FORTINET

Guide partenaires - Ventes PME

Sommaire

Fortinet et les autres fournisseurs

Pourquoi tant d'entreprises préfèrent-elles Fortinet à la concurrence ?
En matière de cybersécurité, il existe de nombreux autres fournisseurs que vous pourriez proposer à vos prospects. Toutefois... :

- Beaucoup de fournisseurs ne travaillent que sur un nombre restreint de vecteurs d'attaque. D'autres proposent des produits et services présentant une évolutivité limitée. Elles ne peuvent faire face aux menaces qui guettent les plus grandes organisations. Résultat : alors qu'elles de développent, les entreprises en expansion sont contraintes de remplacer l'ensemble de leur parc de sécurité. Elles abandonnent alors les outils qu'elles possèdent et renoncent à l'expertise de gestion durement acquise pour la gestion de ces technologies.
- La plupart des fournisseurs de plateformes de sécurité affichent des tarifs très élevés. Après achat, les entreprises n'ont plus les moyens d'investir dans des services de mise en œuvre et de supervision complémentaires mais pourtant essentiels. Les mauvaises configurations les amènent ensuite à blâmer leur fournisseur.
- De nombreux fournisseurs laissent leurs partenaires se débrouiller seuls. Ils partent du principe qu'ils comprennent parfaitement le marché de la sécurité, qu'ils savent écouter les besoins des clients et déceler seuls les nouvelles opportunités.

Fortinet est convaincu qu'une cybersécurité élargie, intégrée et automatisée doit être accessible au plus grand nombre. Les entreprises doivent pouvoir acquérir les technologies de cyber sécurité dont elles ont besoin, tout en ayant les moyens de solliciter des partenaires pour aider à leur mise en œuvre. C'est ainsi que les entreprises en expansion seront capables d'accéder en toute sécurité aux innovations de la cyber sécurité, sans perdre de vue leurs objectifs de croissance.

The Fortinet Security Fabric - Une protection globale, intégrée, automatisée

Fortinet Security Fabric assure aux entreprises une véritable intégration et une automatisation de leur infrastructure de sécurité. Elle offre protection et visibilité sur chaque segment de réseau, sur chaque dispositif et appliance, en environnement virtuel, cloud ou en déploiement local.

Global
Visibilité sur l'ensemble de la surface d'attaque, pour gérer les risques avec plus de précision

Intégré
Pour éviter les complexifications liées aux produits multiples opérant en silos

Automatisé
Flux automatisés pour accroître la rapidité des opérations et des réponses

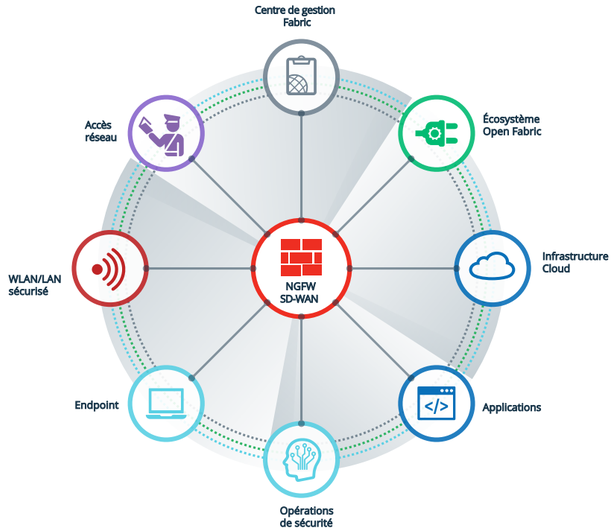


Figure 1 : Fortinet Security Fabric.

Notre Technologie

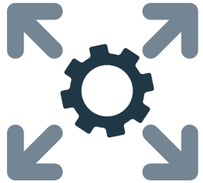
Nous avons conçu un processeur de sécurité (SPU) spécifique. C'est ainsi que nous sommes en mesure d'offrir les meilleures performances et la meilleur rentabilité du secteur, avec une puissance de calcul de sécurité de 3 à 47 fois supérieure aux autres approches logicielles.

Chaque jour, FortiGuard Labs traite et analyse plus de 10 milliards de cyberévénements dans le monde entier, en utilisant l'un des systèmes d'intelligence artificielle (IA) et de machine learning (ML) les plus efficaces du secteur. Les résultats sont envoyés en temps réel, sous forme de renseignements sur les menaces, aux clients de Fortinet.

Avec 662 brevets mondiaux, chiffre en constante augmentation, Fortinet éclipse les autres fourisseurs et prouve son engagement en matière de conception et d'ingénierie. Ensemble, FortiOS, la technologie SPU et nos renseignements sur les menaces générés par l'intelligence artificielle témoignent de notre engagement pour l'innovation et l'excellence en cybersécurité.

Des solutions conçues pour évoluer avec vos clients :

Certaines PME choisissent, à tort, des produits connus des consommateurs, mais dont les capacités de sécurité sont limitées. Ces solutions ne permettent pas de répondre aux besoins évolutifs des entreprises. Sans une solution conçue pour répondre à l'ensemble de leurs besoins (y compris à moyen terme), les entreprises devront abandonner les solutions dans lesquelles elles ont investi pour acquérir des technologies plus performantes. C'est un gaspillage de capital, de temps et d'énergie.



Des solutions évolutives, faciles à implémenter, adaptées aux PME :

Fortinet fournit les meilleures solutions de sécurité adaptatives qui peuvent répondre à n'importe quel environnement et à toutes les exigences de sécurité des PME.
Plutôt que des produits isolés, nous proposons notre solution unifiée Security Fabric qui peut être implémentée, gérée et adaptée en fonction des besoins du client.

Un coût inférieur, de nouvelles opportunités commerciales :

Conçu pour la multilocation (multitenance), cette solution présente un coût total de propriété inférieur à ceux des autres fournisseurs. Fortinet propose un plus grand nombre de fonctionnalités facturables, des marges plus élevées et une grande flexibilité budgétaire.

Nous investissons dans le succès de nos partenaires

Les PME empruntent la route du numérique. Elles ont besoin d'aide pour rester en sécurité et focaliser leurs efforts sur leurs projets générateurs de revenus. Les migrations vers des applications et une infrastructure cloud, le passage au marketing numérique et l'adoption d'applications mobiles impliquent des risques inédits. Des violations de données peuvent se produire et des amendes coûteuses peuvent en résulter. De tels préjudices peuvent causer la perte d'une entreprise. C'est là que vous intervenez - et c'est là Fortinet peut vous aider.

Fortinet est une entreprise 100% centrée sur ses partenaires. Nous vous fournissons la formation et l'accompagnement dont vous avez besoin pour vous démarquer. Vous pourrez ainsi poser les bonnes questions et savoir repérer les opportunités en matière de cybermenaces, de politiques de sécurité et de défenses réseau. Nous vous aiderons à fournir la fiabilité, la réactivité et les services dont les PME ont besoin. De cette manière, elles continueront à vous solliciter à mesure qu'elles se développent.

Vendez mieux, grâce à une formation gratuite en cybersécurité

Webinaires NSE Insider

Les webinaires NSE Insider permettent aux partenaires d'en apprendre davantage sur les solutions Fortinet. Ces webinaires offrent également un aperçu de la concurrence et des cybermenaces actuellement en circulation.

