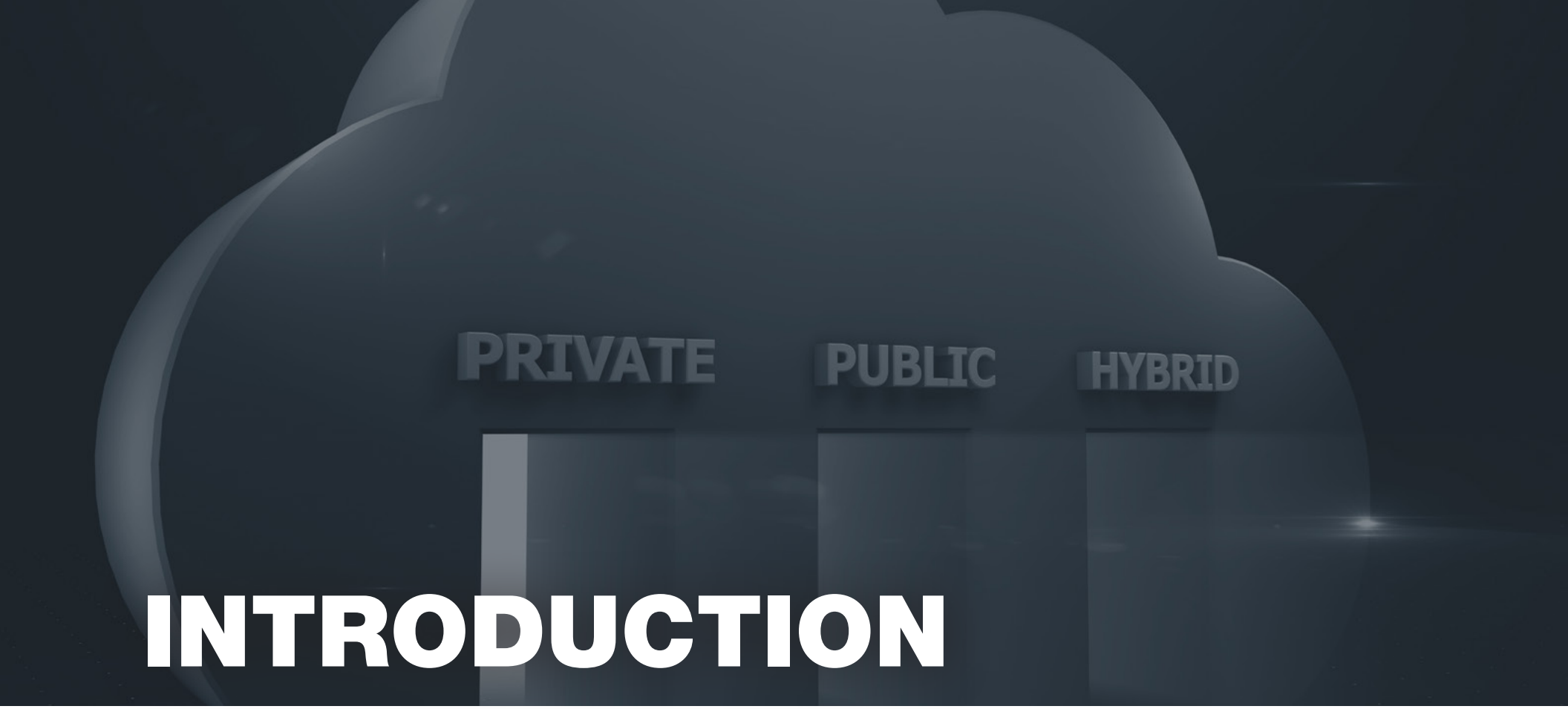
UNE SÉCURITÉ RÉSEAU ADAPTÉE À CHAQUE TYPE DE CLOUD

SOMMAIRE



INTRODUCTION

La sécurité dans le cloud doit satisfaire des exigences uniques propre à chaque cloud. Un **cloud public** repose sur une infrastructure partagée et la nécessité d'utiliser un modèle de sécurité commun. Un **cloud privé** requiert une approche logicielle en matière de sécurité du fait du manque de visibilité induite par le trafic horizontal et les services virtualisés. Un **cloud hybride** implique de combiner des ressources internes stratégiques à des connexions et des sources de données externes, ce qui accroît la nécessité de segmenter les ressources sur le réseau.

Les solutions actuelles de sécurité dans le cloud ne peuvent pas se limiter à prévenir les attaques. Elles doivent tenir compte de la survenue de brèches à un moment ou un autre et être adaptables pour garantir la protection des biens et des utilisateurs.

01 UNE SÉCURITÉ ADAPTÉE AU PARADIGME DU CLOUD

La sécurité dans le cloud de Fortinet est conçue pour s'adapter à la nature même du cloud en fournissant une ressource dynamique qui peut évoluer rapidement en fonction de divers déploiements (public, privé et hybride).

