LIVRE BLANC

Fortinet Security Fabric : favorise la transformation digitale

Globale, intégrée et automatisée

Résumé

Les entreprises misent sur la transformation digitale pour accélérer leurs activités, réduire les coûts, améliorer leur efficacité et offrir une meilleure expérience à leurs clients. Elles mènent plusieurs initiatives en ce sens : migration des applications et flux de travail vers le cloud, déploiement de périphériques connectés (IoT) et extension de la couverture du réseau de l'entreprise à de nouvelles succursales.

Ces évolutions s'accompagnent de risques en matière de sécurité. Les infrastructures se complexifient et les surfaces d'attaque augmentent. Les organisations font face à des cybermenaces avancées et doivent respecter un cadre réglementaire de plus en plus strict. Pour atteindre les résultats souhaités en matière d'innovation numérique tout en réduisant les risques et les complexifications, les entreprises doivent adopter une plateforme de cybersécurité capable de leur offrir une visibilité accrue sur l'ensemble de leur environnement. Elles doivent également pouvoir gérer facilement la sécurité et les opérations réseau.

Fortinet Security Fabric répond à ces nouveaux impératifs avec des solutions étendues, intégrées et automatisées, pour un réseau sécurisé, un accès zero-trust, une protection cloud dynamique et des opérations reposant sur l'intelligence artificielle. Les offres de Fortinet sont complétées par un écosystème de produits tiers parfaitement intégrés : les entreprises peuvent ainsi consolider leur architecture réseau tout en maximisant leur retour sur investissement (RSI) en sécurité.

84% des responsables en cybersécurité estiment que le risque d'attaques va augmenter[1]

77% des professionnels de la sécurité déclarent que leur organisation a transféré des applications ou des infrastructures vers le cloud, malgré les problèmes de sécurité connus.[3]

L'innovation numérique transforme tous les secteurs

Dans tous les secteurs, la transformation digitale est devenue un élément-clé de la croissance des entreprises et de l'amélioration de l'expérience-client. Les responsables informatiques sont nombreux à l'avoir compris : 61% d'entre eux déclarent avoir déjà lancé des opérations d'envergure ciblant le cloud, les objets connectées ou les appareils mobiles.[2]

La transformation digitale implique plusieurs changements au niveau des environnements réseau. Les utilisateurs sont de plus en plus mobiles. Ils accèdent au réseau depuis plusieurs appareils et se connectent directement aux clouds publics pour utiliser des applications professionnelles-clés, comme Office 365. Ils échappent ainsi à l'œil attentif des services informatiques de l'entreprise.

Les objets connectés IoT sont désormais plus nombreux que les appareils classiques. Largement distribués, ils se trouvent souvent dans des lieux éloignés et non-surveillés. Les fournisseurs de services cloud, de leur côté, peuvent couvrir de nombreuses succursales éloignées : ces dernières se connectent directement aux services cloud en contournant les datacenters des entreprises. Tous ces changements rendent obsolète le concept de périmètre réseau défendable. Il devient nécessaire d'adopter une nouvelle stratégie de défense multicouche en profondeur.

Migration des applications et des charges de travail vers le cloud

Presque toutes les entreprises ont commencé à transférer certaines charges de travail et applications vers le cloud. Tout au moins, elles prévoient de le faire. Ces décisions sont souvent motivées par la volonté de réduire les coûts et d'améliorer l'efficacité opérationnelle et l'évolutivité, grâce à la flexibilité offerte par le cloud.

Les fournisseurs de services cloud offrent un large éventail de modèles de déploiements possibles. Les entreprises peuvent profiter des avantages du Software-as-a-Service (SaaS) et des services de type Salesforce ou Box. Les applications conçues et déployées en environnements on-site peuvent quant à elles migrer vers des déploiements Infrastructure-as-a-Service (IaaS) ou Platform-as-a-Service (PaaS) tels qu'Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, Oracle Cloud Infrastructure et IBM Cloud.

Les entreprises se méfient des verrous propriétaires des fournisseurs de services cloud. Elles veillent à déployer chaque application et chaque charge de travail sur le cloud qui lui est le plus adapté. Elles optent ainsi pour des infrastructures multi-clouds, ce qui les contraint à cerner les spécificités propres à chaque environnement cloud. Ce type d'approche obscurcit par ailleurs la visibilité et nécessite l'utilisation de plusieurs consoles pour la gestion des politiques, l'établissement de rapports, etc.

Des appareils nombreux, dans de multiples environnements

Les endpoints constituent sans doute les nœuds les plus vulnérables des réseaux de services cloud. Des milliers d'employés utilisent de multiples appareils (professionnels ou personnels) pour accéder aux ressources du réseau. Garantir la cyberhygiène et la sécurité de ces endpoints tient du défi. Plus redoutable encore : la prolifération des périphériques connectés IoT. Fin 2019, le nombre d'objets connectés IoT actifs dépassait 26,66 milliards. En 2020, les experts estiment que ce nombre atteindra 31 milliards.[5]

Ces équipements connectés sont utilisés dans de nombreux contextes commerciaux. Dans les secteur de la distribution et de l'hôtellerie, ils offrent des expériences personnalisées aux clients. En fabrication et en logistique, ils permettent de suivre les stocks. Dans les usines ou les centrales électriques, ils assurent le monitoring des machines.

Souvent robustes et économes en énergie, ces appareils mettent l'accent sur les performances, souvent au détriment de la sécurité et des protocoles de communication sécurisés. Contrairement à la plupart des endpoints connectés au réseau, ces équipements connectés à internet sont généralement déployés dans des lieux éloignés ou dans des installations comptant pas ou peu de personnel (comme les centrales électriques). Depuis ces lieux peu sécurisés, ils transmettent des données critiques et sensibles à des datacenters sur site et à des services cloud.

