PRÉSENTATION DES STRATÉGIES

Principes et stratégies clés pour sécuriser le cloud d'entreprise

Plan de sécurité cloud de Fortinet

Résumé

Les clients se tournent vers le cloud pour réduire leurs dépenses et rester agiles en terme d'innovation numérique. Malgré ses avantages, la migration vers le cloud entraîne une dispersion des données et des informations sensibles des entreprises. Cela augmente la surface d'attaque possible et avec, les risques de sécurité.

Certaines entreprises se heurtent sans le savoir à un nouveau paradigme de sécurité : le modèle de responsabilité partagée, un modèle qui repose sur l'hypothèse que l'infrastructure cloud est sécurisée par les fournisseurs de services cloud, tandis que la sécurité des services utilisés dans le cloud relève de la responsabilité de l'entreprise.

La solution Fortinet Security Fabric a été spécialement conçue pour corriger ces failles de sécurité dans le cloud grâce à une intégration native dans les infrastructures de cloud public, d'un large éventail de services et de produits de sécurité, ainsi que la gestion, l'automatisation et l'analyse de la sécurité dans le cloud.

Les entreprises utilisent en moyenne 61 applications cloud différentes.[1]

Introduction

Fortinet est conscient que l'innovation numérique entraine une croissance sans précédent de l'adoption du cloud. L'hétérogénéité des environnements cloud en résultant étend la surface d'attaque globale. Il devient alors de plus en plus difficile de protéger les applications. Bien que la confiance du public dans le cloud ait considérablement augmenté au cours de la dernière décennie, la sécurité reste l'une des principales préoccupations des entreprises et des leaders technologiques. Il est essentiel que la sécurité fasse partie intégrante du processus de conception, non seulement pour les solutions cloud individuelles, mais aussi pour une évolution stratégique plus large vers des infrastructures multi-cloud dynamiques.

Un ensemble complexe d'approches de sécurité

Les fournisseurs de services cloud se donnent beaucoup de mal pour protéger leurs infrastructures et isoler leurs clients. Cependant, leurs approches de mise en œuvre et de gestion de leurs fonctionnalités de sécurité natives sont variables. Souvent, les fournisseurs de services cloud mettent en œuvre les mêmes fonctionnalités de sécurité, mais utilisent des outils et des approches différents.

Par exemple, Amazon Web Services (AWS) étend les politiques de sécurité en fonction des groupes de sécurité associés aux ressources cloud. Google Cloud Platform (GCP) utilise des règles de pare-feu qui offrent des fonctionnalités équivalentes à celles d'AWS, mais qui sont gérées par des interfaces différentes. Bon nombre de ces différences proviennent de la manière unique dont l'architecture sous-jacente de chaque cloud est structurée et des diverses philosophies qui sont adoptées concernant les opérations dans le cloud.

Pour les clients opérant dans plusieurs clouds, l'état de sécurité par défaut est une architecture hétérogène sans visibilité ni contrôle centralisé, et sans cohérence d'application et de gestion de la sécurité. Dans ce contexte, chaque cloud public et privé, ainsi que les datacenters sur site, deviennent des silos indépendants dans une infrastructure de sécurité fragmentée.

Le modèle de responsabilité partagée dans le cloud

Le modèle de responsabilité partagée en matière de sécurité définit les rôles des fournisseurs et des clients de services cloud dans la sécurisation des applications et des données cloud. Selon ce modèle, le fournisseur de services cloud est responsable de la sécurisation de l'infrastructure et de l'isolement des clients, tandis que le client est responsable de la sécurisation de tous les services et ressources utilisés dans l'environnement cloud. Le fournisseur de services cloud est également responsable de la protection de l'infrastructure sous-jacente contre l'exploitation, l'intrusion et les abus, et doit également assurer l'étanchéité des différents clients.

Il existe différentes versions du modèle de responsabilité partagée en fonction du type de déploiement dont dispose le client. La répartition des responsabilités entre le client et le fournisseur varie selon le type de service cloud offert.

Dans les déploiements SaaS (Software-as-a-Service), le client est limité à un ensemble de contrôles de sécurité de base. Par exemple, il

incombe à Microsoft de sécuriser Office 365, de s'assurer que l'application ne peut être compromise et que les clients peuvent y accéder en toute sécurité. Les clients, quant à eux, sont responsables de la configuration de la plateforme, du suivi des événements de sécurité et des données.

Les déploiements de cloud public, notamment IaaS (Infrastructure-as-a-Service) ou PaaS (Plate-forme-as-a-Service), exigent que le client soit davantage impliqué dans la sécurité, car il met en place de plus grandes infrastructures qui doivent être configurées et gérées de manière sécurisée. Bien que les fournisseurs de services cloud public proposent certains outils de sécurité, il incombe au client de choisir, de configurer et de gérer les solutions de sécurité qui répondent à ses besoins. Dans ce cas, le client est responsable du contrôle et de la configuration de la plateforme, de la visibilité des événements de sécurité, du contrôle d'accès, du chiffrement des données et de la sécurité des applications, éventuellement via une solution WAF (Web Application Firewall). Le client est également responsable de toutes les parties sur site des applications hybrides.

Les clients peuvent s'adresser à un fournisseur de sécurité désigné, tel que Fortinet, pour protéger tout ce qu'ils développent, déploient ou stockent dans le cloud.

Schéma 1. Le modèle de responsabilité partagée montre que le client et le fournisseur de services cloud sont responsables de la sécurisation de différentes ressources.

Les différents éléments d'une sécurité complète

Aujourd'hui, le paysage des menaces en constante évolution exige une approche cohérente et unifiée de la sécurité dans le cloud. Fortinet suit trois grands principes pour concevoir une solution de sécurité multi-cloud efficace :

1. Intégration native
2. Protection étendue
3. Gestion et automatisation

Une solution de sécurité cloud efficace doit être développée en tenant compte de ces trois éléments afin de sécuriser les entreprises cloud dynamiques. Comme démontré ci-dessous, les solutions de sécurité cloud de Fortinet ont été spécifiquement conçues conformément à ces principes.

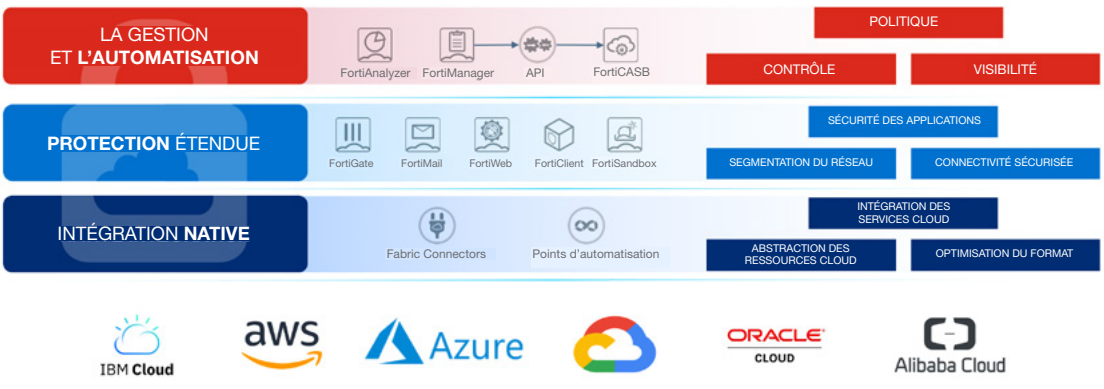

Schéma 2. L'approche de Fortinet en matière de sécurité multi-cloud.

1. Une intégration native

Fortinet se distingue des autres fournisseurs de solutions de sécurité cloud par une large intégration native aux plateformes de cloud public. L'intégration native permet aux solutions d'interagir avec la classification des informations cloud dans le cadre des capacités globales de gestion et d'application des politiques de sécurité. Elle permet également d'exploiter les services cloud natifs pour l'automatisation, le suivi et la surveillance des menaces. Voici quelques-unes des principales fonctionnalités de la solution de sécurité cloud de Fortinet intégrée nativement :

Les Fabric Connectors. Les solutions de sécurité de Fortinet s'intègrent par programme à la plateforme cloud sous-jacente pour fournir une sécurité maximale sans surcharge opérationnelle.

Comme les ressources cloud utilisent généralement des métadonnées et des étiquettes pour indiquer leur fonction logique ou classer des informations, et que les informations relatives aux adresses IP ne sont pas fiables pour prendre des décisions de sécurité, les Fabric Connectors peuvent être utilisés pour normaliser l'utilisation de différents types de métadonnées de ressources dans plusieurs clouds. Ils aident à élaborer et appliquer des politiques de sécurité cohérentes dans les régions et les clouds.