Évolutivité : la sécurité doit correspondre à l'évolutivité et à la flexibilité des charges de travail dans le cloud. Par conséquent, l'automatisation est une caractéristique essentielle de la sécurité dans le cloud de Fortinet. Les politiques de risque et d'accès sont définies au préalable de manière à configurer automatiquement les nouveaux dispositifs ajoutés au réseau afin de prendre en charge plus d'utilisateurs ou une bande passante plus importante dans l'environnement de cloud.

Tableau de bord unique : la politique, la mise en conformité et l'automatisation doivent être appliquées uniformément sur les ressources statiques et dynamiques par le biais d'une vue unique sur la stratégie de sécurité globale. Notre solution permet de traiter de la même manière les charges de travail ou les systèmes partageant le même profil de risque lors de leur connexion/déconnexion du réseau, indépendamment de leur localisation (dans votre centre de données ou chez votre fournisseur).

Segmentation : la possibilité de segmenter les systèmes, les charges de travail, voire les composants réseau spécifiques est indispensable pour gérer les risques de l'entreprise. Le cloud introduit également de nouveaux problèmes inhérents à la conformité. Lorsque des données peuvent transiter par votre réseau, voire le quitter, via le cloud public, la conformité des données est impérative pour garantir la surveillance et le contrôle d'un trafic spécifique, des applications ou des types de données.

02 LA SÉCURITÉ DANS UN CLOUD PUBLIC

Le problème de sécurité le plus médiatisé concerne le cloud public. Les dirigeants d'entreprise et les utilisateurs n'ont surmonté que récemment le scepticisme inhérent à l'abandon du contrôle de leur infrastructure, ainsi qu'au partage des systèmes et de la bande passante avec des tiers qu'ils ne connaissent pas.

La solution de sécurité cloud de Fortinet permet de sécuriser les charges de travail sur les clouds publics pour garantir le respect de la vie privée et la confidentialité tout en tirant profit de l'évolutivité, de la mesure de la consommation et des délais de commercialisation.

Un modèle de sécurité partagé : un modèle de sécurité partagé comprend deux éléments stratégiques :

- La sécurité **« du » cloud**. Elle inclut tous les centres de données mis à disposition par le fournisseur de services dans le cloud qui doit en assurer la sécurité.
- La sécurité **« dans » le cloud**. Elle inclut ce que vous, en tant qu'abonné aux services cloud, fournissez en termes de données et d'applications dans le cloud. C'est à vous qu'il incombe de protéger ces éléments.

L'offre de sécurité cloud de Fortinet s'adresse aux composants clients tels que : les données, les applications, les systèmes d'exploitation, la gestion des accès et des identités, le chiffrement et le trafic réseau. Elle vient compléter les fonctionnalités de protection du fournisseur afin d'offrir une protection complète et conforme.

L'intégration des fournisseurs : notre solution s'intègre également étroitement à la sécurité de votre fournisseur de services dans le cloud public afin de protéger votre puissance de calcul, votre capacité de stockage et votre interconnexion réseau. Elle propose également un tableau de bord commun qui offre les deux vues et gère tous les aspects de la sécurité.

La sécurité dans le cloud public de Fortinet comprend :

- La prise en charge des cinq principales plates-formes de cloud public : AWS, Azure, Google, IBM et Oracle
- La prise en charge des plates-formes SaaS (Software-as-a-Service), comme Office 365 et Salesforce.com. Le SaaS est un autre format essentiel du cloud public dont la sécurisation est toute aussi importante que celle du IaaS (Infrastructure-as-a-Service).
- La prise en charge d'une architecture mutualisée pour le cloud et des domaines virtuels pour la segmentation réseau
- L'orchestration de cloud native pour automatiser l'évolution, la haute disponibilité et la segmentation
- Une interface de gestion extensible : des API d'automatisation et d'orchestration de cloud supplémentaires

03 LA SÉCURITÉ DANS UN CLOUD PRIVÉ

La virtualisation est à la base de toutes les formes de cloud computing et ne doit surtout pas être négligée dans la sécurité des clouds privés. Le Software Defined networking (SDN) et autres types d'infrastructures sont sur la couche virtualisation afin de constituer des clouds privés flexibles émergeant des centres de données traditionnels.

La solution Software-Defined Security de Fortinet est certifiée par les principales plates-formes SDN et de virtualisation de la fonction réseau (NFV) et applicable à n'importe quel centre de données transformé en environnement cloud.

La Software-Defined Security : du fait du développement des SDN, les ressources d'interconnexion réseau ne sont plus physiquement associées à des équipements dédiés. Elles sont plutôt utilisées en tant que services dans le centre de données mais peuvent aussi fonctionner sur tous les éléments physiques ou sur les sites. De même, la solution de cloud privé de Fortinet a été conçue pour offrir des services de sécurité à la configuration et au provisionnement dynamiques. Cette approche évolutive étend la sécurité à chaque couche conceptuelle de l'architecture réseau (du plan de données au plan de contrôle, sans oublier le plan de gestion).