Une présence accrue dans les zones géographiques et les marchés dispersés

À mesure que les entreprises étendent leur couverture mondiale (nouvelles installations, nouvelles succursales, emplacements satellites), elles sont confrontées à des besoins inédits en termes de débit. Bien que les applications SaaS, la vidéo et la VoIP stimulent la productivité, elles contribuent à une croissance exponentielle du volume de trafic WAN.

Le MPLS, de par sa fiabilité, représente depuis de nombreuses années le premier choix en matière de connectivité WAN. Toutefois, avec ce protocole, il est difficile d'optimiser l'utilisation de la bande passante WAN et de faire varier les niveaux de qualité de service en fonction des besoins propres à chaque application. Le développement de succursales et l'amélioration des services peuvent rapidement entraîner une explosion des coûts WAN.

Fortes de ce constat, les organisations se tournent vers le SD-WAN, qui exploite efficacement le MPLS, les connexions internet et même les liaisons de télécommunications. Le SD-WAN possède un autre atout : il achemine de manière dynamique chaque type de trafic sur la liaison la plus adaptée.

Les quatre grands défis

L'impact de ces transformations digitales sur la sécurité des réseaux est souvent négligé ou minimisé. Près de 80 % des organisations introduisent des transformations digitales plus rapidement qu'elles ne peuvent les protéger contre les cybermenaces[9]. Sur la route de l'innovation numérique, les responsables informatiques sont confrontés à quatre grands défis en matière d'architectures sécurisées :

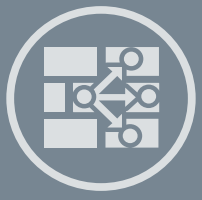
- Une surface d'attaque plus vaste

Les données sensibles peuvent potentiellement résider n'importe où et peuvent désormais voyager sur de nombreuses connexions, hors du contrôle de l'entreprise.

Les environnements cloud sont dynamiques : 74 % des entreprises ont transféré une application vers le cloud avant, finalement, de la rapatrier sur site[4]

84% des entreprises ont une stratégie multi-cloud. 81 % des entreprises considèrent la sécurité comme l'un des principaux défis du cloud.[6]

Entre 2017 et 2019, le nombre d'organisations victimes de violations de données imputables à des applications ou des équipements connectés (IoT) non-sécurisés a augmenté de 73 %.[7]



Le SD-WAN offre de meilleures performances et une meilleure sécurité, avec un coût inférieur à celui du MPLS.[8]

Sur le cloud, les applications sont exposées à internet. Chaque nouvelle instance cloud, chaque nouvel équipement connecté élargit la surface d'attaque de l'entreprise. Or, dans les parties reculées de la surface d'attaque, les intrusions peuvent passer inaperçues pendant des semaines, voire des mois, avant de faire des ravages sur le reste de l'entreprise. Les appareils mobiles personnels ajoutent à l'imprévisibilité : les utilisateurs se déplacent dans les entreprises, dans l'espace public et même au-delà des frontières. Résultat : la migration cloud, les plateformes mobiles et les équipements connectés augmentent le coût des violations de données, les portant jusqu'à plusieurs centaines de milliers de dollars.[10]

Cette surface d'attaque étendue et dynamique dissout un réseau autrefois bien défini. Il devient beaucoup plus facile pour les pirates informatiques de s'infiltrer. Une fois sur le réseau, ils ne trouvent souvent que peu d'obstacles et peuvent alors se déplacer librement vers leurs cibles sans être détectés. Dans les entreprises innovantes, la sécurité doit être assurée à plusieurs niveaux, avec des contrôles sur chaque segment de réseau. Il est nécessaire de partir du principe suivant : tôt ou tard, le périmètre sera franchi. L'accès aux ressources réseau doit être octroyé selon le principe du moindre privilège, sur la base de vérifications continues.

- **Les cybermenaces avancées**

Les cybermenaces se diversifient rapidement. Les pirates informatiques tentent de contourner et de déjouer les cyberdéfenses traditionnelles. Jusqu'à 40 % des logiciels malveillants détectés chaque jour sont 0-day ou précédemment inconnus.[15]

L'augmentation du nombre de malwares 0-day est liée à la multiplication des malwares polymorphes et à la disponibilité de trousses à outils (toolkits) de piratage. Cette tendance rend les algorithmes traditionnels de détection basés sur les signatures moins efficaces. Les hackers continuent par ailleurs à recourir à l'ingénierie sociale pour déjouer les méthodes statiques des approches de cybersécurité traditionnelles. Des études révèlent que l'an dernier, 85 % des organisations ont subi des attaques de phishing ou d'ingénierie sociale.[16]

Les cybermenaces deviennent de plus en plus sophistiquées et les incidents et violations de données sont plus difficiles à détecter et à neutraliser. Entre 2018 et 2019, le temps nécessaire pour identifier et contenir une violation de données est passé de 266 à 279 jours.[17] Les organisations doivent désormais identifier plus rapidement les attaques réussies. Le risque d'attaques est généralisé : plus de 88 % des entreprises déclarent avoir connu au moins un incident au cours de l'année écoulée.[18] La cyber-résistance est devenue essentielle.