Les implémentations de Fabric Connectors plus avancées apprennent et répertorient l'ensemble des ressources cloud, et les représentent sous la forme d'une topologie réseau. Il est ainsi plus facile pour les équipes de sécurité d'examiner la posture de sécurité du cloud et de mettre en œuvre des politiques de sécurité efficaces.

L'optimisation. Alors que certains fournisseurs se contentent de porter leur système d'exploitation matériel sur une instance virtuelle, les solutions Fortinet sont conçues dès le départ pour un déploiement cloud. Les solutions Fortinet répondent à un large éventail d'exigences en matière de ressources et de performances. Les solutions vont des images à faible encombrement qui maximisent les avantages des architectures à grande échelle, permettant aux équipes de déployer des solutions à faible encombrement là où elles sont nécessaires, aux solutions à encombrement élevé qui exploitent des pilotes réseau haute capacité sur différentes plateformes cloud, comme Azure Accelerated Networking, le mode natif d'Oracle et les instances AWS C5n.

L'automatisation. Fortinet facilite l'automatisation de tâches courantes, telle que la réponse à différents types de menaces, en offrant des points d'automatisation, des modèles d'automatisation et une aide importante à la gestion programmatique via des interfaces de programmation d'applications (API) RESTful. Les points d'automatisation permettent aux entreprises d'automatiser des actions courantes via l'interface utilisateur graphique sans aucune expérience de programmation ou expertise approfondie dans le domaine du cloud. Fortinet fournit une documentation complète sur les API disponibles pour celles qui nécessitent des fonctionnalités d'automatisation plus flexibles et plus puissantes.

La haute disponibilité (HA). Les solutions Fortinet ont été conçues pour être déployées dans différents modes de haute disponibilité. Chaque cloud prend en charge la haute disponibilité en tirant parti de différentes fonctionnalités. La sécurité sous-jacente doit être appliquée de façon cohérente et prévisible dans chaque environnement cloud. Dans ce cas, elle doit prendre en charge différents schémas actifs/actifs ou actifs/passifs, s'intégrant nativement à chaque cloud pour assurer la disponibilité des systèmes essentiels.

L'adaptation automatique. L'un des principaux avantages d'une infrastructure cloud est son élasticité et ses fonctionnalités à la demande, notamment la possibilité d'adapter les services en fonction des différents besoins de l'entreprise, en ne payant que ce qui est utilisé. La prise en charge par Fortinet de l'intégration native aux fonctionnalités d'adaptation automatique du cloud permet à l'infrastructure de sécurité de suivre l'évolution de l'infrastructure cloud en fonction du volume et de la demande, garantissant ainsi la protection continue des applications.

Les modèles de configuration. Les modèles peuvent à la fois réduire les erreurs et permettre d'automatiser des processus clés, tels que l'adaptation automatique des déploiements cloud. Les modèles de configuration Fortinet prennent en charge un éventail d'infrastructures, tels que AWS CloudFormation Templates (CFT), Azure Resource Manager (ARM), HashiCorp Terraform et Ansible, afin d'aider les administrateurs de sécurité à fournir des solutions rapidement et précisément sur différentes plateformes cloud et à répondre aux besoins des déploiements de charges de travail dans le cloud. Les modèles de configuration contribuent à réduire le risque d'erreur humaine tout en accélérant la possibilité d'associer la sécurité à de nouvelles charges de travail et en permettant ainsi aux administrateurs de sécurité de déployer de nouvelles charges de travail en toute confiance.

L'intégration des services. Les plateformes cloud offrent des services de logiciels et de plateformes qui simplifient l'utilisation de différentes fonctionnalités en éliminant la nécessité pour les utilisateurs de maîtriser chaque technologie. Il est essentiel que les solutions de sécurité s'intègrent à chaque plateforme cloud et offrent des fonctionnalités de sécurité dans le cadre du modèle de consommation de services natifs. Ici, l'intégration étend la sécurité à un plus grand nombre de cas d'usage et de services en tant que fonctionnalité fondamentale, offrant une protection de base pour les environnements d'expérimentation ainsi que ceux qui ne font pas encore partie d'une routine plus large de gestion du cycle de sécurité.

2. Une protection étendue

Fortinet offre le portefeuille de sécurité le plus large et le plus complet du secteur, notamment une sécurité réseau et des applications à l'échelle de l'entreprise, ainsi que des produits d'accès sécurisé qui partagent des renseignements et fonctionnent ensemble pour former un tissu coopératif. Fortinet Security Fabric combine un système d'exploitation intuitif, plusieurs couches de détection des menaces et des renseignements sur les menaces, appliqués pour assurer la sécurité, la visibilité et le contrôle.

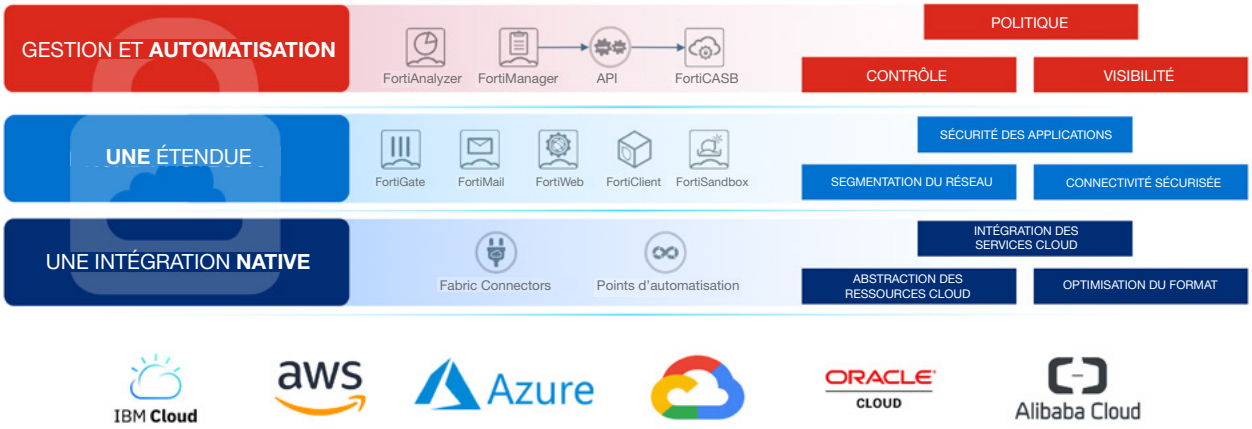

Schéma 3. Les trois piliers de la sécurité multi-cloud.

Les équipes de sécurité peuvent réduire et gérer la surface d'attaque grâce à une visibilité intégrée, empêcher les menaces grâce à une prévention intégrée de la violation des données basée sur un moteur d'intelligence artificielle (IA) et réduire la complexité grâce à des opérations et une orchestration automatisées. Vous découvrirez ci-dessous comment Fortinet offre une protection étendue pour le cloud :

Une protection contre les menaces de type « zero-day ». De nouvelles menaces jusqu'alors inconnues sont découvertes presque chaque jour et affectent les déploiements dans le cloud et sur site. Comme les pirates informatiques utilisent de plus en plus l'intelligence artificielle et la technologie d'apprentissage automatique (machine learning – ML), le nombre de menaces de type « zero-day » est susceptible d'augmenter.

Fortinet fournit un certain nombre de technologies pour identifier et arrêter les menaces de type « zero-day », notamment l'analyse sandbox qui observe les logiciels malveillants potentiels dans un environnement simulé. Le sandbox détermine ensuite s'ils peuvent être exécutés en toute sécurité et examinés à l'aide d'outils comportementaux pour détecter les intentions malveillantes.

Cependant, l'analyse sandbox est gourmande en temps et en ressources processeur, et peut réduire les performances jusqu'à un point de saturation si la majeure partie du trafic n'est pas préfiltrée. Fortinet utilise l'intelligence artificielle et l'apprentissage automatique pour la détection des menaces via l'analyse des caractéristiques, permettant ainsi de repérer de nombreuses menaces avant qu'elles ne soient soumises à l'analyse sandbox. La capacité à déployer des technologies sandbox dans une application IaaS-VM ou SaaS est une fonctionnalité essentielle qui devrait faire partie de toute stratégie de sécurité multi-cloud.

SSL et VPN IPSec. L'extension de la connectivité sécurisée dans les clouds est primordiale. Comme le trafic circule sur Internet et dans les environnements cloud, la capacité à isoler le trafic et à élaborer des politiques de sécurité réseau cohérentes est un facteur clé pour unifier des environnements cloud disparates. La prise en charge des VPN IPsec (IP security) entre les sites et des VPN sur les réseaux cloud virtuels est essentielle pour sécuriser et isoler le trafic de manière cohérente. Les mises en œuvre de VPN doivent être interopérables avec différentes solutions de VPN cloud, offrant ainsi une flexibilité aux différentes entreprises et unités administratives. En outre, la capacité à fournir une connectivité VPN haut débit est cruciale. La solution FortiGate-VM est optimisée pour fournir une connectivité haut débit sécurisée sans ralentir les applications cloud.