Une sécurité centrée sur l'application : bien que plusieurs applications partagent la même infrastructure physique sur un cloud privé, elles ne présentent généralement pas les mêmes risques. La sécurité dans le cloud de Fortinet isole les données et les applications au fur et à mesure de la consolidation du centre de données. Avec l'augmentation du trafic horizontal dans les environnements Software Defined, notre solution garantit une micro-segmentation pour séparer davantage les types de trafic spécifiques.

La sécurité dans le cloud privé de Fortinet comprend :

- La prise en charge des principales plates-formes SDN, y compris VMware NSX, Cisco ACI et OpenStack
- L'orchestration NFV supplémentaire pour l'insertion et le chaînage des services aux clouds et environnements mutualisés des fournisseurs de services
- La prise en charge d'un domaine virtuel et mutualisé pour la segmentation du réseau et le déploiement fonctionnel d'un service de sécurité
- Une interface de gestion extensible : des API d'automatisation et d'orchestration cloud
- Un tableau de bord de gestion unique intégré
- Un portefeuille très étendu et des options de déploiement flexibles

04 LE CLOUD HYBRIDE

La plupart des entreprises sont en passe de basculer d'un centre de données sur site vers un service de cloud public et envisagent de conserver un déploiement informatique conventionnel combiné à un déploiement de cloud public. La mise en œuvre d'un cloud hybride dynamique nécessite une migration ouverte et sécurisée de gros volumes de données et d'applications, une connectivité fiable entre les sites et un ajustement des topologies réseau à l'échelle du réseau étendu (WAN).

La solution de cloud hybride de Fortinet confère à votre équipe une visibilité complète incluant la gestion de bout en bout, la segmentation et la sécurisation des connexions externes.

Une gestion via un tableau de bord unique : les ressources étant réparties entre les partitions physiques et virtuelles, les professionnels de la sécurité ne doivent pas basculer entre plusieurs tableaux de bord pour avoir une vue d'ensemble ou travailler sans analyse centrale des renseignements sur les menaces. La solution de cloud hybride fournit une vue intégrée unique de tous les systèmes opérant dans le cloud et permet ainsi une gestion centralisée. Vous pouvez ainsi suivre les flux de données à l'échelle du réseau dans un format proposant des informations pertinentes et exploitables.

La segmentation : la sécurité dans le cloud hybride de Fortinet identifie les entités commerciales et les applications stratégiques qui ne sont pas directement associées à des environnements hybrides mixtes et les segmente afin de réduire les risques en cas de brèche. Elle permet également de contrôler le trafic persistant entre les segments de cloud pour prévenir les pertes de données et garantir l'acheminement des données en fonction des risques et de la politique.

Une connectivité sécurisée : migration des données entre les sites, chargement d'ensembles de données volumineux à partir de sources externes, recours aux services d'analyses basées sur le cloud gérés par des tiers; Tous ces éléments requièrent de se connecter discrètement à des réseaux externes. Notre solution offre une protection adaptée reposant sur le profil de risque de ces connexions réseau uniques. Elle intègre également une fonctionnalité VPN robuste qui permet notamment de fournir un accès provisoire sécurisé aux ressources, au besoin, tout en protégeant le reste du réseau.

La sécurité dans le cloud hybride de Fortinet comprend :

- Une adaptation automatique de l'efficacité de la sécurité du réseau et du planning de capacité
- Une gestion centralisée pour un provisionnement automatique
- Une connectivité VPN entre les sites
- La segmentation des connexions persistantes
- Une visibilité complète et un contrôle total des logs de sécurité afin d'optimiser la gouvernance de la conformité

CONCLUSION

Fortinet est la seule entreprise à proposer des solutions de sécurité dédiées au réseau, aux terminaux, aux applications, aux centres de données, au cloud et aux accès conçues pour fonctionner de pair comme un système de sécurité intégré tout en garantissant une protection véritablement complète.

Notre solution de sécurité dans le cloud dédiée est compatible avec les principaux produits Fortinet pour diversifier les modèles de déploiement dans le cloud tout en prenant en charge une gestion centralisée, l'intégration d'API ouvertes, la mesure de la consommation, l'orchestration de plate-forme de cloud et l'automatisation.

La solution Security Fabric de Fortinet partage les renseignements sur les menaces de manière dynamique avec le reste de l'infrastructure de sécurité interconnectée. Elle induit ainsi une réduction de la nécessité de disposer de plusieurs points de contact et politiques redondantes à travers les installations de cloud tout en garantissant la gouvernance à travers les limites de sécurité multi-couches.

www.fortinet.fr