40 minutes pour développer votre entreprise

40 minutes pour développer votre entreprise La série de webinaires 40 Minutes, exclusivement réservée aux partenaires, présente les principales mises à jour de nos produits et solutions. Chaque présentation est réalisée en direct et suivie d'une séance de questions-réponses approfondie.

Formations accélérées

Une série d'ateliers gratuits, courts (une demi-journée) mais complets, axés sur Fortinet Security Fabric. Ce programme couvre les aspects techniques et commerciaux. Ces formations peuvent être dispensées en ligne ou en présentiel.

Programme de formation NSE

Le programme Fortinet Network Security Expert (NSE) guide les partenaires à travers 8 niveaux de formation et d'évaluation en sécurité des réseaux. De nombreux cours et exercices pratiques sont proposés pour vous permettre de maîtriser les concepts complexes de la sécurité réseau.

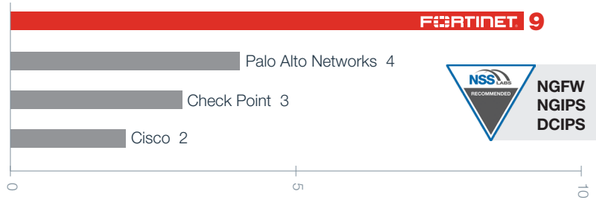
Figure 2 : Formation des partenaires Fortinet.

Contactez votre représentant Fortinet pour plus d'informations sur les certifications et les formations officielles proposées aux partenaires Fortinet.

#1 Validations indépendantes

NSS Labs, ISCA, VB, et plus

Source : Résultats des tests les plus récents de NSS Labs, au 31 décembre 2019. Voir les pages 10 et 11 pour plus de détails.



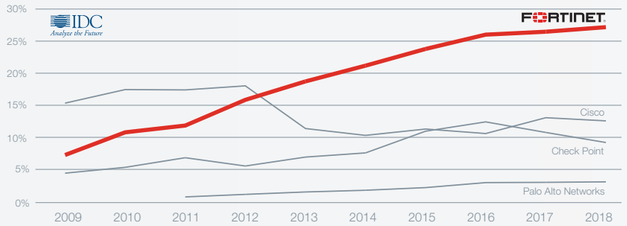
NSS RECOMMENDED

NGFW	DCSG	AEP
NGIPS	BPS	WAF
DCIPS	BDS	SD-WAN

#1 Sécurité réseau la plus déployée

~30% de toutes les expéditions d'appliances FW/UTM

Source : IDC Worldwide Security Appliance Tracker, mars 2019 (sur la base des livraisons annuelles d'appliances Firewall, UTM et VPN)

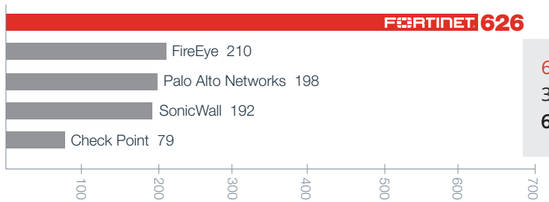


Source: IDC Worldwide Security Appliance Tracker, March 2019 (based on annual unit shipments of Firewall, UTM and VPN appliances)

#1 Innovateur en sécurité réseau

3x plus de brevets que les sociétés de sécurité réseau comparables

Source : Office américain des brevets, au 31 décembre 2019



626 Brevets américains
36 Brevets internationaux
662 Brevets mondiaux

+ de 440 000 clients à travers le monde

■ RECOMMANDÉ/CERTIFIÉ ■ AVERTISSEMENT O NON-MENTIONNÉ

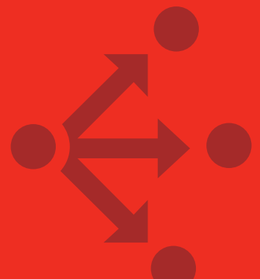
	CERTIFICATION	FORTINET	Check Point	Cisco	Palo Alto	Juniper SRX	FireEye
1	**NSS** Next-Gen Firewall	■	■	O	■	O	X
2	**NSS** DC Security Gateway	■	X	■	■	■	X
3	**NSS** Next-Gen IPS	■	X	O	■	O	X
4	**NSS** DC IPS	■ ■	X	■	X	X	X
5	**NSS** Breach Detection	■	X	■	X	X	■
6	**NSS** Breach Prevention	■	■	■	■	■	X
7	**NSS** WAF	■	X	X	X	X	X
8	**NSS** Advanced Endpoint	■	■	■	O	X	X
9	**NSS** SD-WAN	■	X	X	X	X	X
	ICSA ATD—Sandbox	■	X	X	X	■	X
	ICSA ATD—Email	■	X	X	X	X	X
	ICSA Network Firewall	■	■	X	■	X	X
	ICSA Network IPS	■	X	X	X	X	■
	ICSA Anti-malware Network	■	X	X	X	X	X
	ICSA WAF	■	X	X	X	X	X
	Virus Bulletin 100	■	X	X	X	X	■
	Virus Bulletin Spam	■	X	X	X	X	X
	Virus Bulletin Web	■	X	X	X	X	X
	Common Criteria	■	■	■	■	■	■
	FIPS	■	■	■	■	■	■
	UNH USGv6/IPv6	■	■	■	■	■	X

Le 4 février 2020

Sécurité et SD-WAN

L'ère du 100% chiffré frappe à la porte. Plus de 80 % du trafic réseau est désormais chiffré, contre environ 50 % en 2017.[1]

NSS Labs a constaté que l'activation du déchiffrement dégradait les performances firewall de 80 % et réduisait les transactions par seconde de 92 %.[2]



Catalyseurs du marché et principales problématiques

Comprendre et contrôler le trafic réseau sans interrompre les opérations

Les entreprises opèrent dans des contextes complexes. Il devient difficile pour les administrateurs réseau d'utiliser des politiques générales pour gérer la sécurité sans nuire à la productivité des utilisateurs. Le simple fait d'appliquer un blocage sur une application ou sur une catégorie d'utilisateurs peut conduire à une avalanche de plaintes et de tickets d'assistance. Pour contrôler et optimiser le réseau sans interrompre l'activité, les administrateurs doivent comprendre quels utilisateurs utilisent quelles applications, pour faire quelles actions. C'est en procédant ainsi qu'ils peuvent exercer des contrôles modulaires. En appliquant des politiques basées sur le fonctionnement réel de l'entreprise, ils peuvent obtenir un bien meilleur contrôle et une protection plus efficace.

Le déchiffrement du trafic, consommateur de performances

Durant l'analyse, le trafic chiffré peut masquer un code potentiellement malveillant. Il devient alors possible, pour les pirates informatiques, de contourner sans effort les mécanismes de sécurité en place. L'entreprise doit donc veiller à déchiffrer ce trafic pour l'inspecter. Or, un volume de trafic considérable doit désormais passer par les firewalls nouvelle génération (NGFW). De plus en plus d'applications quittent les centres de données traditionnels pour le cloud et les utilisateurs accèdent à d'importants volumes de données, depuis une multitude d'appareils. Il est nécessaire d'assurer un fonctionnement normal des opérations réseau avec toutes les fonctionnalités NGFW nécessaires activées. Si les processeurs ont déjà atteint leurs limites en matière d'inspection du trafic, l'ajout du déchiffrement entraînera une saturation du réseau, avec un impact significatif sur la productivité.