Le contrôle applicatif. Application Control est un service FortiGuard qui renforce la sécurité des applications Internet et permet aux entreprises de créer rapidement des politiques pour autoriser, refuser ou restreindre l'accès aux applications. Ce service offre une visibilité et un contrôle de milliers d'applications et permet aux entreprises d'ajouter des applications personnalisées. Les équipes peuvent ajuster précisément les politiques de sécurité en fonction du type d'application et optimiser la bande passante grâce à une gestion du trafic basée sur les applications.

Le Secure SD-WAN. Fortinet a redéfini le marché du SD-WAN en incluant à son meilleur pare-feu de nouvelle génération (NGFW) le SD-WAN, le routage avancé et des fonctionnalités d'optimisation WAN, permettant ainsi une transformation de la périphérie du WAN axée sur la sécurité dans l'offre FortiGate unifiée. Une connexion cloud sécurisée est également essentielle pour garantir des opérations de sécurité transparentes. Fortinet a obtenu la recommandation du NSS Labs lors du test du groupe SD-WAN et offre le meilleur rapport coût total de possession (TCO) par Mbit/s parmi les huit fournisseurs évalués.[2]

Le Zero Trust. Les réseaux conçus avec une confiance implicite simplifient la capacité des données et des applications à se déplacer à l'intérieur du périmètre. Cela contribue aux violations du réseau qui peuvent rester non détectées, permettant à des programmes malveillants internes de voler des données essentielles. Le pare-feu NGFW FortiGate-VM prend en charge la segmentation dynamique qui utilise les attributs logiques des données et des applications sur plusieurs sites et dans le cloud pour assurer un isolement cohérent des ressources avec zéro hypothèse, en validant chaque connexion, quel que soit le VLAN ou le réseau d'origine.

NGFW. Les entreprises développant davantage d'applications essentielles dans le cloud, le besoin de fonctionnalités de sécurité avancées est plus important. Les appliances virtuelles FortiGate qui sécurisent l'entrée et la sortie offrent le même éventail de fonctionnalités de sécurité dans le cloud que sur site. En outre, ces solutions s'intègrent parfaitement aux différentes plateformes cloud et sont optimisées pour offrir des performances élevées dans les infrastructures cloud.

Le WAF (Web Application Firewall). Alors que l'innovation numérique favorise la transition vers les applications essentielles, les nouvelles applications sont de plus en plus basées sur le Web. La solution FortiWeb WAF offre une protection contre les menaces pour les applications Web et les API essentielles. FortiWeb offre des fonctionnalités de prévention des menaces et d'atténuation des bots basées sur l'apprentissage automatique qui permettent d'ajuster précisément les politiques de sécurité Web et d'éliminer les faux positifs. FortiWeb aide les entreprises à répondre aux exigences des politiques de gestion des risques et aux exigences réglementaires relatives à la protection des informations des utilisateurs finaux, et assure la continuité des activités.

La sécurité de la messagerie électronique. Les e-mails restent un vecteur courant de logiciels malveillants, en particulier lorsque les entreprises migrent leurs systèmes de messagerie électronique vers le cloud et s'en servent comme systèmes de sauvegarde. D'ici fin 2022, les comptes de messagerie électronique professionnels dans le cloud devraient représenter 87% de tous les comptes de messagerie électronique professionnels.[3] Les solutions de sécurité de la messagerie électronique de Fortinet offrent une protection complète contre les menaces véhiculées par les e-mails dans le cloud et sur site, et sont idéales pour assurer la migration vers le cloud.

3. La gestion et l'automatisation

L'unification de l'infrastructure de sécurité d'une entreprise facilite non seulement la gestion, mais contribue également à garantir la mise en oeuvre de politiques de sécurité cohérentes, où que les applications soient exécutées, les données stockées ou les infrastructures construites. De plus, elle permet d'automatiser les processus de gestion du cycle de sécurité et de garantir la conformité. Ces fonctionnalités permettent aux entreprises de gérer de façon similaire les infrastructures cloud et sur site en tirant parti du même niveau de visibilité et de contrôle. La gestion centralisée et l'automatisation aident les entreprises à atteindre leurs objectifs de gestion des risques et de conformité réglementaire.

Une gestion et une automatisation efficaces de la sécurité se composent de quatre éléments principaux : la visibilité, le contrôle, la politique et la conformité. Fortinet met en œuvre ces éléments via sa suite de produits de gestion, notamment FortiManager, FortiAnalyzer, FortiCASB et FortiCWP (service de protection des charges de travail dans le cloud).

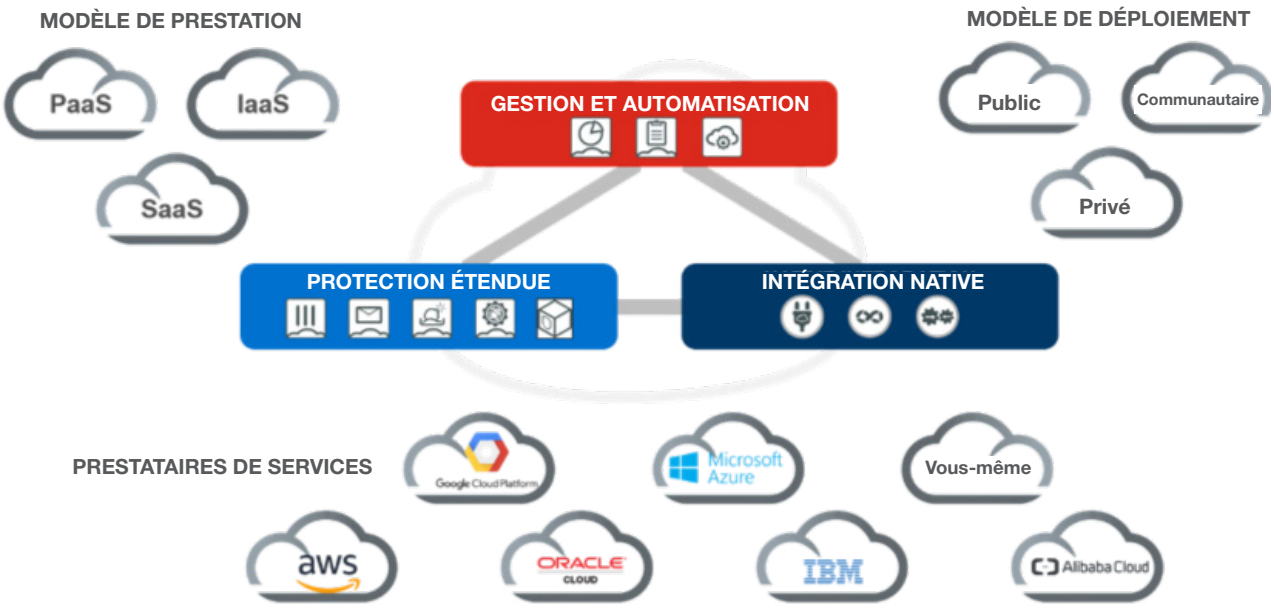

Schéma 4. Une solution complète qui fonctionne avec différents modèles de prestation et de déploiement, ainsi que de multiples fournisseurs de services.

La visibilité. La capacité à voir de manière cohérente toutes les applications, réseaux, infrastructures, événements de sécurité et journaux dans un environnement multi-cloud est la pierre angulaire de l'évaluation de sa politique de sécurité. Cette évaluation est la fois un point de départ et un processus continu de gestion de la sécurité. Les entreprises doivent identifier les ressources réparties dans l'infrastructure, associer les flux de trafic, comprendre quelles applications sont utilisées et identifier les données qui traversent le réseau. FortiAnalyzer offre une visibilité en ligne de l'ensemble des systèmes Fortinet pour une analyse approfondie, et FortiCWP fournit une visibilité de la pile de cloud public en exploitant des API spécifiques au cloud.

Ces informations permettent à une entreprise de vérifier si les politiques de sécurité sont efficaces et si des politiques de sécurité supplémentaires sont nécessaires. Dans un environnement multi-cloud où les applications communiquent entre les différentes infrastructures, la capacité à centraliser la traçabilité des flux de trafic et à comprendre la séquence des événements dans chaque environnement cloud offre souvent plus d'informations que ce que révèlent les outils de sécurité standards. En outre, la possibilité de regrouper les informations sur l'infrastructure de sécurité et la visibilité de l'infrastructure cloud dans une interface unique simplifie davantage les opérations.