- **Une plus grande complexité**

Selon près de la moitié des responsables informatiques, le plus grand défi des surfaces d'attaque en expansion concerne la complexité croissante des infrastructures de sécurité.[19] De nombreuses organisations s'appuient en effet sur un ensemble de produits indépendants et non-intégrés. Les grandes entreprises utilisent en moyenne plus de 75 solutions de sécurité distincte.[20]

Ce manque d'intégration empêche les entreprises de s'appuyer sur une sécurité automatisée. 30 % des responsables informatiques considèrent que le nombre trop important de tâches manuelles constitue un problème de sécurité majeur pour leur entreprise.[21] Sans automatisation de la sécurité, les directeurs informatiques ont besoin de professionnels en cybersécurité plus qualifiés pour surveiller et sécuriser leur réseau.

Parallèlement, les entreprises peinent à recruter les experts dont elles ont besoin. Plus de 4 millions de postes de cybersécurité sont actuellement vacants, et leur nombre ne cesse d'augmenter.[22] 67 % des directeurs informatiques estiment que cette pénurie d'experts empêche leur entreprise de garder le cap en matière de sécurité.[23]

Les pirates informatiques l'ont bien compris et ils cherchent à en tirer avantage.

61 % des responsables en cyber sécurité déclarent qu'ils ont déjà lancé d'importantes opérations concernant le cloud, les équipements connectés ou les appareils mobiles.[11]

Jusqu'à 40 % des nouveaux logiciels malveillants détectés chaque jour sont 0-day ou précédemment inconnus.[12]

Lorsqu'elles mènent des initiatives d'innovation numérique, les équipes de sécurité doivent déployer des protections pour 17 types de endpoints différents.[13]

L'an dernier, un tiers des entreprises a subi une violation de données critique susceptible d'entraîner des sanctions réglementaires.[14]

- **Des exigences réglementaires renforcées**

Le règlement général sur la protection des données (RGPD) de l'Union européenne (UE) et la loi californienne sur la protection de la vie privée des consommateurs (CCPA) figurent parmi les règlements les plus connus en matière de protection des données. Mais il y en a bien d'autres. Chaque État américain dispose d'une loi sur la notification des violations de données. Ces lois prévoient des mesures supplémentaires de protection de la vie privée des consommateurs. Face à la pression politique et sociale, ces réglementations devraient être renforcées dans les années à venir, et les sanctions en cas de manquement devraient se multiplier.

Les organisations doivent également se conformer aux normes industrielles, souvent difficiles à respecter. En effet, moins de 37 % des organisations passent avec succès leur audit PCI DSS.[24] À une heure où la norme PCI DSS est supplantée par la norme PCI Software Security Framework (PCI SSF), il est probable que les entreprises se retrouvent face à des difficultés réglementaires plus importantes encore.

Fortinet Security Fabric
- Global
- Automatisé
- Intégré

FORTINET
Fabric-Ready

Les impératifs de conformité réglementaire ont des répercussions importantes sur les objectifs de modernisation de la sécurité. Sur les 71 % d'organisations qui ont rapatrié leurs applications cloud vers leurs centres de données sur site, 21 % ont pris cette mesure pour assurer leur conformité réglementaire.[25]

Fortinet Security Fabric

Fortinet Security Fabric a été conçu pour répondre à l'ensemble de ces défis de sécurité : cette solution intégrée offre une visibilité accrue et un contrôle optimal sur toute la surface d'attaque, pour minimiser les risques. Elle permet d'éviter les problèmes de complexification liés au déploiement de produits en silos et fournit des flux de travail automatisés pour des opérations plus rapides.