[1] « Encrypted Traffic Analysis Will Be Mandatory Soon » Security Boulevard, 10 janvier 2020.
[2] « NSS Labs Expands 2018 NGFW Group Test with SSL/TLS Security and Performance Test Reports » NSS Labs, 24 juillet 2018.

Applications cloud : garantir une expérience utilisateur de qualité

Les PME, en quête de flexibilité et de réduction des coûts, choisissent de se tourner vers le cloud. Cependant, les solutions traditionnelles WAN n'ont pas été conçues pour traiter et acheminer le trafic de manière à garantir des performances optimales pour les applications SaaS et cloud public. Certaines applications, telles que la VoIP et la vidéoconférence, peuvent présenter une qualité médiocre, voire même ne pas fonctionner. L'expérience utilisateur s'en trouve affectée, tout comme la productivité des employés.

Moins de dépenses, moins de complexité, plus de sécurité

Les entreprises distribuées utilisent traditionnellement des lignes dédiées telles que le MPLS (Multiprotocol Label Switching), qui assure le backhaul du trafic des succursales vers le datacenter, pour effectuer des contrôles de sécurité centralisés. Ces connexions sont, certes, sûres, mais elles sont également très coûteuses et lentes à déployer. Et, en cas de problème, une succursale entière peut se retrouver isolée jusqu'à ce que sa connexion soit réparée.

Les technologies WAN définies par logiciel (SD-WAN) ont permis de réduire les problèmes de coûts et de performances liés au MPLS en apportant aux succursales des connexions internet directes. La plupart des entreprises utilisent désormais deux appareils distincts pour gérer le trafic réseau : un appareil NGFW et un appareil SD-WAN mais il est complexe de reproduire les politiques de sécurité (applications, utilisateurs, NGFW) sur le dispositif SD-WAN.

Par ailleurs, certaines solutions SD-WAN avec sécurité intégrée présentent certains paramètres de sécurité pouvant dégrader les performances réseau. Par exemple, le fait d'activer l'inspection approfondie du trafic chiffré peut avoir un impact considérable sur les performances de débit. Enfin, toutes les solutions SD-WAN ne disposent pas d'options de sécurité ayant fait l'objet d'évalutations approfondies par des experts indépendants (comme les laboratoires NSS).

61 % des PME déclarent que la gestion des succursales et le maintien de la sécurité réseau constituent les motivations principales de leur déploiement SD-WAN.[3]

Quatre PME sur dix opèrent dans au moins cinq lieux physiques. Les équipes de travail géographiquement réparties recourent désormais à des applications professionnelles à forte intensité de bande passante (par exemple, la voix et la vidéo). Les besoins en bande passante et le nombre croissant d'appareils connectés au réseau incitent les entreprises à recourir au SD-WAN, qui constitue une option de déploiement abordable.[4]

[3] « Report: Security Concerns Spark Rise of SD-WANs in Small, Medium-Sized Businesses » Virtualization & Cloud Review, 9 sept. 2019.
[4] « The Benefits of SD-WAN for Branch Office Connectivity » Security Boulevard, 7 novembre 2019.

Présentation et avantages

SD-WAN et NGFW FortiGate : Innovation et gestion centralisée des appareils réseau

Les NGFW de FortiGate offrent une protection proactive contre les menaces grâce à une inspection minutieuse du trafic en clair et chiffré (y compris TLS 1.3). Les contrôles de politiques basés sur les utilisateurs, les applications, les appareils et/ou les catégories pertinentes (comme les différents services de l'entreprise) permettent un fonctionnement fluide et sécurisé, via l'inspection du trafic à l'entrée et à la sortie du réseau. Les différents modèles proposés permettent aux entreprises de sélectionner l'appareil correspondant à leurs besoins réels.

Fortinet Secure SD-WAN fournit des performances de pointe pour les applications SaaS (Software-as-a-Service) stratégiques : cette solution permet d'identifier les applications, d'attribuer automatiquement au trafic le chemin optimal et d'assurer une connectivité directe, via le cloud, vers les SaaS, les Infrastructure-as-a-Service (IaaS) et les installations de colocation. Fortinet Secure SD-WAN permet une adoption optimale des applications SaaS, un accès rapide en environnements multi-cloud et une expérience utilisateur de haute qualité. Toutes les pertes de données sont traitées avant qu'elle n'affecte l'application. Intégrée aux NGFW FortiGate, la sécurité protège l'ensemble de l'entreprise contre les attaques sophistiquées.

Le FortiGate fait également office de console de gestion principale. Les administrateurs peuvent ainsi étendre la sécurité aux dispositifs suivants :

- FortiGate (NGFW et SD-WAN)
- FortiSwitch
- FortiAP
- FortiExtender

SD-WAN inclus sans coût supplémentaire

Un NGFW leader du secteur, conçu pour les entreprises en expansion

- Intégration de plusieurs fonctions de sécurité au sein d'un unique NGFW FortiGate, en installation locale ou cloud
- Élaboration et gestion facile de politiques basées sur les utilisateurs, les applications et les appareils
- Réponse aux incidents accélérée grâce à une visibilité accrue, via des cartes de menaces personnalisées et des politiques one-click (exemple : mise en quarantaine des appareils)

Déchiffrement et performances

- Processeurs sur mesure répartissant intelligemment les fonctionnalités pour maintenir de haut niveaux de performances
- Coût total de possession (TCO) le plus bas (2$ / Mb/s) selon NSS5
- Efficacité de la sécurité : 99,3 % et blocage de 100 % des évasions[6]

Le SD-WAN intégré réduit les coûts, simplifie les opérations et offre des performances supérieures pour les applications

- Puce ASIC SD-WAN spécialement conçue pour des performances 10x supérieures aux solutions concurrentes[7]
- Reconnaissance automatique et acheminement optimisé de plus de 5 000 requêtes
- Reconnaissance des applications, renseignements automatisés sur les chemins réseau et prise en charge de la superposition WAN pour VPN

[5] « Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report » Fortinet, 19 juin 2019
[6]« Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report » Fortinet, 19 juin 2019
[7]« Fortinet's New SD-WAN Capabilities Help Achieve Maximum Application Performance » Fortinet, 9 avril 2019

Les NGFW de FortiGate offrent un large éventail de fonctionnalités et de services de sécurité intégrés

- Protection NGFW contre les menaces
- Inspection SSL/TLS
- Système de prévention des intrusions (IPS)
- Filtrage des URL
- Indice de sécurité
- Segmentation basée sur la finalité
- VPN IPsec/SSL
- Identité et authentification des utilisateurs/appareils
- Sandboxing
- Mise en réseau
- (LAN, WAN, Wi-Fi)
- Gestion et rapports

Abonnements FortiGuard

La plupart des clients ajoutent à leur achat des services d'abonnement FortiGuard pour obtenir une protection en temps réel et une couverture totale de la Fortinet Security Fabric. FortiGuard Labs propose une protection contre les menaces et des renseignements basés sur l'intelligence artificielle, pour protéger les clients contre les menaces les plus récentes. La supériorité de Fortinet dans la neutralisation des cybermenaces a été validée par des experts indépendants comme NSS Labs, Virus Bulletin, AV-Comparatives et d'autres organismes de tests.