Le contrôle. Une fois qu'une entreprise a une visibilité totale en matière de sécurité, l'étape suivante consiste à appliquer des contrôles aux fonctions concernées. Cela implique d'appliquer des modifications de configuration et d'alimenter l'infrastructure de sécurité avec les informations pertinentes relatives aux ressources concernant la politique de sécurité multi-cloud. Les outils de gestion de la sécurité doivent étendre une infrastructure de contrôle cohérente au large éventail de fonctions de sécurité.

De plus, l'infrastructure de contrôle doit s'étendre à la fonctionnalité de sécurité native fournie par chaque plateforme cloud. Cela permet aux administrateurs et opérateurs d'appliquer les modifications de sécurité dans l'ensemble de l'infrastructure, quelle que soit la technologie sous-jacente. FortiManager aide les administrateurs à appliquer des politiques cohérentes dans les infrastructures.

La politique. L'exploitation des fonctionnalités de visibilité et de contrôle de Fortinet Security Fabric permet aux entreprises d'obtenir une gestion et une application cohérentes de la sécurité dans l'ensemble de l'infrastructure. Comme le cycle de vie global des applications est ce qui favorise l'apport de modifications à l'infrastructure, la charge et le temps d'interprétation de la façon dont les modifications apportées aux applications affectent l'infrastructure sont considérablement réduits. À la place, le personnel de sécurité peut modifier les paramètres de sécurité en fonction des événements du cycle de vie des applications afin d'obtenir des politiques de sécurité plus cohérentes.

FortiCWP aide à identifier les erreurs de configuration des politiques et les violations de la conformité. Ce service utilise les renseignements sur les menaces et l'intégration native pour évaluer les configurations, surveiller l'activité des comptes cloud, contrôler le trafic réseau cloud, analyser les données et fournir des rapports de conformité.

FortiManager facilite encore plus la gestion des politiques multi-cloud en permettant aux entreprises de gérer tous leurs appareils Fortinet depuis une console unique. Cette solution offre une visibilité totale du réseau, en proposant des outils de déploiement et d'automatisation rationalisés.

Le personnel de sécurité peut exploiter ces fonctionnalités pour passer à une posture de sécurité stratégique en mettant rapidement en œuvre les politiques dans une plateforme centralisée qui permet des mises à jour plus rapides.

La conformité. Le maintien d'une politique de sécurité cohérente et l'automatisation des opérations de sécurité augmentent considérablement la capacité d'une entreprise à garantir la conformité réglementaire. En outre, la gestion centralisée de la sécurité, les flux de travail automatisés et le partage des renseignements sur les menaces aident les entreprises à réagir rapidement aux menaces émergentes. Ces fonctionnalités peuvent également réduire plus efficacement les risques sur l'ensemble de la surface d'attaque sans nécessiter des opérations de sécurité trop difficiles. FortiCWP et FortiCASB répondent aux besoins des entreprises en matière de conformité en identifiant les problèmes de conformité et en fournissant des rapports sur l'état de la conformité.

La sécurité et la recherche sur les menaces

Ce plan documente les principaux éléments de la mise en œuvre de solutions efficaces pour une sécurité cohérente dans le cloud hybride avec une intégration native, une protection étendue, la gestion et l'automatisation. Toutefois, la technologie seule ne suffit pas. Une solution de sécurité cloud de renommée internationale doit inclure des services de renseignement de sécurité utilisés comme sources de données pour les produits déterminant les menaces. Ces services doivent être soutenus par des experts en sécurité ayant les compétences et les ressources nécessaires pour maîtriser le monde en constante évolution de la cybersécurité.

FortiGuard Labs dispose de l'une des plus grandes équipes de recherche et d'analyse en matière de sécurité du secteur, avec des experts du monde entier. Ces experts dévoués sont toujours à l'affût des nouvelles menaces et techniques. Ils étudient tous les domaines essentiels du paysage des menaces, notamment les logiciels malveillants, les botnets, les vulnérabilités des appareils mobiles et de type « zero-day ».

De plus, FortiGuard Labs maintient un écosystème intégré de renseignement sur les menaces avec plus de 200 partenariats et collaborations en matière de renseignement de sécurité. La combinaison d'une équipe de recherche et d'analyse leader du secteur et d'un vaste écosystème de renseignement de sécurité permet à Fortinet de fournir aux entreprises une détection et une protection de pointe nécessaires pour prévenir, détecter et gérer les nouvelles menaces dès leur apparition.

Cas d'usage de la sécurité dans le cloud

Il existe une variété d'initiatives d'adoption du cloud et de cas d'usage de la sécurité à prendre en compte dans le cadre d'une stratégie de sécurité cloud. Les cas d'usage appropriés pour les différentes initiatives cloud peuvent varier. Souvent, les entreprises s'engagent dans l'un des trois types d'initiatives d'adoption du cloud suivants :

- L'utilisation d'applications SaaS
- La création d'applications cloud natives
- La migration ou l'extension d'applications existantes dans le cloud

Ces trois initiatives exigent des solutions de sécurité différentes pour maintenir une posture de sécurité et un modèle opérationnel solides. Bien que le modèle de responsabilité partagée fournisse des conseils utiles, la plupart des entreprises devront étendre leur visibilité et leur contrôle à l'ensemble du cloud, quel que soit le type d'initiative d'adoption du cloud qu'elles prennent.

Bien que l'objectif principal d'accroître la visibilité, le contrôle et la protection des applications dans le cloud soit primordial pour ces trois initiatives, les cas d'usage et les produits spécifiques pour atteindre chaque objectif seront différents. Les trois gammes de solutions de sécurité cloud offertes par Fortinet sont les suivantes : (1) la visibilité et le contrôle, (2) la sécurité des applications, et (3) la connectivité sécurisée. La section suivante explique les différents cas d'usage associés à chaque solution.

1. La visibilité et le contrôle

La visibilité et le contrôle des applications SaaS

Les équipes informatiques et les chefs d'entreprise ont adopté le modèle SaaS comme un moyen flexible, évolutif et rentable de déployer des applications essentielles. Le problème est qu'à mesure que l'utilisation du modèle SaaS augmente, elle est souvent non réglementée et la sécurité traitée comme un ajout après coup. Une stratégie de sécurité cloud efficace doit surveiller toutes les activités SaaS et s'intégrer aux solutions de sécurité pour appliquer des politiques de sécurité uniformes aux applications classiques et SaaS.

Fortinet offre un contrôle centralisé des applications SaaS afin que les entreprises puissent déployer les meilleures pratiques en matière de conformité et de gouvernance. Fortinet aide également les entreprises à protéger les données sensibles des applications contre les menaces avancées et contrôler de manière centralisée les applications de type « Shadow IT ». Les entreprises bénéficient également de politiques de contrôle des applications cohérentes dans l'ensemble de leurs succursales. La sécurité renforcée permet également de réduire la latence et d'offrir le niveau de performance que les utilisateurs attendent.

FortiCASB offre une visibilité centralisée et détaillée de l'utilisation des applications SaaS. Cela permet aux entreprises de mettre en œuvre des politiques uniformes de contrôle et de sécurité des applications, de protéger leurs données sensibles contre les menaces avancées, et d'assurer la conformité et la gouvernance de la sécurité.

La visibilité et le contrôle des infrastructures cloud

Le risque d'erreur de configuration augmente en même temps que l'utilisation du cloud. En outre, comme l'utilisation du cloud public n'est pas toujours surveillée, elle peut entraîner des vulnérabilités non contrôlées.

FortiCWP exploite les API de gestion de cloud public pour surveiller l'activité et la configuration de diverses ressources cloud. Cette solution évalue continuellement les configurations dans les différentes régions et les différents types de clouds publics, et offre une visibilité cohérente. FortiCWP simplifie le signalement des violations de conformité et améliore la conformité en fournissant des conseils sur les meilleures pratiques de sécurité. Ce service propose également des outils de gestion des menaces et des risques qui permettent de déterminer l'origine des erreurs de configuration. FortiCWP prend en charge AWS, Google Cloud Infrastructure et Microsoft Azure.

La conformité dans le cloud

La mise en conformité avec la norme de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard ou PCI DSS), la loi américaine sur l'assurance maladie (Health Insurance Portability and Accountability Act ou HIPAA), la loi Sarbanes-Oxley (SOX), le règlement général sur la protection des données (le RGPD) et d'autres réglementations, peut prendre du temps. La migration vers un ou plusieurs clouds ne fait qu'augmenter cette charge. Les solutions de conformité cloud de Fortinet sont les suivantes :

FortiCWP regroupe et organise les informations de sécurité provenant de plusieurs API et services cloud dans des rapports de conformité significatifs et des tableaux de bord de conformité dynamiques.