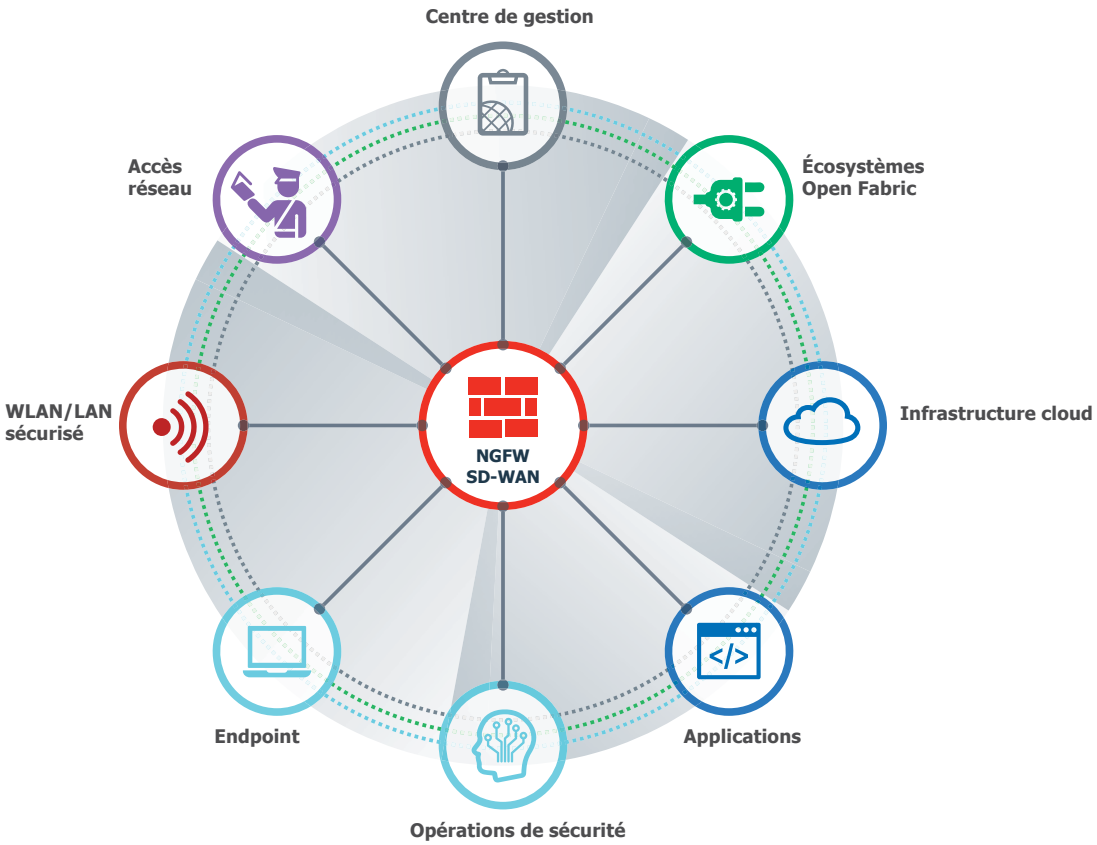


Figure 1 : Fortinet Security Fabric permet à plusieurs technologies de sécurité de fonctionner ensemble de manière intégrée, dans tous les environnements. Elle se base sur une source unique de renseignements sur les menaces et fonctionne via une seule et unique console. Ce fonctionnement intégré permet de combler les failles de sécurité réseau et de réagir plus rapidement en cas d'attaque ou d'intrusion informatique.

Une large visibilité sur la surface d'attaque

Les transformations liées à l'innovation numérique engendrent une expansion des périmètres organisationnels. Fortinet Security Fabric relève le défi en fournissant aux entreprises une sécurité et une visibilité complète sur leur infrastructure. Fortinet Security Fabric protège, en toute flexibilité, chaque segment du réseau, en s'appuyant sur la plus large gamme de solutions réseau du secteur. Elle apporte sécurité et hautes performances aux datacenters, aux succursales, aux petites entreprises et à tous les principaux fournisseurs cloud.

Tous les composants sont configurés, gérés et surveillés depuis un unique système de gestion centralisé. Cette interface unique élimine les silos associés aux infrastructures composées de produits isolés. Elle permet aussi de minimiser la nécessité de formation pour un personnel souvent restreint. Le système de gestion facilite le déploiement Zero-Touch des composants à distance, pour réduire les coûts d'exploitation.

Tous les composants sont pilotés par le même système d'exploitation réseau FortiOS. Fortinet Security Fabric permet donc une gestion des politiques cohérente et une communication fluide, en temps réel, au sein de l'infrastructure de sécurité. Résultat : des délais moindres pour la détection et la neutralisation des menaces, une réduction des risques de sécurité liés aux erreurs de configuration et erreurs de compilation manuelle des données, et de meilleurs résultats aux audits de conformité.

En plus d'intégrer les produits et solutions Fortinet, Security Fabric propose des API préconçues pour plus de 70 partenaires Fabric-Ready, pour une interopérabilité parfaite avec tous les composants Security Fabric.

Pour les produits de sécurité ne faisant pas partie de l'écosystème des partenaires Fabric-Ready, les API REST (Representational State Transfer) et les scripts DevOps (Development Operations) permettent aux clients de réaliser des intégrations faciles et rapides.

Opérations, orchestration et réponses automatisées

La structure Fortinet Security Fabric recourt au machine learning pour suivre l'évolution rapide des cybermenaces. Elle comporte des fonctionnalités avancées d'orchestration, d'automatisation et de réponse pour la sécurité (SOAR). Elle assure également la détection proactive, la corrélation, les alertes de partage de renseignements ainsi que la recherche et l'analyse des menaces.

Et pour permettre aux entreprises de gagner en réactivité face aux cyberincidents, Fortinet Security Fabric assure l'agrégation automatisée des logs, la corrélation des données et la génération de rapports à l'aide de modèles intégrés. Ces fonctionnalités permettent de décharger le personnel de sécurité des tâches de collecte de données et de production de rapports (conformité, hiérarchie). au profit de missions plus proactives.

Près de la moitié des décisionnaires informatiques indiquent que l'intégration de la sécurité et l'amélioration de l'analyse constituent des priorités majeures quant à leur stratégie de cybersécurité.[26]

Les NGFW de FortiGate offrent le meilleur rapport prix/performances dans les évaluations indépendantes. Ils analysent le trafic chiffré et atteignent des performances SSL de 5,7 Gb/s tout en bloquant 100 % des évasions.[27]

La réduction du temps de détection et de réponse peut permettre une réduction de 25 % des coûts généraux engendrés par une violation de données. [28]

Solutions Security Fabric

Fortinet Security Fabric apporte des solutions dans cinq domaines clés : l'accès Zero-Trust, la mise en réseau sécurisée, la sécurité cloud dynamique, les opérations de sécurité axées sur l'intelligence artificielle et l'interopérabilité des écosystèmes. Dans chacun de ces domaines, Fortinet Security Fabric propose les meilleures solutions, comme en attestent les laboratoires indépendants comme NSS Labs et les analystes de premier plan, comme Gartner.[29,30]