SERVICE	PROTECTION UNIFIÉE	PROTECTION ENTREPRISE	PROTECTION 360
Cloud FortiManager			✓
Cloud FortiAnalyzer			✓
Monitoring de soutien cloud SD-WAN			✓
Superposition VPN SD-WAN One Click			✓
Service FortiConverter			✓
Service de sécurité industrielle		✓	✓
Indice de sécurité		✓	✓
AntiSpam	✓	✓	✓
Filtre web	✓	✓	✓
Protection avancée anti-malware	✓	✓	✓
IPS	✓	✓	✓
FortiCare + Application Control	✓	✓	✓

**Les offres groupées FortiGuard comprennent également une assistance FortiCare 24 heures sur 24, 7 jours sur 7. Mises à jour des microprogrammes. Abonnements aux politiques dynamiques FortiGuard*

De nombreuses PME choisissent l'offre Protection 360

Le pack de protection à 360 degrés s'appuie sur une architecture de sécurité intégrée avec une visibilité complète, un contrôle centralisé et des analyses de risques. Les entreprises disposent ainsi de plusieurs avantages :

- Réduction des risques grâce à des réponses automatisées, des configurations optimisées et une gestion améliorée
- Gains d'efficacité et de productivité grâce à l'élimination des processus manuels et à la centralisation du contrôle et de l'analyse
- Coût total de possession réduit grâce à la réduction des incidents nécessitant une intervention manuelle
- Assistance complète assurée par FortiCare ASE. Des ingénieurs spécialisés, présents dans le monde entier, ont conclu des accords de niveau de service ambitieux (SLA) pour que tous les problèmes soient résolus efficacement, en temps opportun.

FortiCloud Manager
Provisionnement Zero-Touch et gestion simplifiée grâce à un ensemble d'outils permettant de gérer de manière centralisée un nombre illimité de périphériques, depuis une console unique, avec contrôles d'accès définis en fonction des profils, gestion centralisée de la configuration, gestion des changements et conformité aux règles de bonne pratique.

Monitoring cloud SD-WAN
Le monitoring cloud SD-WAN permet de contrôler la qualité et la bande passante du SD-WAN cloud.

FortiConverter
FortiConverter offre un moyen simple de faire migrer vos configurations et politiques firewall existantes vers des politiques FortiGate. Cet outil permet également d'appliquer des règles réellement orientées sur les résultats opérationnels.

Évaluation de la sécurité
Fournit des outils d'audit pour identifier les vulnérabilités critiques et les défauts de configuration, et appliquer les règles de bonnes pratiques.

Filtrage Web
Blocage des sites web malveillants, piratés ou inappropriés.

IPS
Regroupe les données IP de sources malveillantes pour fournir des renseignements actualisés sur les menaces en temps quasi-réel. Bloque les attaques de manière proactive.

FortiAnalyzer Cloud
FortiAnalyzer Cloud permet aux clients d'identifier en temps réel les anomalies opérationnelles sur votre réseau.

Contrôleur VPN de superposition SD-WAN
Le contrôleur VPN de superposition SD-WAN est un service cloud permettant une orchestration simplifiée de la superposition.

Service de sécurité industrielle
Fournit des signatures pour les protocoles communs ICS/SCADA.

Antispam
Détection et filtrage des spams.

Protection avancée anti-malware
Technologies de pointe offrant une protection contre les menaces connues et inconnues. Comprend : antivirus, FortiSandbox Cloud, anti-botnet, protection mobile, Virus Outbreak Protection, désinfection des contenus et reconstitution.

Contrôle des applications
Fournit une visibilité en temps réel sur les applications que les utilisateurs exécutent. Permet d'améliorer la sécurité et de respecter l'application des politiques d'utilisation.

Accès sécurisé

Dynamiques et catalyseurs de marché

Les appareils se multiplient, la sécurité peine à suivre

En entreprise, les appareils de tout type se multiplient. Certains de ces appareils sont traditionnels (ordinateurs, smartphones, tablettes), d'autres appartiennent à la famille des objets connectés (caméras de sécurité, lecteurs de cartes, écrans publicitaires). Résultat : le réseau lui-même (commutateurs, points d'accès, étendeurs) et les produits de sécurité en silos peinent à suivre. Les coûts de gestion et de maintenance augmentent et des failles de sécurité apparaissent. Les entreprises doivent déployer une sécurité opérant comme un système global et cohérent, capable d'étendre facilement la protection à l'ensemble de l'infrastructure réseau et de partager automatiquement les renseignements sur les menaces. Sans cela, elles devront remplacer leurs solutions à mesure qu'elles se développent.

[8] « Cyberattacks and Your Small Business: A Primer for Cybersecurity » Business News Daily. 21 août 2019.
[9] « Ponemon's Third Annual Study on Third Party IoT Risk: Companies Don't Know What They Don't Know. » Business Wire. 7 mai 2019.
[10] « IDC's 7th Annual Global IoT Decision Maker Survey Reveals IoT as a Leading Digital Transformation Initiative, but Organizations Struggle with Skills Gaps and Infrastructure Readiness » IDC, 12 août 2019.

Face aux nombreuses décisions à prendre, les entreprises négligent souvent les mesures de cybersécurité. Le risque est alors de laisser aux pirates des points d'entrée.[8]

Ponemon fait état d'une augmentation spectaculaire (de **15** à **26 %**), depuis 2017, des violations de données ciblant les objets connectés, notamment les dispositifs non-sécurisés.[9]

85 % des professionnels interrogés dans **29** pays ont mené des projets consacrés aux équipements connectés (IoT).[10]

Présentation et avantages

Connectivité

- Installation plug-and-play des NGFW, commutateurs et points d'accès
- Architecture flexible et évolutive
- Options 3G/4G/LTE pour améliorer la flexibilité sans fil et assurer la continuité des opérations

Gestion et dépannage

- Gestion cloud, via un tableau de bord unique, de l'ensemble de l'infrastructure réseau
- Visibilité et dépannage simplifié depuis une plateforme unique
- Pas de frais de licence de gestion supplémentaires

Sécurité

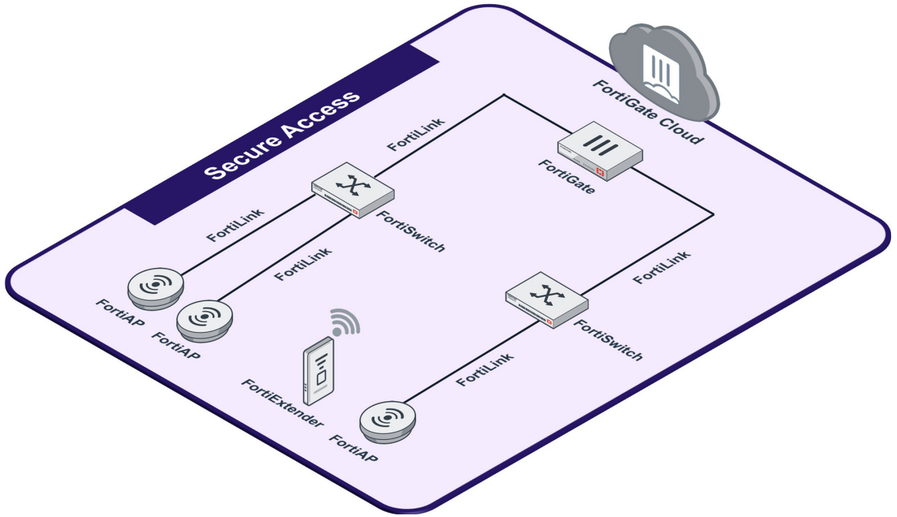
- Prolongement des politiques de sécurité au réseau WLAN et protection des transmissions sans fil sensibles
- Détections et corrections automatiques sur l'ensemble de l'infrastructure
- Partie de l'architecture Fortinet Security Fabric

