FICHE SOLUTION

La Security Fabric de Fortinet pour protéger Microsoft 365

Synthèse

Fortinet Security Fabric offre une protection étendue, intégrée et automatisée des utilisateurs et des dispositifs sur l'ensemble du périmètre d'entreprise. Pour les entreprises utilisant Microsoft 365, la Security Fabric propose différents modules : FortiMail pour protéger la messagerie, FortiCASB pour surveiller l'usage, les données et les configurations de Microsoft 365, des outils pour une authentification multifactorielle et un accès réseau zero-trust et la sécurité des terminaux. La solution Secure SD-WAN offre une connexion rapide et sûre à Microsoft 365 et autres applications basées sur le cloud, tout en respectant les principes et recommandations de Microsoft 365 en matière de réseau.

La Security Fabric offre une visibilité et une protection sans précédent pour votre infrastructure (sur site et dans le cloud), tout en sécurisant les utilisateurs et les dispositifs. La détection des menaces avancées, leur prise en charge automatisée et l'évaluation continue des niveaux de confiance ont fait l'objet d'évaluations particulièrement positives de la part de tiers. Le pare-feu nouvelle génération (NGFW) FortiGate est la clé de voûte de la Security Fabric.

Une protection supplémentaire pour Exchange Online

Le courrier électronique est le vecteur de diffusion de 92,4 % de tous les malware et de 49 % des malware qui s'installent avec succès.[1] Au-delà des logiciels malveillants, le courrier électronique permet d'attirer les utilisateurs vers des sites de phishing, les expose à des escroqueries et peut être utilisé pour détourner des informations réseau sensibles. Microsoft propose des solutions de sécurité pour M365, telles que Exchange Online Protection et Advanced Threat Protection. Mais même lorsque déployée et correctement configurée, la sécurité native de Microsoft ne détecte avec précision que moins de 30 % des emails malveillants. Pour protéger vos utilisateurs, vos clients et votre entreprise, il est essentiel de déployer des outils de sécurité pour l'email. FortiMail et FortiCASB renforcent la sécurité native de Microsoft 365 avec :

- Les services de sécurité de FortiGuard Labs : antispam, antivirus, sandboxing, CDR (Content Disarm and Reconstruction), prévention des clics orientant vers des contenus malveillants, analyse des usurpations d'identité, etc.
- Des technologies de protection contre les pertes de données, également disponibles dans FortiGate et FortiCASB
- Un chiffrement des e-mails basé sur l'identité, robuste et simple à utiliser
- L'intégration avec FortiGate, FortiAnalyzer et FortiSIEM, pour une visibilité intégrale sur les évènements de sécurité
- Des API ouvertes pour partager, sur l'ensemble de Security Fabric, des informations de veille sur les attaques en plusieurs étapes initiées par e-mail

Tirez pleinement parti de la protection intégrée de FortiMail

Protéger intégralement les solutions dans le cloud est un vrai défi, compte tenu des fournisseurs de Software-as-a-Service (SaaS), comme Microsoft, qui contrôlent aussi bien l'infrastructure que la couche applicative. Heureusement, il est désormais courant que les principaux fournisseurs de services cloud proposent d'accéder à leurs applications via une API. C'est ainsi que procède FortiCASB pour enrichir la visibilité native qu'offre Microsoft 365 Admin Center, et proposer des outils de sécurité pour évaluer les utilisateurs, les comportements et les données associées à Microsoft 365 et autres applications SaaS. D'autre part, les fonctions avancées de FortiCASB étendent les règles de sécurité et les informations de veille aux data centers.

Plus précisément, les clients de Microsoft 365 peuvent :

- Inspecter les contenus en transit ou stockés pour détecter les menaces, grâce à la veille sur les menaces fournie par FortiGuard Labs et les services de sandbox
- Surveiller et valider les comportements des utilisateurs et les autorisations dont ils bénéficient
- Identifier et contrôler différents profils de données sensibles et valider leur légitimité par rapport à la réglementation du secteur ou aux règles d'entreprise
- Détecter et contrôler de la même manière d'autres applications et infrastructures dans le cloud
- Assurer l'intégration avec FortiGate, FortiAnalyzer et FortiSIEM, pour une vision d'ensemble de la sécurité, sur site et dans le cloud

Schéma 1 : FortiCASB s'intègre avec Microsoft 365 et étend la sécurité aux clouds SaaS.

Assurer une gestion solide des identités et des accès

Avec Microsoft 365, les pertes de données sensibles n'ont pas toujours pour origine un malware installé ou une erreur de la part d'un collaborateur. En 2020, le détournement d'identifiants reste une technique largement utilisée par les cybercriminels pour s'immiscer au sein d'un réseau. Pour maîtriser ce risque, Fortinet propose FortiToken, son outil de gestion des identités et des accès, ainsi que FortiAuthenticator.