Cas d'usage de la sécurité dans le cloud par Fortinet

1. La visibilité etle contrôle

- La visibilité et le contrôle des applications SaaS
- La visibilité etle contrôle des infrastructures cloud
- La conformité dans le cloud
- La gestion et l'analyse de la sécurité dans le cloud

2. La sécurité des applications

- La Sécurité des applications Web
- La segmentation logique (basée sur l'intention)
- La sécurité des conteneurs
- Une productivité sécurisée
- La protection des charges de travail dans le cloud

3. Une connectivité sécurisée

- Un cloud hybride sécurisé
- Un hub de services de sécurité cloud
- Un accès à distance sécurisé

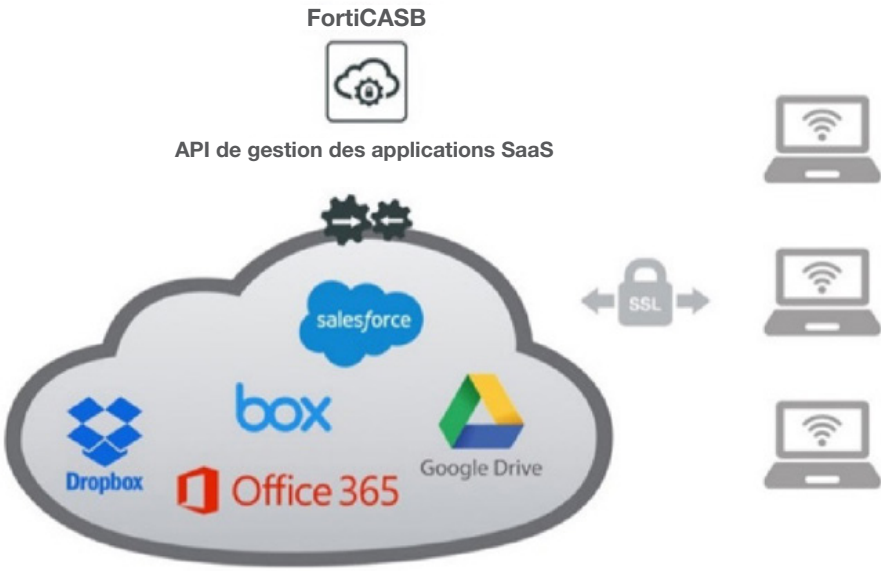

Schéma 5. Cas d'usage de la sécurité dans le cloud public.

FortiSIEM offre une vision plus large de la conformité dans plusieurs clouds, dans la Fortinet Security Fabric et dans les produits tiers. Cette solution vous permet de créer des rapports de conformité d'un simple clic.

FortiAnalyzer collecte les journaux des éléments de Fortinet Security Fabric, et FortiManager permet de contrôler, d'examiner, d'approuver et de mettre en œuvre les modifications. Ensemble, ils ferment la boucle en matière de réduction des écarts de conformité. Tous les systèmes prennent en charge des processus automatisés pour faciliter le flux de travail et la gestion des politiques de conformité, réduisant ainsi les risques lorsque les politiques sont modifiées.

La gestion et l'analyse de la sécurité dans le cloud

L'utilisation d'outils de gestion existants parallèlement aux nouvelles technologies crée des incompatibilités complexes, en particulier lors de la gestion de la sécurité dans le cloud.

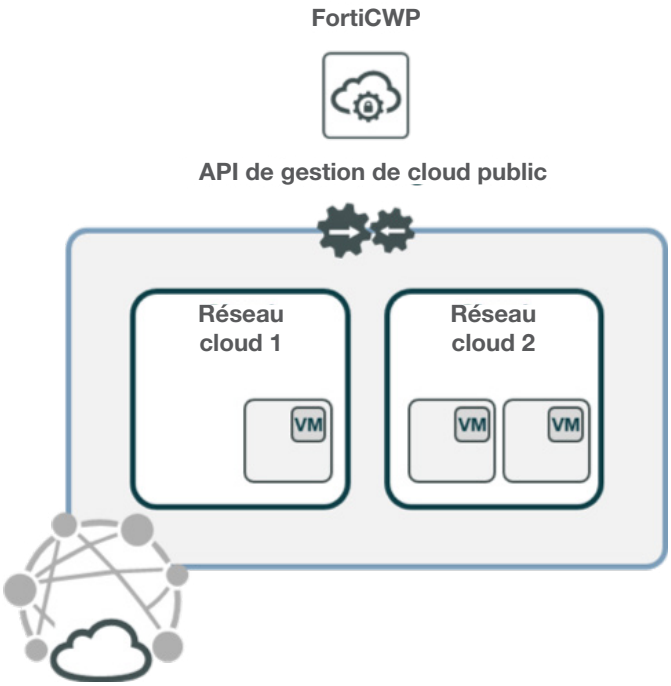

Schéma 6. FortiCWP utilise des API directement dans le cloud public pour surveiller l'activité et la configuration dans les clouds.

Pour relever ces défis, les entreprises peuvent tirer parti de la présence multirégionale et mondiale des principaux fournisseurs d'infrastructures cloud pour déployer des systèmes centralisés et mondiaux de gestion et d'analyse de la sécurité dans le cloud. Les solutions FortiManager-VM, FortiAnalyzer-VM et FortiSIEM-VM peuvent toutes être déployées dans le cloud pour garantir l'évolutivité et la mondialisation. Les avantages sont notamment les suivants :

- Une gestion et une visibilité centralisées et unifiées de la sécurité
- Une optimisation des rapports d'audit et de conformité
- Une réponse plus rapide aux incidents
- L'amélioration de l'efficacité opérationnelle et de la rentabilité, la réduction des risques
- Une capacité accrue à automatiser la gestion de la sécurité

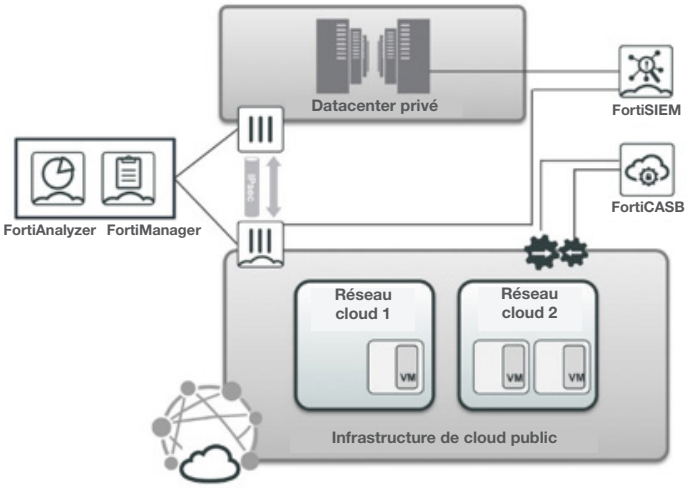

Schéma 7. Solutions Fortinet garantissant la conformité dans le cloud.

2. La sécurité des applications

La sécurité des applications Web

Les applications cloud utilisent souvent des services Web pour communiquer aussi bien en interne qu'en externe, ce qui les rend vulnérables à diverses menaces. De plus, les entreprises qui exploitent ces applications doivent souvent répondre à des exigences de conformité.

Fortinet offre une variété de solutions de sécurité des applications Web idéales pour les clients de services cloud. FortiWeb-VM, une solution WAF de pointe offerte sur toutes les principales plateformes cloud, sécurise les API de services Web ainsi que les applications Web frontales contre les menaces connues et inconnues. Intégrées à FortiWeb, les appliances FortiGate-VM appliquent de manière centralisée les politiques de sécurité et offrent une visibilité accrue. Le service sandbox de Fortinet effectue une analyse dynamique pour identifier les logiciels malveillants jusqu'alors inconnus.

La segmentation logique (basée sur l'intention)

La segmentation des environnements cloud est un défi, car le déploiement dynamique entraîne un changement constant des adresses IP. La segmentation du réseau basée sur des règles d'adresses IP statiques est donc inefficace.