Sécurité intégrale de l'infrastructure LAN

Les entreprises peuvent déployer la sécurité NGFW de Fortinet sur la couche d'accès réseau et la gérer depuis un unique panneau de contrôle géré via le FortiGate ou via FortiGate Cloud. Elles sont ainsi protégées lors d'ajouts - volontaires ou non - de nouveaux appareils au réseau.

Le provisionnement Zero-Touch accélère les déploiements, simplifie les opérations et réduit les coûts.

Fortinet fournit au réseau sécurité, performances et fiabilité, avec un contrôle unifié et une visibilité centralisée sur toute la surface d'attaque de l'entreprise.



FortiGate : Combine les fonctionnalités de pointe de NGFW et de SD-WAN au sein d'une solution unique livrée localement ou via le cloud, avec la possibilité de gérer les appareils ci-dessous depuis un panneau de contrôle unique.

FortiLink : Ce composant de FortiOS permet aux équipements réseau de devenir des prolongements intégrés de FortiGate. Les administrateurs peuvent gérer ces appareils grâce à des fonctions de provisionnement automatique et obtenir une visibilité sur l'ensemble de la couche d'accès réseau via FortiGate et FortiGate Cloud.

FortiSwitch & FortiAP : Commutateurs Ethernet et points d'accès Wi-Fi sécurisés, simples et évolutifs, disponibles en différents modèles pour satisfaire à des cas d'utilisation et à des fourchettes tarifaires spécifiques.

FortiExtender: Utilise la connectivité LTE pour fournir un haut-débit pouvant être utilisés pour le basculement, l'équilibrage de charge ou les connexions internet primaires pour les sites sans haut-débit.

FortiGate Cloud : Gestion centralisée via le cloud pour FortiGate, FortiSwitch, FortiAP et FortiExtender, depuis un unique panneau de contrôle.

Bureau cloud sécurisé

Dynamiques et catalyseurs de marché

Un manque de visibilité et de contrôle sur les différents SaaS et clouds publics

Les données voyagent instantanément d'un cloud à l'autre. Il est difficile d'effectuer un quelconque suivi de ces données. Les entreprises peinent à obtenir la visibilité et le contrôle dont elles ont besoin sur leur statut de sécurité, notamment lorsqu'elles recourent à plusieurs plateformes cloud disparates aux fonctionnalités et interfaces multiples, qui n'ont pas été conçues pour travailler ensemble. À cela, s'ajoute le désordre causé par le déploiement permanent de nouveaux services et applications cloud (souvent sans l'autorisation du service informatique). Les entreprises ont besoin d'un accès mondial, à la demande et sécurisé aux ressources du cloud, offrant des contrôles d'accès sophistiqués, un suivi des événements et des données d'analyses. Les VPN traditionnels d'accès à distance ne peuvent pas répondre à ces exigences.

La sécurisation des applications cloud

Les entreprises se tournent vers le cloud et les applications web deviennent leur nouvelle vitrine, leur nouveau point de vente. Si le cloud peut être tout aussi sécurisé que les solutions en installation locale, il introduit toutefois une complexité supplémentaire et étend la surface d'attaque. Les systèmes de gestion et d'orchestration cloud, les interfaces de programmation d'applications (API) ouvertes et l'intégration de processus de déploiement décentralisés contournent souvent les processus traditionnels de sécurité. Les applications deviennent plus vulnérables aux cybermenaces, notamment aux téléchargements « drive-by », au vol des identifiants et au vol de données sensibles.

La sécurisation des applications cloud nécessite des couches de sécurité supplémentaires : une protection réseau pour sécuriser les données en transit, une protection pour les applications web et une protection des plateformes cloud garantissant que ces applications et bases de données en ligne soient mises à jour et correctement configurées. À une heure où la pénurie d'experts se fait sentir dans le secteur, cette tâche devient particulièrement difficile pour les petites et moyennes entreprises.

Alors même que les dépenses SaaS ont augmenté de **78 %** l'an dernier, près de la moitié des responsables informatiques estiment que le développement du SaaS les rend aujourd'hui plus vulnérables aux menaces provenant de l'intérieur (initiés).[11]

61 % des PME utilisent une solution multi-cloud.[12]

Les violations de données accidentelles, dues à des erreurs humaines, à une mauvaise configuration et à des dysfonctionnements du système (par opposition aux attaques malveillantes ou criminelles) sont la principale cause de près de la moitié (**49 %**) des violations de données.[13]

[11] « SaaS Ecosystem Complexity Ratcheting Up Risk of Insider Threats » Dark Reading, 31 mars 2019.·
[12] « 2019 State of the Cloud Report » Flexera/RightScale, février 2019.
[13] « 2019 Cost of a Data Breach Report » Ponemon Institute and IBM Security, juillet 2019.

Présentation et avantages

Intégration native pour un déploiement simplifié

- S'intègre aux plateformes de cloud computing pour offrir une sécurité maximale sans surcharge opérationnelle
- Automatise les actions communes et réduit le besoin d'expertise en programmation ou dans le domaine du cloud, grâce à un tableau de bord intuitif
- Les modèles de configuration réduisent les erreurs et aide à automatiser les processus-clés tels que les déploiements cloud auto-scale

Protection élargie et automatisée en environnements multiclouds

- Blocage des menaces avancées grâce à une protection 0-day faisant appel au machine learning et à l'intelligence artificielle, notamment via le sandboxing
- Connectivité sécurisée et à haut débit pour les environnements cloud, sans ralentir les applications grâce au VPN/IP de sécurité (IPsec)
- Contrôle des applications (web et personnalisées) : création rapide de politiques permettant d'autoriser, de refuser ou de restreindre les accès