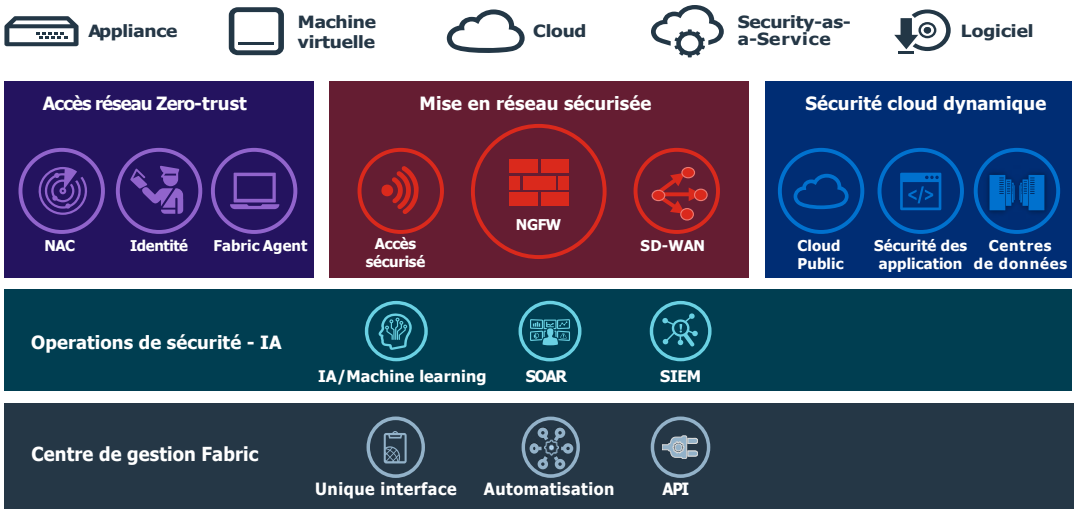


Figure 2 : Cadre conceptuel de Fortinet Security Fabric.

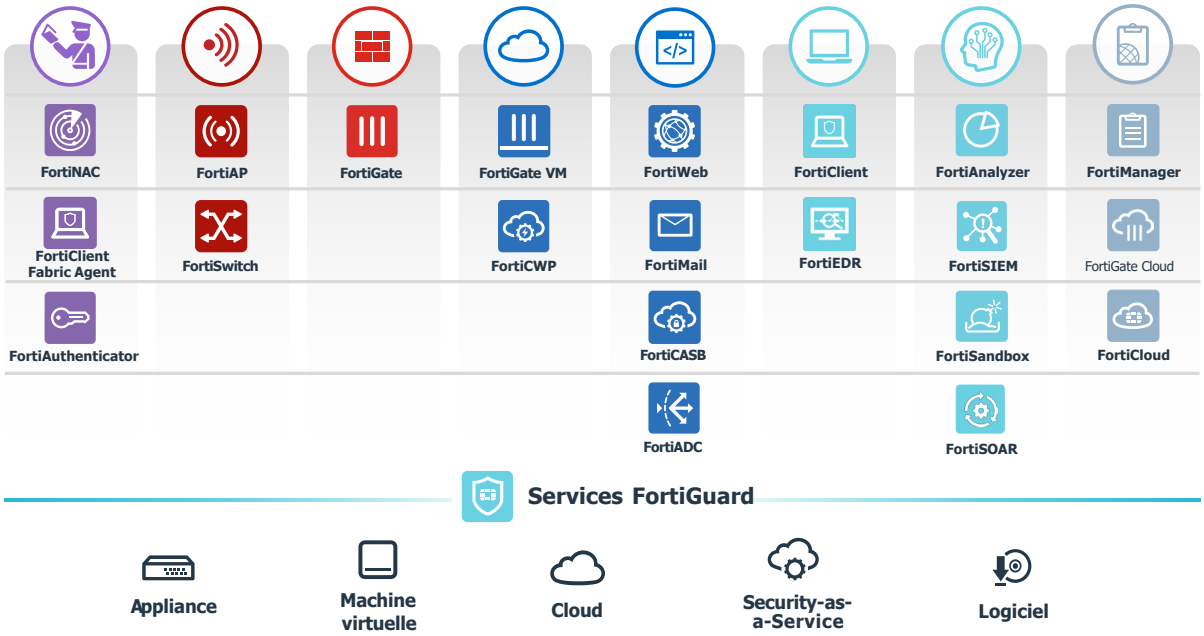


Figure 3 : Principales offres de la solution Security Fabric

Accès au réseau Zero-trust

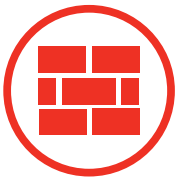
Les cybermenaces devenant de plus en plus sophistiquées, un modèle de sécurité fondé sur le périmètre ne suffit plus. En procédant au vol d'identifiants et en lançant des logiciels malveillants, les pirates informatiques peuvent accéder au réseau de l'entreprise. Fortinet Security Fabric permet d'appliquer une politique d'accès Zero-Trust sur l'ensemble du réseau étendu.

Les solutions de contrôle d'accès au réseau (NAC) **FortiNAC** permettent de détecter automatiquement les dispositifs se connectant au WAN de l'entreprise. Ces appareils sont ensuite soumis à une analyse de sécurité. L'équipe de sécurité peut définir des politiques spécifiques à appliquer. Une fois qu'un appareil a été autorisé à accéder au réseau, il est surveillé en permanence pour détecter toute anomalie comportementale pouvant indiquer une infection ou une utilisation par un individu malveillant.

Après avoir identifié les appareils connectés à leur réseau, les entreprises peuvent appliquer un accès Zero-Trust afin de déterminer qui utilise ces appareils. Le serveur de gestion des identités utilisateurs FortiAuthenticator offre une authentification intégrée et un contrôle d'accès basé sur les profils, selon le principe du « moindre privilège ». Les tokens à deux facteurs FortiToken renforcent les mécanismes d'identification : ils empêchent les pirates utilisant des identifiants volés d'accéder à un compte utilisateur.