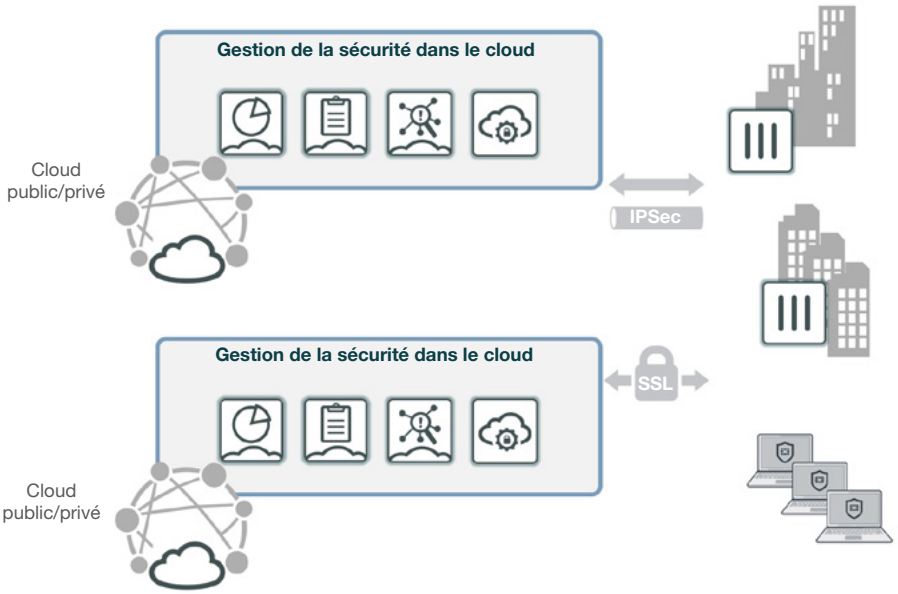

Schéma 8. Solutions Fortinet pour la gestion et l'analyse de la sécurité dans le cloud.

Les appliances FortiGate-VM permettent une segmentation basée sur l'intention, qui crée des segments et des règles d'accès en fonction de l'identité de l'utilisateur ou de la logique métier et les ajuste de façon dynamique en réponse à une évaluation continue de la confiance. Les appliances FortiGate-VM exploitent les métadonnées ou les balises associées aux ressources cloud dans plusieurs clouds pour appliquer les politiques de sécurité. Par conséquent, elles déterminent intuitivement les charges de travail et les éléments dans le cloud qui sont autorisés à communiquer avec d'autres charges de travail et éléments, et si ces derniers se trouvent à l'intérieur ou à l'extérieur du cloud.

La sécurité des conteneurs

Les conteneurs sont rapidement devenus un élément clé du cloud computing. Les conteneurs sont prisés parce qu'ils permettent de packager les applications et leurs dépendances afin de pouvoir déplacer de façon fiable les applications d'un environnement informatique à un autre. Les conteneurs isolent les logiciels du système d'exploitation et du matériel sous-jacent, garantissant ainsi le fonctionnement de l'application où qu'elle se trouve.

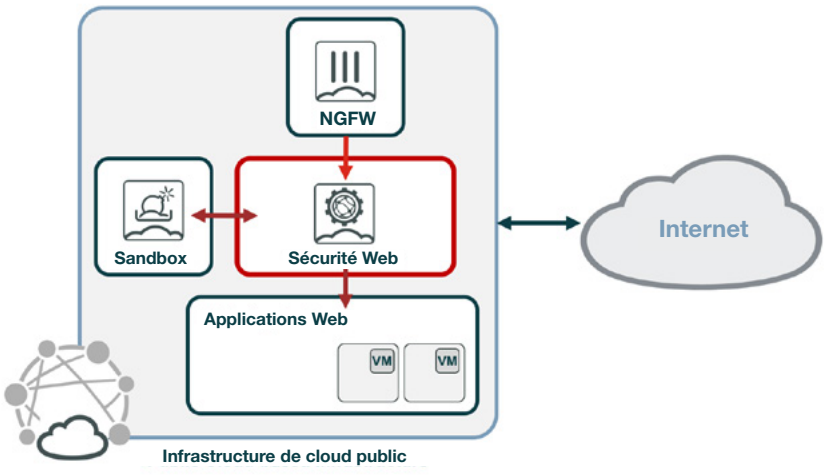

Schéma 9. Fortinet protège les applications contre les menaces connues et inconnues.

La sécurité des conteneurs commence par la protection de l'intégrité des conteneurs sous-jacents. Elle va également plus loin, jusqu'au pipeline des conteneurs, l'infrastructure sur laquelle les conteneurs sont exécutés et les plans de données sur lesquels ils s'appuient.

La solution de sécurité des conteneurs de Fortinet est divisée en quatre domaines de protection complémentaires. Les Fabric Connectors permettent de définir des politiques de sécurité en fonction des étiquettes de conteneurs. FortiGate peut jouer un rôle essentiel dans la sécurisation du trafic nord-sud à l'entrée et à la sortie des conteneurs. Les pare-feux NGFW FortiGate proposent des Fabric Connectors qui s'interfacent avec les principaux systèmes d'orchestration des conteneurs pour exploiter les métadonnées comme objets de politique de sécurité, notamment les outils natifs Kubernetes, AWS EKS, GCP GKE, Azure AKS et OCI OKE.

La solution **FortiWeb**, en tant qu'image de conteneur, peut être intégrée au sein d'une chaîne d'applications. La sécurité intégrée aux conteneurs permet d'intégrer de façon dynamique une solution Fortinet dans les clusters Kubernetes et de l'insérer dans la chaîne d'applications afin de sécuriser les applications Web basées sur des conteneurs.

FortiSandbox garantit la sécurité du registre des conteneurs en analysant les images de conteneurs préconfigurées et extraites pour détecter les codes malveillants et les menaces de type « zero-day ». Enfin, FortiNAC peut s'assurer que l'application et son conteneur ne sont accessibles qu'aux personnes ayant des rôles et des privilèges appropriés.

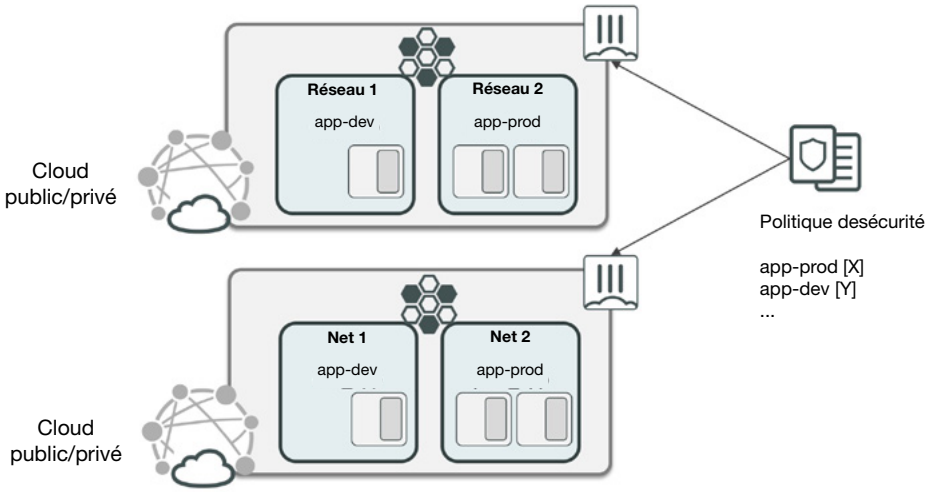

Schéma 10. La segmentation logique.

Une productivité sécurisée

Comme les entreprises externalisent de plus en plus la gestion informatique des applications de productivité et de messagerie, la visibilité et le contrôle de ces applications sont réduits. Les équipes de sécurité doivent être en mesure d'assurer une sécurité dédiée et cohérente dans les environnements multi-cloud.

La combinaison de FortiMail, FortiSandbox et FortiCASB-SaaS permet de bénéficier de fonctionnalités essentielles pour sécuriser les applications de productivité, telles que Microsoft Office 365. La Fortinet Security Fabric offre une grande visibilité du trafic des applications, tandis que les services de sécurité et la technologie sandbox de Fortinet identifient et bloquent les menaces persistantes avancées et de type « zero-day ».

La protection des charges de travail dans le cloud

Les applications intégrées ou migrées vers le cloud doivent être protégées contre les menaces classiques provenant d'Internet, ainsi que contre les nouvelles menaces qui se propagent dans les charges de travail et qui sont introduites via les API.

La combinaison d'une protection en ligne pour le trafic nord-sud, d'une protection basée sur l'hôte pour le trafic est-ouest et d'une protection contre les risques liés aux API et à la configuration du cloud offre la solution de sécurité la plus performante pour le cloud. FortiGate-VM vous permet de protéger vos réseaux cloud virtuels contre les menaces provenant d'Internet et de fournir une connectivité sécurisée entre les clouds. Étendez la sécurité au sein du cloud en utilisant FortiClient sur les machines virtuelles afin d'assurer la conformité et la connectivité. FortiCASB-Cloud offre une protection contre les configurations non souhaitées ou non supervisées au niveau des comptes cloud.