Gestion, visibilité et contrôle unifiés

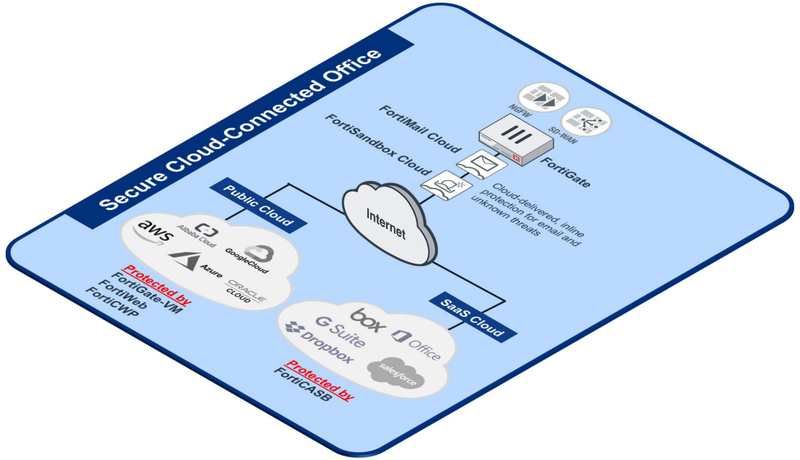
- Visibilité sur l'ensemble des applications, réseaux, infrastructures, événements de sécurité et logs, en environnement multi-cloud
- Établissement d'un cadre cohérent pour un meilleur contrôle des fonctionnalités propres à chaque plateforme cloud
- Gestion simplifiée de la sécurité globale : des politiques permettent de modifier les paramètres de sécurité en fonction des évènements liés au cycle de vie des applications

Cloud public

Les politiques de sécurité multiclouds sont appliquées contrôlées via un panneau de contrôle unique, pour sécuriser à la fois les applications et la connectivité. Les administrateurs disposent de rapports de conformité cohérents pour leurs environnements multi-clouds et peuvent effectuer des enquêtes simplifiées en cas d'incident.

SaaS

Avec Fortinet, les entreprises peuvent appliquer des politiques unifiées pour les contrôles d'accès, la consommation de ressources, les configurations et la sécurité.
Nos solutions analysent les fichiers stockés afin que les fichiers malveillants non-contrôlés ne puissent se répandre sur le réseau.
La centralisation du contrôle des applications SaaS permet d'appliquer les règles de bonnes pratiques en matière de conformité et de gouvernance, tout en réduisant la latence pour optimiser les performances des applications.



FortiGate : Associe des fonctionnalités NGFW et SD-WAN de pointe au sein d'une solution unique, disponible en installation locale ou cloud.

FortiGate-VM : Assure une sécurité cohérente et protège la connectivité en clouds publics et privés, tandis que les connexions VPN à haut-débit protègent les données.

FortiWeb : Le Firewall pour applications web de Fortinet protège vos applications web critiques contre les attaques ciblant les vulnérabilités connues et inconnues. Fortiweb couvre la réputation IP, la protection DDoS, la validation des protocoles, les signatures d'attaques d'applications, la neutralisation des bots, et plus encore.

FortiCWP : Évalue la sécurité de la configuration du cloud, détecte les menaces potentielles provenant de mauvaises configurations, analyse le trafic cloud (entrant et sortant) et évalue les respect des règles de bonnes pratiques.

FortiCASB : Conçu pour assurer visibilité, conformité et sécurité des données et pour protéger les services cloud contre les menaces. FortiCASB fournit des informations sur les utilisateurs, les comportements et les données stockées sur les principales applications SaaS. Cet outil propose également des outils de reporting complets.

FortiMail Cloud : Entièrement géré par Fortinet et assuré via le cloud, FortiMail Cloud assure une détection dess spams atteignant près de 100 %, une prévention avancée contre les menaces et une protection intégrée des données. FortiMail Cloud peut traiter plus de 1,5 million de messages par heure.

FortiSandbox Cloud : Offre une détection rapide et une réponse automatisée aux menaces inconnues, avec une solution cloud clé-en-main.

Les Fortinet Fabric Connectors fournissent une interopérabilité avancée et une intégration ouverte avec les technologies et plateformes partenaires en écosystèmes multifournisseurs. Ces composants peuvent être installés et configurés en quelques minutes, pour automatiser la sécurité et simplifier les processus de gestion.

Gestion et analyses

Dynamiques et catalyseurs de marché

Réduire la complexité, assurer le respect des réglementations et limiter les erreurs

Lorsqu'une entreprise se développe, les utilisateurs et les appareils se multiplient. Le réseau devient plus complexe à gérer. La conformité réglementaire peut alors poser problème, en particulier si les équipements ne sont pas destinés à être gérés de manière unifiée : le personnel doit, dans ce cas, corréler les données en utilisant les outils d'audit de chaque fournisseur. Il devient, par ailleurs, difficile de recruter des professionnels qualifiés pour déployer et configurer ces produits isolés. Les erreurs de configuration peuvent alors se produire, engendrant des pannes réseau, des problèmes de sécurité et une augmentation des opérations de dépannage.

Prise en charge des groupes d'utilisateurs et réseaux distribués

À mesure que l'entreprise se développe, les administrateurs doivent veiller à ce que le réseau puisse supporter des charges plus élevées. Le trafic doit être optimisé pour les services critiques et les outils de collaboration répartis sur le cloud et les succursales. Un tel travail s'avère difficile sans l'adoption de nouvelles technologies.

En 2019, les pannes de système ont causé **25 %** des violations de données. L'erreur humaine était à l'origine de **24 %** des violations.[14]

Deux tiers des entreprises s'emploient activement à réduire leur nombre de fournisseurs de services en cybersécurité afin d'optimiser leur efficacité opérationnelle et de réduire leurs coûts.[15]

59% des professionnels de la sécurité déclarent que la protection des informations personnelles identifiables (IPI) est leur priorité absolue.[16]

[14] « Cost of a Data Breach Report » Security Intelligence, 23 juillet 2019.
[15] « The cybersecurity technology consolidation conundrum » CSO, 26 mars 2019.
[16] « Compliance mandates, cybersecurity best practices dominate 2019 security priorities » CSO, 23 octobre 2019

Quelle option de gestion choisir ?

Présentation et avantages

Les avantages du cloud, en toute sécurité

Une croissance soutenue implique plus d'utilisateurs, plus d'appareils, plus de technologies à gérer. Pour garder le cap, les entreprises doivent comprendre comment mettre en place une protection unifiée et être capable de gérer efficacement les changements.

FortiGate Cloud

Basic Deployment et gestion individuelle des appareils via FortiGate

- FortiGate NGFW et SD-WAN, FortiSwitch, FortiAP, FortiExtender
- Pour chaque FortiGate, il est possible d'appliquer individuellement des configurations et d'extraire les logs si nécessaire

FortiManager et FortiAnalyzer en machines virtuelles ou cloud

Déploiements avancés et surveillance de l'ensemble de Fortinet Security Fabric

- Gérer + que : FortiGate NGFW et SD-WAN, FortiSwitch, FortiAP, FortiExtender
- Des configurations optimisées pour chaque région, succursale et/ou département de sécurité
- Regroupement d'appareils, domaines administratifs (ADOM)
- Agrégation des aperçus des différents groupes d'appareils et mise en commun rapide des logs

Une unique console de gestion SaaS

Fortinet offre aux entreprises en expansion une interface unique SaaS pour gérer l'ensemble de leur architecture de sécurité.

FortiCloud : *Basic Deployment*

FortiGate Cloud propose un éventail d'options de gestion sur FortiGate (NGFW et SD-WAN), FortiSwitch, FortiAP et FortiExtender.

Basic Deployment comprend les fonctionnalités suivantes :

- Provisionnement zero-touch (sans contact)
- Gestion de la configuration
- Rapports et analyses
- Sandboxing multitenants
- Indicateurs de compromission
- Authentification à deux facteurs

FortiManager et FortiAnalyzer : Déploiements avancés

Avec FortiManager, les administrateurs peuvent traiter efficacement les différents cas d'utilisation sur des déploiements différenciés. Avec FortiAnalyzer, il est possible d'obtenir des aperçus automatisés sur l'ensemble de leur Security Fabric.