Une fois les appareils connectés au réseau, ils peuvent être monitorés et les politiques de sécurité de l'entreprise peuvent leur être appliquées. Les appareils mobiles, quant à eux, sont de plus en plus nombreux en entreprise. Ils sont susceptibles d'être utilisés hors ligne ou sur d'autres réseaux. L'installation de l'agent **FortiClient** permet d'avoir une visibilité sur ces appareils et d'appliquer un contrôle d'accès dynamique, à la fois sur le réseau interne et hors réseau.

Mise en réseau axée sur la sécurité



À mesure que des initiatives numériques sont lancées, les réseaux d'entreprise et les surfaces d'attaque se développent. Les besoins en sécurité réseau augmentent. Il est essentiel d'assurer une intégration étroite entre l'infrastructure réseau et l'architecture de sécurité, de manière à ce que le réseau puisse être étendu ou modifié sans que sa sécurité ne soit compromise. Cette intégration passe par davantage d'interopérabilité, et donc par la réduction du nombre de produits de sécurité isolés au profit de solutions unifiées.

Chez Fortinet, la mise en réseau axée sur la sécurité repose notamment sur les **FortiGate** nouvelle génération (NGFW), qui constituent la première ligne de défense contre les menaces avancées. Près d'un tiers des violations de données impliquent des attaques de phishing[31]. Ces attaques reposent sur des liens ou des pièces jointes malveillantes pour infecter les endpoints ou voler des identifiants utilisateurs. Les NGFW de FortiGate comprennent une passerelle web sécurisée (SWG) qui identifie et bloque les tentatives de connexion à des URL malveillantes ou suspectes.

Les NGFW FortiGate effectuent également le déchiffrement et l'inspection SSL et TLS. Cette fonctionnalité est devenue essentielle : environ 75 % du trafic réseau des entreprises est protégé par les protocoles SSL/TLS, et environ 82 % du trafic malveillant utilise le chiffrement.[32,33] Les **FortiGate NGFW** utilisent des processeurs de sécurité (SPU) spécialement conçus pour minimiser l'impact de l'inspection du trafic SSL/TLS sur les performances. L'intégration de l'inspection du trafic chiffré à hautes performances via le NGFW évite aux entreprises d'acquérir et de déployer des appareils autonomes pour mener à bien ce travail.

Lorsque les cybermenaces ont réussi à percer le périmètre réseau, il est essentiel de les empêcher d'opérer des déplacements latéraux. Il est possible d'y parvenir aisément en opérant une segmentation en fonction des besoins. Les connexions internes suspectes ou malveillantes sont bloquées par défaut. Et si une menace de type 0-day est identifiée après l'infection, des données sur la menace en question sont communiquées via Security Fabric pour garantir qu'aucune infection secondaire ne se produise.

Les organisations doivent intégrer la sécurité à l'ensemble de leur réseau, y compris au niveau des succursales. **Fortinet Secure SD-WAN** offre des performances réseau optimisées et une intégration pour les succursales. Les NGFW FortiGate intégrés dans les appliances SD-WAN effectuent une inspection du trafic dans chaque bureau distant. Ce fonctionnement permet d'établir une connexion directe à internet pour les applications et services SaaS, tout en réduisant les coûts du WAN et en optimisant les performances.

En succursale, Fortinet Secure SD-Branch permet d'étendre la visibilité et la gestion centralisée de la sécurité jusqu'à la couche de commutation. Fortinet Secure SD-Branch repose sur des solutions FortiNAC, sur des commutateurs d'accès sécurisés FortiSwitch et sur des points d'accès sans fil FortiAP surveillés et contrôlés via les NGFW FortiGate. En intégrant la sécurité aux réseaux WAN, les entreprises simplifient leurs opérations en éliminant les redondances et permettent une réponse rapide et coordonnée face aux menaces avancées.

Sécurité dynamique cloud

Pour les entreprises, il devient essentiel d'étendre le déploiement de la sécurité aux ressources cloud. Fortinet Security Fabric intègre une gamme de solutions cloud natives pour sécuriser toutes les applications et tous les environnements. Les solutions de sécurité Fortinet assurent sécurité, visibilité et contrôle sur les déploiements clouds publics et privés. Les NGFW FortiGate sont disponibles en machine virtuelle. Ils peuvent ainsi fournir une sécurité cloud native automatisée, une connectivité VPN, une segmentation du réseau, une prévention des intrusions et une SWG.

Les entreprises doivent également s'assurer que leurs déploiements cloud sont correctement configurés. Les mauvaises configurations de sécurité constituent un problème majeur du cloud public : 99 % d'entre elles ne sont pas signalées.[34] Les analyses de sécurité cloud **FortiCWP** offrent visibilité et contrôle sur l'infrastructure cloud public. Elles permettent le monitoring des configurations, la protection des données, la mise en conformité et la gestion intégrée des menaces.

Une fois l'infrastructure cloud sécurisée, il faut protéger les applications qui y sont exécutées. Les déploiements cloud publics sont généralement destinés à l'hébergement des applications web et des API web. **FortiWeb** leur fournit une sécurité cloud native. Les firewalls d'applications web (WAF) de FortiWeb protègent les applications web contre les menaces connues et inconnues en recourant à la fois aux détections de signatures, au machine learning et à l'intelligence artificielle.

La plupart des applications web utilisent des API pour se connecter à des services web et s'intégrer à d'autres outils. Il est donc essentiel de sécuriser ces API web en utilisant la validation de schéma et la sécurité OpenAPI pour assurer une protection contre les activités potentiellement malveillantes des bots (scraping, analyses).