3. Une connectivité sécurisée

Un cloud hybride sécurisé

De nombreuses entreprises utilisent le cloud public pour fournir une infrastructure aux solutions informatiques conjointement avec des datacenters sur site. Dans beaucoup de cas, les nouvelles applications sont uniformément déployées dans le cloud public, tandis que dans d'autres cas, elles sont déployées en parallèle dans des clouds publics et privés.

Il est important pour une solution de prendre en charge des technologies de cloud privé et public. Elle doit également offrir

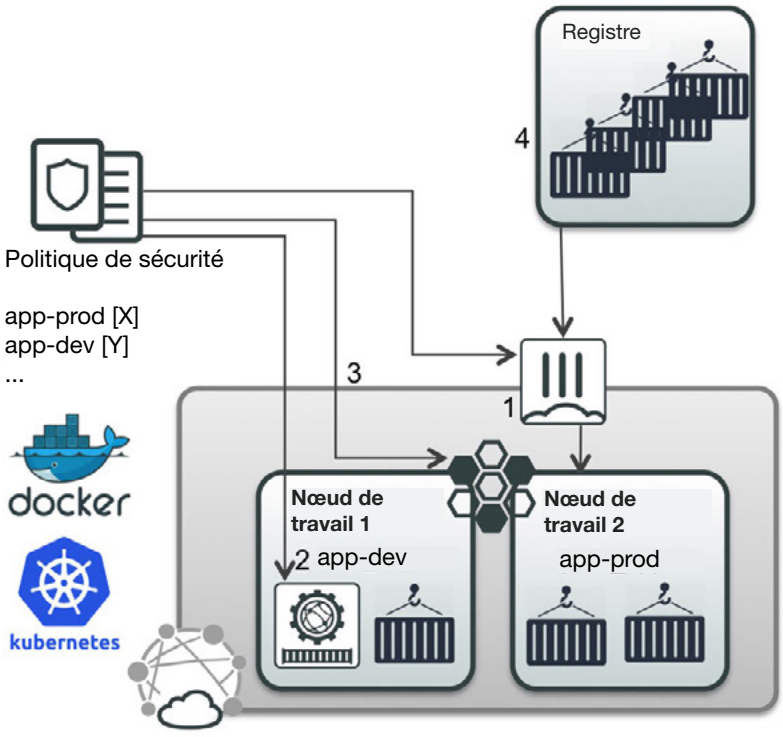

Schéma 11. La sécurité des conteneurs.

une sécurité rapide et puissante afin de faire face à des transferts de gros volumes de données. Une gestion cohérente des politiques de sécurité est également essentielle. Cela permet de garantir que la migration des applications d'une infrastructure à une autre n'entraîne pas de surcharge opérationnelle indésirable en matière de sécurité, qui pourrait éventuellement entraîner des erreurs humaines compromettant la sécurité. De plus, la sécurité doit protéger l'ensemble de la surface d'attaque afin de s'adapter aux changements constants.

Les pare-feux NGFW FortiGate et les solutions de sécurité cloud offrent une connectivité sécurisée, une segmentation du réseau et une sécurité des applications de pointe pour les déploiements de cloud hybride. Ils assurent une application centralisée et cohérente des politiques de sécurité et se connectent via un tunnel VPN haut débit. Les appliances FortiGate-VM déployées dans le cloud public peuvent communiquer et partager en toute sécurité des politiques cohérentes avec des pare-feux NGFW FortiGate de tout format déployés dans un datacenter privé.

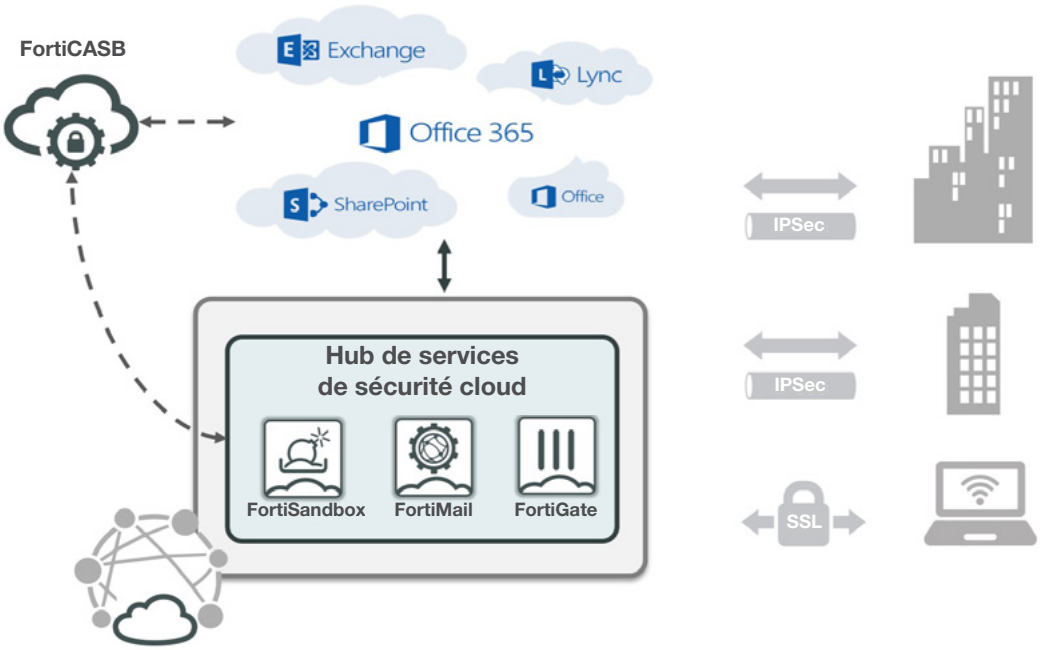

Schéma 12. Une productivité sécurisée dans le cloud par Fortinet.

Les Hub de services de sécurité cloud

Lorsque des équipes développent des applications dans des clouds et réseaux virtuels distincts, la sécurité n'est pas gérée de manière centralisée, ce qui rend difficile la sécurisation des applications résultantes et des divers environnements.

Les équipes de sécurité qui cherchent à unifier des environnements disparates nécessitent un hub de services de sécurité centralisé, ou réseau de transit. Ce hub sépare la sécurité du développement d'applications pour assurer une application centralisée, partagée et cohérente de la sécurité. Il permet également de connecter de façon sécurisée les réseaux, les sites, les clouds et les datacenters. En outre, il analyse et applique les politiques de sécurité sur le trafic entrant et sortant entre le cloud et Internet.

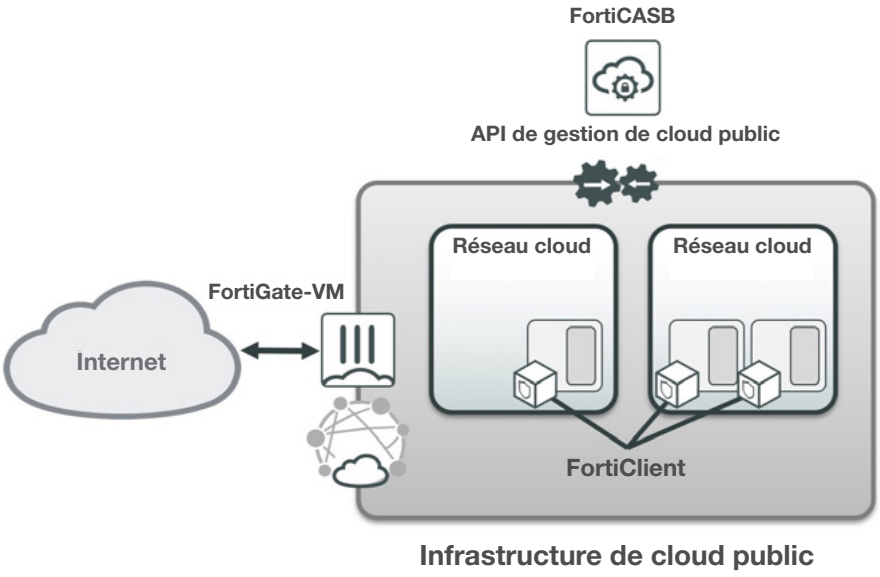

Schéma 13. La protection des charges de travail dans le cloud par Fortinet.

Un accès à distance sécurisé

Les entreprises ont besoin d'un accès sécurisé, à la demande et mondial aux ressources cloud, qui peut intégrer un contrôle d'accès, un suivi des événements et une analyse des données. Les VPN d'accès à distance classiques ne peuvent toutefois pas répondre à ces exigences.