Basic Deployment Plus comprend les fonctionnalités suivantes :

- Gestion et analyses pour l'ensemble de l'architecture Security Fabric
- Regroupement et gestion des appareils
- Configurations et flux de travail automatisés
- Agrégation des logs des ADOM optionnels de Security Fabric
- Rapports en temps réel sur les normes industrielles (PCI, DSS, NIST)
- Tableaux de bord destinés aux dirigeants

Les tests des laboratoires du NSS montrent que Fortinet Secure SD-WAN peut connecter une succursale en moins de six minutes grâce à ses capacités de déploiement zero-touch.[17]

[17] « Software-Defined Wide Area Network Test Report: Fortinet FortiGate 61E » NSS Labs, 19 juin 2019.

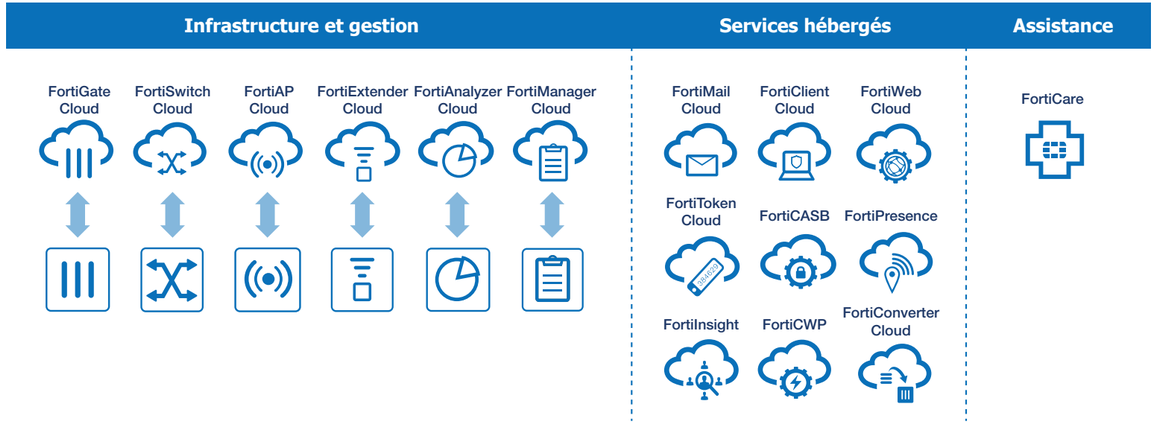
Gérez les solutions cloud Fortinet de tous vos clients

La Security-as-a-Service (SECaaS) est en plein essor. Grâce aux nombreuses offres Fortinet disponibles en version cloud, nos partenaires sont extrêmement bien positionnés pour lancer ou développer ces services en MSSP.

Disponible pour les clients et les partenaires, l'inscription à FortiCloud est gratuite. Elle fournit une solution cloud permettant de gérer facilement la suite de services cloud de Fortinet (y compris FortiCare) depuis un unique point de contrôle, accessible partout.

- Naviguez entre les plateformes de services cloud facilement et en toute sécurité
- Supervisez les droits et les tickets d'assistance pour l'ensemble des clients et des produits
- Gérez les paramètres des comptes et identifiants

Disponibilité des services de la plateforme de gestion FortiCloud



Service FortiCloud Premium

Avec l'abonnement FortiCloud Premium, les entreprises accèdent à des fonctionnalités supplémentaires comme la gestion des actifs. Ils bénéficient également de versions d'essai pour la gestion et les services cloud. Des fonctionnalités supplémentaires continueront d'être apportées afin d'améliorer la gestion à distance et les offres des partenaires. Pour plus de détails, veuillez contacter votre représentant compétent ou votre partenaire de distribution.

Stoppez les attaques de ransomware, les attaques de phishing et les menaces avancées

71% des attaques par ransomware visent les PME[18]

Les attaques de phishing ont atteint leur plus haut niveau en trois ans[19]

[18] « Beazley Breach Briefing – 2019 » Beazley, 21 mars 2019.
[19] « Phishing Activity Trends Report – 3rd Quarter 2019 » APWG, 4 novembre 2019.

Dynamiques et catalyseurs du marché

Le ransomware, principal vecteur d'attaque

Le ransomware reste le malware le plus utilisé par les pirates informatiques. Pour de nombreuses entreprises, les pertes liées aux paralysies des systèmes et des process dépassent de loin les coûts liés au ransomware lui-même.

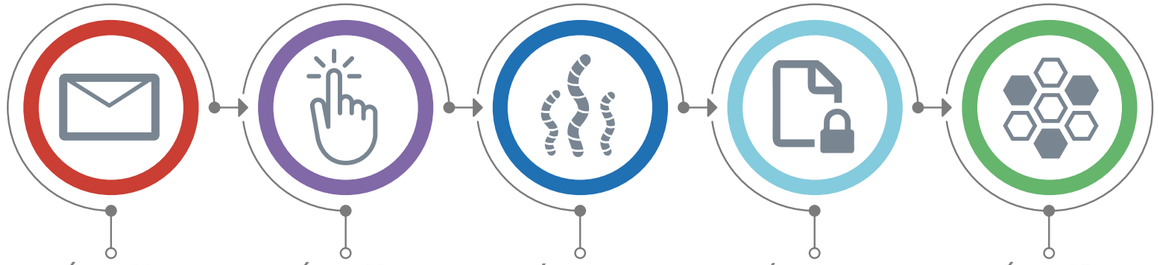
La sécurité peine à garder le cap face à des technologies en permanente évolution

En quête d'efficacité et de rapidité, les entreprises de toutes tailles adoptent des technologies innovantes (outils cloud, SaaS, appareils intelligents). Ces solutions apportent de nombreux avantages mais elles complexifient également les infrastructures. Elles créent des vulnérabilités et permettant aux menaces les plus élémentaires de franchir des défenses obsolètes, sur différents points d'entrée.

Facilité d'exécution

Le Ransomware-as-a-Service (RaaS) permet à des pirates informatiques d'investir dans une attaque conçue par d'autres. Des hackers jeunes, familiers des nouvelles technologies, peuvent alors - sans grande expérience - s'en prendre à des cibles d'envergure et exploiter des failles de sécurité. Ce phénomène explique notamment le nombre élevé d'attaques ransomware ciblant les PME.

La méthode ransomware



Étape 01

E-mail

Parmi les innombrables e-mails malveillants, certains parviennent à tromper les utilisateurs.

Étape 02

L'utilisateur clique. L'attaque débute.

Sans le filtrage URL (pour empêcher les utilisateurs de se rendre sur des sites malveillants) ou sans une protection efficace des endpoints (pour empêcher la détection et l'exécution de fichiers malveillants), l'attaque est déclenchée, sans éveiller de soupçons.

Étape 03

Réseau de vers

Sans prévention ni détection, les attaques traquent les données et les dossiers-clés. Elles désactivent les mécanismes de sauvegarde et de récupération.

