées à leurs besoins dans le cadre de leur stratégie de sécurité IT. Je travaille également avec la R&D pour les demandes de fonctionnalités particulières, mais aussi à l'évolution future de nos solutions pour contrer les menaces et répondre aux défis de sécurité auxquels nos clients font face.

### Le Cloud Computing, l'Internet des Objets et notre économie digitale hyperconnectée exposent les entreprises à davantage de menaces en matière de sécurité. Quelles sont-elles ?

Actuellement, les ransomwares sont les menaces les plus répandues. Il s'agit de logiciels malveillants, prenant en otage les données. Le ransomware chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer. Peu coûteux et très lucratifs, ils se développent très vite, à raison de plusieurs centaines par jour.

En parallèle, on constate une autre tendance majeure : la professionnalisation du marché des vulnérabilités, facilement accessibles à l'achat sur des réseaux comme Tor. Certaines de ces vulnérabilités sont connues et font l'objet de correctifs par les éditeurs. D'autres sont inconnues et sont donc très intéressantes pour les cybercriminels, qui vont s'introduire dans les systèmes des entreprises et exfiltrer des informations.

### Comment s'en prémunir ? Quelle est la stratégie à adopter pour se protéger efficacement ?

À l'ère du monde numérique et des menaces qui en découlent, de nombreuses entreprises continuent à appliquer des stratégies de sécurité classiques, et aujourd'hui obsolètes, car non adaptées à l'accélération qui s'opère dans l'univers des affaires. Aucune technologie prise individuellement ne permet de se prémunir contre tous les types de menaces, obligeant à utiliser tout un arsenal de contre-mesures pour mieux se protéger. En résulte une plus grande complexité dans l'exploitation, car toutes ces technologies nécessitent des systèmes de gouvernance différents et ne communiquent pas nécessairement entre elles. De ce constat est née la Security Fabric : la vision Fortinet intégrant étroitement des composants matériels et logiciels sophistiqués, favorisant ainsi une communication directe entre les solutions et une prise en charge unifiée et rapide des menaces. Grâce à cette cohésion entre les différentes solutions de sécurité, Fortinet apporte à ses clients des fonctions d'automatisation, de veille, de contrôle tout en facilitant la gouvernance et l'exploitation.

Au sein de la Security Fabric, les pare-feux de nouvelle génération sont capables d'analyser les différentes informations qui transitent pour détecter des menaces connues ou non. Au besoin, ces informations sont envoyées sur un système de sandboxing – système permettant l'analyse comportementale rapide d'un élément



suspect dans un environnement sécurisé afin d'étudier son action et de détecter une menace potentielle – et va renvoyer la réponse au pare-feu. La Sandbox va alors générer une signature antivirus à la volée et la diffuser sur l'ensemble des modules de la Security Fabric : le pare-feu de nouvelle génération, le poste de travail, le système de protection des serveurs web, etc. On a donc un outil de confinement

#### **Quelques mots sur la prochaine entrée en vigueur du RGDP, Règlement européen général sur la protection des données?**

L'objectif du RGDP est de protéger les données personnelles au niveau de la collecte, du traitement, de la restitution jusqu'à la suppression. Demain, toutes les entreprises seront concernées, dès lors qu'il y a un fichier client ou un fichier salarié. La mise en conformité des entre-

Fabric de Fortinet est une solution pertinente simplifiant cette mise en œuvre. Elle offre un management centralisé, une vision en un seul point et une gestion de la sécurité globale, déployée sur l'ensemble des systèmes d'information. ■

METTRE EN PLACE DES MOYENS POUR SE PROTÉGER AFIN D'EMPÊCHER LA MENACE DE S'INTRODUIRE DANS LE SYSTÈME N'EST PLUS GARANTI. IL S'AGIT DAVANTAGE AUJOURD'HUI D'IDENTIFIER RAPIDEMENT LA MENACE POUR ÉVITER ET BLOQUER SA PROPAGATION.

entièrément automatisé, qui va bloquer la menace là où elle était, sans qu'elle puisse se propager.

Fortinet est également le seul acteur en cybersécurité à disposer d'une équipe de plus de 200 chercheurs déployée à l'échelle mondiale et dédiée à la recherche et veille de menaces Internet appelée FortiGuard. L'objectif? Offrir les meilleurs temps de réponse de l'industrie face aux nouvelles et émergentes menaces.

prises va nécessiter une approche intégrée de la sécurité, visant à faire cohabiter les différentes technologies ensemble et y apporter de la synergie. Or, les grandes entreprises ont souvent une multitude de solutions de sécurité, ce qui est difficile à intégrer. Ce niveau de sécurité accru sur la protection des données personnelles ne peut être atteint qu'en déployant des solutions de sécurité sur l'ensemble du système d'information de l'entreprise pour protéger les données durant tout leur cycle de vie, où qu'elles se trouvent. En cela, la Security

**FORTINET**®

[www.fortinet.com](http://www.fortinet.com)

# L'INVISIBLE DEVIENT VISIBLE

## **LES CYBERMENACES SONT INVISIBLES.**

Véhiculées par de nouveaux vecteurs tels que l'Internet des Objets, la mobilité ou le Cloud, elles peuvent échapper à une sécurité qui ne couvre pas la totalité du réseau. Une protection complète et coordonnée devient un impératif pour détecter et neutraliser ces menaces.

Fortinet est le seul acteur à proposer des solutions de sécurité pour le réseau, les applications, les data centers, le Cloud et les accès. Ces solutions collaborent entre elles au travers de fonctionnalités communes évoluées et d'une veille mutualisée sur les menaces. Cette approche intelligente et collaborative est la clé de voûte de la Security Fabric, une architecture signée Fortinet qui déploie une protection robuste, intégrée et intégrale, sur l'ensemble des vecteurs d'attaques.

**Fortinet – Maîtrisez les risques pour revenir à l'essentiel, votre cœur de métier.**

# **FORTINET**®

**FORTINET SECURITY FABRIC**  
Adaptive end-to-end network security

[www.fortinet.com/whyfortinet](http://www.fortinet.com/whyfortinet)