Les équipes de sécurité ont besoin de modèles de configuration qui permettent une terminaison de l'accès à distance sécurisé dans le cloud. Ensuite, elles peuvent déployer de façon dynamique des instances FortiGate-VM préconfigurées avec ces modèles au niveau mondial. Cela permet au personnel mobile, aux clients et aux partenaires commerciaux de se connecter au réseau virtuel de l'entreprise, ainsi que de connecter le réseau cloud aux applications métiers via des tunnels VPN, qu'ils soient déployés dans le cloud ou sur site.

Conclusion

Le cloud offre aux entreprises d'immenses opportunités commerciales. Mais sans infrastructures de sécurité et d'exploitation adéquates, le cloud présente de sérieux défis en matière de sécurité qui peuvent avoir des répercussions considérables. Les données et les applications essentielles sont dispersées dans plusieurs clouds. L'adoption rapide et décentralisée de services cloud se traduit souvent par un ensemble hétérogène d'outils et de politiques de sécurité gérés de façon cloisonnée.

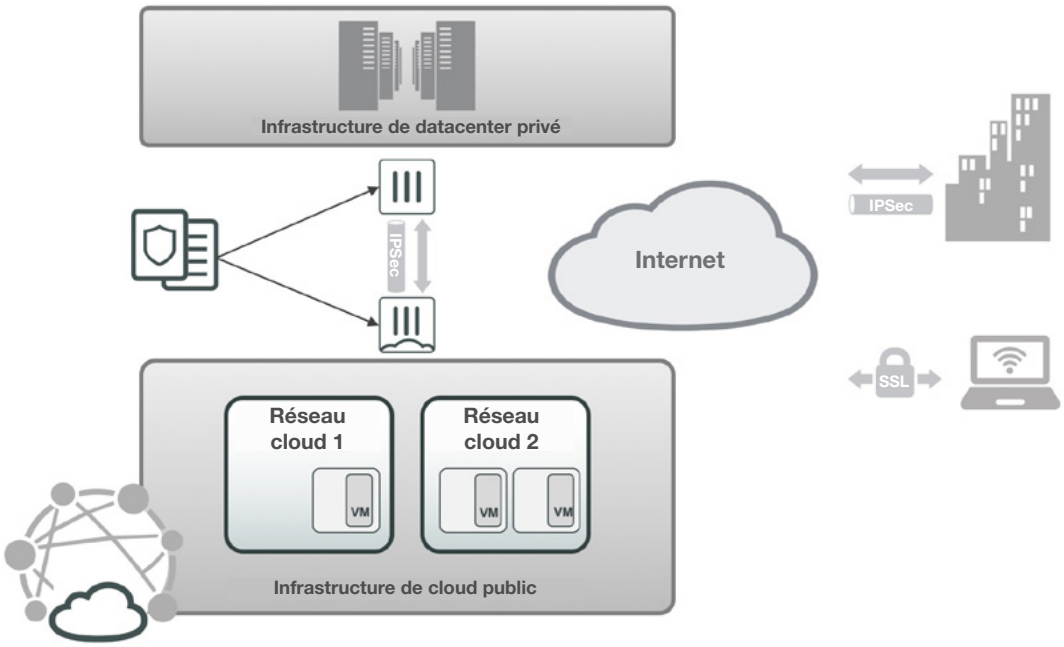

Schéma 14. Un Cloud hybride sécurisé.

Le modèle de responsabilité partagée en matière de sécurité dans le cloud impose aux fournisseurs de services cloud de protéger uniquement l'infrastructure et non les applications déployées et exécutées, ni les données stockées dans le cloud. Ce sont les utilisateurs finaux qui sont responsables de la sécurité de la couche applicative. Comme chaque fournisseur de services cloud utilise des outils et des méthodes de sécurité différents, il est difficile pour les entreprises de les associer aux outils de sécurité qu'elles utilisent pour protéger leurs applications.

Pour sécuriser les environnements multi-cloud, les entreprises doivent suivre trois principes :

- Une intégration native avec tous les principaux fournisseurs de services cloud
- Une vaste suite d'outils de sécurité qui couvrent la totalité de la surface d'attaque
- Une gestion centralisée de la sécurité, notamment l'automatisation des flux de travail et le partage des renseignements sur les menaces

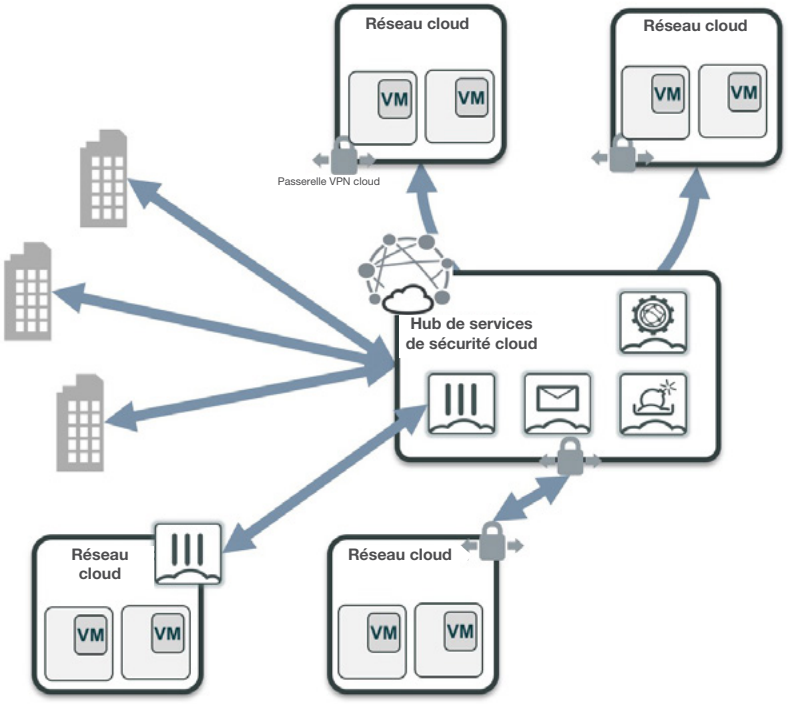

Schéma 15. Fortinet agit comme un point de contrôle unique dans les clouds et les datacenters.

En raison de l'hétérogénéité des déploiements cloud, les entreprises doivent prendre en compte différents cas d'usage de sécurité. Chacun d'entre eux s'accompagne d'exigences de sécurité, telles que l'intégration de tous les éléments de sécurité sur l'ensemble de la surface d'attaque, l'automatisation de la sécurité sur plusieurs clouds, des infrastructures de sécurité spécifiques au cloud avec une gestion centralisée des politiques pour garantir la conformité réglementaire, une sécurité qui s'étend tout au long du cycle de vie des applications, un hub de services de sécurité cloud, etc.

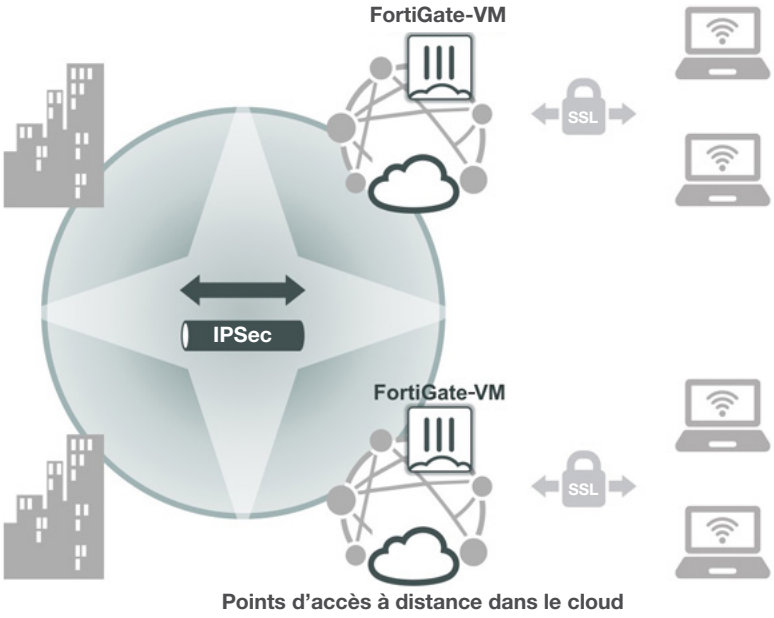

Schéma 16. Fortinet agit comme un point de contrôle unique dans les clouds et les datacenters.

[1] « Q3 2017 Threat Landscape Report », Fortinet, 17 novembre 2017.

[2] « FortiGate: Secure SD-WAN », Fortinet, 2019.

[3] « Cloud Business Email Market, 2018-2022 », The Radicati Group, Inc., Juin 2018.

5 mai, 2020 3:39 PM

471739-0-1-FR

Key Principles and Strategies for Securing the Enterprise Cloud A4_FR