Étape 04

Command & Control et chiffrement

L'attaque passe par le Command & Control pour communiquer avec le pirate informatique et chiffrer les fichiers

Étape 05

Mouvement latéral

Sans segmentation pour isoler les systèmes, le chiffrement se propage latéralement et recherche d'autres réseaux connectés

Présentation et avantages

Prévention

E-mail

Phishing—FortiMail
FortiMail est doté de puissantes capacités anti-spam et anti-malware. Cet outil fournit également d'autres fonctionnalités avancées : protection contre les épidémies de malware, désarmement et reconstitution de contenus, analyses par sandboxing ou encore détection des vols d'identifiants.

L'utilisateur clique. L'attaque commence.

URL malveillantes — Filtrage Web ForteGuard
Le service de filtrage web FortiGuard améliore les capacités de filtrage web de base des NGFW FortiGate en classant des milliards de pages web selon un grand nombre de catégories que les utilisateurs peuvent autoriser ou bloquer.

Protection des endpoints — FortiEDR
Les solutions FortiEDR de protection en temps réel des endpoints réduisent de manière proactive la surface d'attaque. Cete protection est assurée grâce au machine learning anti-malware et aux technologies de détection comportementale.

Vol d'identifiants - Authentification à deux facteurs avec FortiToken Mobile
Avec l'authentification à deux facteurs, un mot de passe est utilisé avec un token de sécurité et un serveur d'authentification afin d'assurer une sécurité optimale. Les employés habilités peuvent accéder aux ressources de l'entreprise en toute sécurité, depuis plusieurs appareils (ordinateurs portables, téléphones mobiles, etc).

Menaces connues et avancées - Service anti-malware Fort-Guard
La protection avancée contre les logiciels malveillants de FortiGuard Labs associe notre service antivirus (AV) récompensé et notre service FortiSandbox Cloud au sein d'une offre unique. FortGuard assure une défense solide contre les attaques sophistiquées, grâce à une protection contre les menaces connues et inconnues.

Détection et réponse
FortiEDR assure une protection en temps réel contre les menaces, avant et après infection. Cet outil détecte et désamorce les menaces potentielles pour stopper les intrusions informatiques et bloquer les attaques ransomware avant qu'elles ne causent des dommages. FortiEDR automatise également les procédures de réponse et de réparation grâce à des playbooks personnalisables.

Réseau de vers

Mouvement latéral - Segmentation basée sur les objectifs
La segmentation Fortinet basée sur les intentions assure une protection réseau de bout en bout. Elle segmente intelligemment les actifs réseau et l'infrastructure, en installation locale ou cloud. Des fonctionnalités d'analyse et d'automatisation assurent une détection et une neutralisation rapides des menaces.

Détection et réponse
FortiEDR assure une protection en temps réel contre les menaces, avant et après infection. Cet outil détecte et désamorce les menaces potentielles pour stopper les intrusions informatiques et bloquer les attaques ransomware avant qu'elles ne causent des dommages. FortiEDR automatise également les procédures de réponse et de réparation grâce à des playbooks personnalisables.

Command & Control et chiffrement

Détection et réponse
FortiEDR assure une protection en temps réel contre les menaces, avant et après infection. Cet outil détecte et désamorce les menaces potentielles pour stopper les intrusions informatiques et bloquer les attaques ransomware avant qu'elles ne causent des dommages. FortiEDR automatise également les procédures de réponse et de réparation grâce à des playbooks personnalisables.

Mouvement latéral

Mouvement latéral - Segmentation basée sur les objectifs
La segmentation Fortinet basée sur les intentions assure une protection réseau de bout en bout. Elle segmente intelligemment les actifs réseau et l'infrastructure, en installation locale ou cloud. Des fonctionnalités d'analyse et d'automatisation assurent une détection et une neutralisation rapides des menaces.

Programme d'évaluation des cybermenaces

Les architectes de réseaux sécurisés doivent travailler sans relâche pour garder le cap face aux menaces persistantes avancées les plus récentes. Il existe deux manière de déterminer si la solution de vos clients est défaillante : attendre qu'une intrusion informatique se produise... ou bien effectuer des tests de validation. Notre Cyber Threat Assessment Program (CTAP) est conçu pour vous aider à donner aux entreprises une visibilité accrue sur l'état actuel de leur réseau. Lors d'une création ou d'un renouvellement de contrat, vous pourrez ainsi mieux les convaincre.

Dans le cadre du CTAP, un FortiGate est déployé pour surveiller le réseau d'un prospect durant une courte période. Cette opération de monitoring permet de générer un rapport dressant l'inventaire des risques encourus par le réseau. En vous appuyant sur ce document, vous pouvez proposer à l'entreprise une stratégie pour l'avenir. Vous obtiendrez ainsi rapidement l'adhésion des décideurs techniques et commerciaux de l'entreprise.

QuandutiliserleCTAP?

Vous pouvez recourir au CTAP à quatre moments-clés :

1. **Pré-vente**
   Utilisez cette évaluation comme un outil de prévente pour susciter l'intérêt du client et entamer le dialogue
2. **Compétitivité**
   Utilisez le CTAP pour montrer les points faibles du concurrent auquel le prospect fait actuellement appel
3. **Renouvellements**
   Menez une évaluation pour justifier le besoin de fonctionnalités supplémentaires ou de services FortiGuard
4. **Développements**
   Réalisez des ventes croisées avec d'autres solutions de Security Fabric<

Rapide et facile : *moins de 7 jours de surveillance sans interruption de l'infrastructure*

Complet et sans frais : *sécurité, productivité et performances*

L'évaluation des cybermenaces Fortinet peut vous aider à mieux évaluer :

Les risques —Pour identifier les vulnérabilités logicielles utilisées pour attaquer le réseau, les logiciels malveillants/botnets, les attaques de phishing parvenant à percer les défenses et les appareils « à risque » face aux intrusions informatiques.

La productivité—Déterminer quelles applications (peer-to-peer, réseaux sociaux, messagerie instantanée et autres) sont exécutées pour obtenir une visibilité accrue sur ces dernières et identifier les spams, les newsletters et les contenus pour adultes potentiellement indésirables.

L'utilisation et les performances —Identifier les besoins (débit, sessions, bande passante) du réseau, du système de messagerie et des applications critiques, notamment en périodes de pic.

Ressources partenaires

Portail partenaires Fortinet

Page d'accueil des partenariats Fortinet : liens rapides (listes de tarifs, assistance, CTAP et enregistrement des transactions)

https://partnerportal.fortinet.com

Portails revendeurs PME Fortinet

Présentation de notre offre PME, pour la promotion et la vente.

https://partnerportal.fortinet.com/English/NAReseller/smb_reseller/home.aspx

Informations sur les formations Fortinet

Accès rapide aux formations *NSE*, *Fast Tracks* et *How to Grow Your Business*.

https://partnerportal.fortinet.com/prm/English/c/overview

Programme d'engagement des partenaires Fortinet

Plateforme performante et flexible pour une sécurité rentable et différenciée. Elle mobilise les meilleures solutions du secteur pour assurer la réussite de vos clients.

https://partnerportal.fortinet.com/prm/English/c/engage-home

Ce guide de vente a été conçu pour informer nos partenaires, afin qu'ils puissent optimiser leurs ventes de nos solutions réseau. Ce document n'est pas destiné aux clients.

v8.0 03.17.20