Les entreprises se tournent également de plus en plus vers des solutions de messagerie cloud, comme Google G Suite et Microsoft Office 365. Les attaques de phishing étant l'une des principales causes de cyberincidents et de violations de données, il est essentiel de sécuriser ces services. Disponibles en appliance physique, en applicance virtuelle ou en service hébergé, les solutions **FortiMail** protègent les déploiements de messagerie en installation locale ou cloud. Elles bloquent les cybermenaces traditionnelles et avancées ciblant les messageries et offrent des fonctionnalités de sauvegarde pour éviter la perte d'informations sensibles.

De nombreuses entreprises recourent également aux applications SaaS telles que Google G Suite, Box, Microsoft Office 365, Dropbox et Salesforce. Les CASB de **FortiCASB** gèrent les risques de mauvaise configuration, fournissent une visibilité et un contrôle centralisés, assurent la sécurité des données en applications SaaS et veillent à ce que les configurations soient conformes aux réglementations applicables.

Le rôle de l'intelligence artificielle

Le volume et la sophistication des attaques malveillantes rendent les solutions de cybersécurité traditionnelles insuffisantes. Les outils de détection des logiciels malveillants basées sur les signatures ne sont capables de détecter que la moitié des attaques de malware.[35] Le recours à l'intelligence artificielle et au machine learning est devenu essentiel pour détecter et prévenir ces attaques.

FortiGuardAI permet aux entreprises de garder une longueur d'avance sur les cybercriminels. Les laboratoires FortiGuard recueillent des données sur les menaces à partir de millions de capteurs répartis dans le monde entier et via des partenariats établis avec plus de 200 organisations mondiales. En s'appuyant sur plus de 5 milliards de nœuds, FortiGuard AI identifie des caractéristiques uniques, pour détecter les menaces connues et inconnues. Les volumes traités par les laboratoires FortiGuard sont considérables : notre équipe traite plus de 100 milliards de requêtes web chaque jour et bloque, chaque seconde, plus de 3 600 requêtes d'URL malveillantes.

Face à des menaces de plus en plus sophistiquées, une prévention à 100 % n'est plus possible. Les mécanismes avancées de détection sont devenus essentiels pour aider les entreprises à éviter les violations. L'intelligence artificielle et le machine learning intégrés à **FortiDeceptor**, **FortiSandbox** et **FortiInsight** aident les organisations à identifier la présence de logiciels malveillants inconnus et de hackers, pour finalement les neutraliser.

Pour contenir et éliminer les menaces plus rapidement, les entreprises doivent s'appuyer sur l'automatisation stratégique. **FortiSIEM** et **FortiAnalyzer** permettent d'obtenir une visibilité globale sur l'infrastructure réseau et mènent des analyses de sécurité basées sur l'intelligence artificielle. À partir des données collectées, les analystes peuvent déterminer la nature et la gravité des menaces, avec l'aide de **FortiAI**, notre analyste virtuel. **FortiSOAR** propose ensuite des fonctionnalités d'orchestration et d'automatisation pour remédier aux intrusions. Les centres d'opérations de sécurité (SOC), souvent surchargés, peuvent ainsi se focaliser sur le Threat Hunting et sur d'autres tâches essentielles.

En matière de réponse aux cyberincidents, les endpoints doivent, eux aussi, pouvoir compter sur l'intelligence artificielle. **FortiEDR** Endpoint Detection and Response (EDR) et FortiClient assure une protection avancée des endpoints via l'analyse des vulnérabilités, l'installation de correctifs et la prévention des exploits en environnements en ligne et air-gap. Si un endpoint est infecté, la détection des menaces et la protection post-infection FortiEDR empêchent les malwares de communiquer avec les serveurs command-and-control ou d'opérer des déplacements latéraux. FortiEDR assure une réponse fondée sur le degré de risque et permet des actions automatisées en ligne.

Fortinet Security Fabric

La structure Fortinet Security Fabric a été conçue pour simplifier la gestion de l'architecture de sécurité des entreprises. Elle assure une gestion unifiée et un monitoring centralisé en intégrant des outils de sécurité d'ordinaire proposés séparément.

FortiManager, plateforme de gestion centralisée et **FortiAnalyzer**, outil de journalisation et de reporting centralisé, apportent ensemble visibilité et contrôle sur l'ensemble de l'infrastructure réseau. Ces outils permettent l'analyse et l'automatisation des flux de travail, via une unique console de gestion.

Ces outils s'appuient sur des intégrations API avec les partenaires Fortinet Fabric-Ready. Douze Fabric Connectors permettent une intégration accrue avec des solutions tierces. Des intégrations API sont également disponibles pour plus de 135 partenaires Fabric-Ready. Pour les solutions non-partenaires, Fortinet Security Fabric propose une API REST et des scripts DevOps permettant une intégration simplifiée.

De nombreuses organisations transfèrent leurs opérations vers le cloud. Une solution single-point-of-access et single-sign-on (SSO) est essentielle pour réduire la complexité des déploiements multi-clouds. **FortiCloud** fournit une SSO et des portails à 15 solutions Fortinet SaaS et Metal-as-a-Service (MaaS) ainsi qu'un portail de services baptisé **FortiCare**. Fortinet Security Fabric prend en charge tous les principaux fournisseurs de cloud public, pour simplifier tous les déploiements multi-clouds.

En combinant FortiManager, FortiAnalyzer et FortiCloud, il est possible d'obtenir une intégration complète des déploiements locaux et cloud. Cette intégration permet de simplifier la gestion de la sécurité. En s'appuyant sur les Fabric Connectors et sur les API, les équipes de sécurité peuvent recevoir des informations en temps réel sur l'état du réseau, automatiser la gestion des logs réseau et générer facilement des rapports de conformité, depuis un unique panneau de contrôle.