Utilisés conjointement avec les services Active Directory (AD) de Microsoft 365, qui permettent une authentification Single Sign-On (SSO) notamment, les solutions de gestion des identités et des accès de Fortinet déploient les fonctionnalités suivantes pour renforcer la sécurité :

- Authentification à facteurs multiples, avec des jetons matériels ou logiciels (authentification par e-mail, SMS ou application mobile)
- Intégration avec des annuaires sécurisés comme AD
- Notifications « push » pour une validation en un clic sur les appareils mobiles
- Protection contre les attaques par force brute, avec suppression des informations critiques en cas d'échecs répétés d'authentification
- Service central d'authentification pour accéder aux ressources sur site et dans le cloud

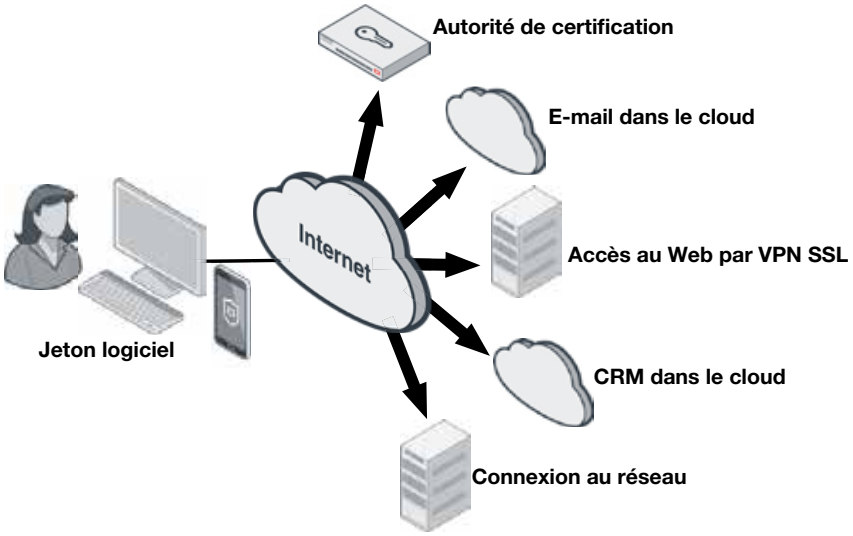

Schéma 2 : FortiToken contribue à protéger les données sensibles sur et hors du réseau, dans tous les types de clouds.

Pourquoi Fortinet

De nombreux fournisseurs tiers proposent leurs solutions de CASB, de sécurité des e-mails et de gestion des identités et des accès. Trois avantages distinguent Fortinet de ces fournisseurs :

1. Fortinet est le seul acteur à fournir un ensemble pertinent de fonctions de sécurité couvrant le réseau local, la messagerie électronique et les principaux services de cloud. Des services antimalware et de sandbox pour identifier les menaces traditionnelles et avancées, des capacités de protection contre la perte de données pour sécuriser les informations sensibles et une authentification multifactorielle font partie de ces fonctions.
2. Ces fonctions traditionnelles et avancées de protection contre les menaces ont été certifiées et approuvées par de nombreux tiers indépendants. Validées par Virus Bulletin, ICSA Labs, AV-Comparatives et NSS Labs, les solutions Fortinet fournissent une sécurité rigoureusement testée qui se déploie, de manière native ou via une API ouverte, sur l'ensemble de votre infrastructure de sécurité.

3. Avec une interface utilisateur et une gestion cohérente de l'ensemble des composants, Fortinet accélère les opérations de déploiement, de configuration, de monitoring et de gestion de la sécurité pour Microsoft 365.

Schéma 3 : Fortinet offre une interface utilisateur commune à tous les composants de sécurité dédiés à Microsoft 365.

[1] « 2020 Data Breach Investigations Report, » Verizon, juin 2020.

FORTINET

www.fortinet.fr

Copyright © 2020 Fortinet, Inc. Tous droits réservés. Fortinet®, FortiGate®, FortiCare®, FortiGuard® et certaines autres marques sont des marques déposées de Fortinet, Inc., et les autres noms Fortinet mentionnés dans le présent document peuvent également être des marques déposées et/ou des marques de droit commun de Fortinet. Tous les autres noms de produit ou d'entreprise peuvent être des marques commerciales de leurs détenteurs respectifs. Les données de performances et autres indicateurs de mesure figurant dans le présent document ont été obtenus au cours de tests de laboratoire internes réalisés dans des conditions idéales, et les performances et autres résultats réels peuvent donc varier. Les variables de réseau, les différents environnements réseau et d'autres conditions peuvent affecter les performances. Aucun énoncé du présent document ne constitue un quelconque engagement contraignant de la part de Fortinet, et Fortinet exclut toute garantie, expresse ou implicite, sauf dans la mesure où Fortinet conclut avec un acheteur un contrat écrit exécutoire, signé par le directeur des affaires juridiques de Fortinet, qui garantit explicitement que les performances du produit identifié seront conformes à des niveaux de performances donnés expressément énoncés et, dans un tel cas, seuls les niveaux de performances spécifiques expressément énoncés dans ledit contrat écrit exécutoire ont un caractère obligatoire pour Fortinet. Dans un souci de clarté, une telle garantie sera limitée aux performances obtenues dans les mêmes conditions idéales que celles des tests de laboratoire internes de Fortinet. Fortinet rejette intégralement toute convention, déclaration ou garantie en vertu des présentes, qu'elle soit expresse ou implicite. Fortinet se réserve le droit de changer, de modifier, de transférer ou de réviser par ailleurs la présente publication sans préavis, et c'est la version la plus à jour de la publication qui est applicable. Fortinet rejette intégralement toute convention, déclaration ou garantie en vertu des présentes, qu'elle soit expresse ou implicite. Fortinet se réserve le droit de changer, de modifier, de transférer ou de réviser par ailleurs la présente publication sans préavis, et c'est la version la plus à jour de la publication qui est applicable.

décembre 7, 2020 11:18 AM

759500-0-1-FR

sb-FA-securing-M365-with-fortinet-security-fabric-942020