Gérer les risques, saisir les opportunités

L'innovation numérique donne aux organisations la possibilité d'atteindre des niveaux d'efficacité inédits, de réduire leurs dépenses et d'améliorer l'expérience-client. Cependant, les initiatives de modernisation élargissent et modifient la surface d'attaque. De nouveaux vecteurs d'attaque apparaissent, qui peuvent être exploités par les pirates informatiques.

Pour les entreprises innovantes, il est primordial de reconnaître, d'accepter et de gérer correctement les risques. Fortinet Security Fabric peut constituer le socle d'une telle démarche.

Cette infrastructure fédère les solutions de sécurité au sein d'une seule plateforme. Elle offre une visibilité optimale sur la surface d'attaque, intègre la prévention des intrusions informatiques grâce à l'intelligence artificielle et automatise les opérations, l'orchestration et la réponse. Fortinet Security Fabric permet aux organisations de tirer pleinement parti de l'innovation numérique sans avoir à négliger la sécurité au profit de la flexibilité, de la simplicité ou des performances.

[1] Nick Lansing, « Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources » Forbes et Fortinet, 2019.

[2] « The CIO and Cybersecurity: A Report on Current Priorities and Challenges », Fortinet, 23 mai 2019.

[3] Jeff Wilson, « The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments » IHS Markit, 2019.

[4] Ibid.

[5] Gilad David Maayan, «The IoT Rundown For 2020: Stats, Risks, and Solutions » Security Today, 13 janvier 2020.

[6] « 2019 State of the Cloud Report » Flexera, 2019.

[7] Larry Ponemon, « Third-party IoT risk: companies don't know what they don't know » ponemonsullivanreport.com, consulté le février 2020.

[8] Nirav Shah, « SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019 » Fortinet, 9 septembre 2019.

[9] Kelly Bissell, et al., « The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study » Accenture Security et Ponemon Institute, 2019.

[10] « 2019 Cost of a Data Breach Report » IBM Security et Ponemon Institute, 2019.

[11] « The CIO and Cybersecurity: A Report on Current Priorities and Challenges » Fortinet, 23 mai 2019.

[12] Selon les données internes de FortiGuard Labs.

[13] « 6 Obstacles to Effective Endpoint Security: Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders » Fortinet, September 8, 2019.

[14] Selon les données internes de Fortinet.

[15] Selon les données internes de FortiGuard Labs.

[16] Kelly Bissell, et al.,« The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study » Accenture Security et Ponemon Institute, 2019.

[17] « 2019 Cost of a Data Breach Report » IBM Security et Ponemon Institute, 2019.

[18] Basé sur une recherche interne Fortinet.

[19] « The CIO and Cybersecurity: A Report on Current Priorities and Challenges » Fortinet, 23 mai 2019.

[20] Kacy Zurkus, « Defense in depth: Stop spending, start consolidating » CSO, 14 mai 2016.

[21] « The CIO and Cybersecurity: A Report on Current Priorities and Challenges » Fortinet, 23 mai 2019.

[22] « Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019 » (ISC)², 2019.

[23] « CIO Survey 2019: A Changing Perspective » Harvey Nash et KPMG, 2019.

[24] « 2019 Payment Security Report » Verizon, 2019.

[25] Jeff Wilson, « The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments » IHS Markit, 2019.

[26] « Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources » Forbes et Fortinet, 2019.

[27] « Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests » Fortinet, 14 octobre 2019

[28] « 2019 Cost of a Data Breach Report » IBM Security et Ponemon Institute, 2019.

[29] « Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests » Fortinet, 14 octobre 2019.

[30] « Gartner Magic Quadrant Reports » Fortinet, consulté le 22 janvier 2020.

[31] « 2019 Data Breach Investigations Report » Verizon, 2019.

[32] Alex Samonte, « TLS 1.3: What This Means For You » Fortinet, 15 mars 2019.

[33] Robert Lemos, « Attackers Are Messing with Encryption Traffic to Evade Detection » Dark Reading, 15 mai 2019.

[34] Charlie Osborne, « 99 percent of all misconfigurations in the pu»blic cloud go unreported » ZDNet, 24 septembre 2019.

[35] Robert Lemos, « Only Half of Malware Caught by Signature AV Dark Reading, 11 décembre 2019.

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 dénominations Fortinet mentionnées sont susceptibles d'être également détenues par Fortinet. Toutes les autres marques appartiennent à leurs détenteurs respectifs. Les performances et autres mesures présentées dans ce document ont été évaluées dans un laboratoire interne et dans des conditions optimales. Elles peuvent varier en conditions réelles. Les variations réseau, la diversité des environnements réseau et d'autres éléments sont susceptibles d'affecter ces performances. Fortinet s'exonère de toute garantie sur le contenu de ce document, implicite ou explicite, sauf si cette garantie résulte d'une obligation contractuelle, signée par le Directeur des affaires juridiques de Fortinet, avec un acheteur. Celle-ci doit alors fait mention du fait que le produit respecte les performances et spécifications indiquées sur ce document. Alors, seules les performances et spécifications indiquées dans le cadre de cette obligation contractuelle engagent Fortinet. Toute garantie de ce type sera limitée aux performances dans les mêmes conditions idéales que celles des tests internes du laboratoire Fortinet. Fortinet décline entièrement tout engagement, déclaration et garantie en vertu des présentes, qu'ils soient explicites ou implicites. Fortinet se réserve le droit de changer, modifier, transférer ou réviser de quelque manière que ce soit cette publication sans avis préalable. La version anglaise la plus récente de ce document fait foi, en cas d'erreur de traduction notamment.

13 février 2020 1:29 AM

570099-0-0-EN