FORTINET SECURITY FABRIC ÉTEND LA SÉCURITÉ AVANCÉE DE MICROSOFT AZURE

RÉSUMÉ

Microsoft Azure est conçu pour augmenter la conformité et la sécurité du cloud, en facilitant la migration vers le cloud hybride et les chemins de coexistence. Microsoft Azure prend en charge un large éventail de solutions et de technologies de sécurité destinées à protéger les informations situées dans Azure et sur site. De plus, Azure présente des avantages uniques aux entreprises habituées à utiliser depuis longtemps les services d'entreprise de Microsoft, qui sont progressivement déplacés vers le cloud via Office 365. Cependant, Azure et Office 365 n'offrent pas de fonctions de sécurité d'entreprise complètes, capables de protéger les données dans le cloud. Les entreprises nécessitent une visibilité approfondie accrue et un contrôle granulaire supplémentaire sur les applications et les informations au sein des infrastructures locales et de cloud public. Fortinet Security Fabric pour Azure permet aux entreprises d'appliquer des politiques de sécurité cohérentes à l'ensemble de leurs infrastructures multi-cloud afin de bénéficier d'une plus grande visibilité, d'un meilleur contrôle et d'une protection renforcée contre les redoutables attaques basées sur le cloud.

SÉCURISATION D'UNE VARIÉTÉ DE CLOUDS PUBLICS AZURE

La solution Fortinet Security Fabric pour Azure étend aux environnements cloud Microsoft Azure des fonctions de sécurité d'entreprise haut de gamme uniformes. Elle protège les charges de travail métiers dans les data centers locaux comme dans les environnements cloud (sécurité multicouche pour applications cloud incluse). La solution Security Fabric prend en charge une grande variété d'environnements cloud d'entreprise courants, notamment les suivants :

1. **Cloud hybride.** Les entreprises nécessitent une orchestration transparente de la sécurité, capable de s'adapter aux charges de travail du cloud. Fortinet Security Fabric comprend des pare-feux NGFW (Next-Generation Firewall) qui complètent les fonctions de sécurité Azure natives tout en prenant en charge une connectivité sécurisée et chiffrée pour tout type d'infrastructure cloud. Il est possible de gérer ces pare-feux à partir d'un déploiement dans le cloud public ou d'un déploiement local au sein d'un data center privé.
2. **Prévention avancée des menaces.** Une proportion de plus en plus importante des applications métiers modernes sont déployées sur des infrastructures de cloud public. Parallèlement à cela, les applications Web et de messagerie sont responsables du plus grand nombre de violations par schéma. Fortinet Security Fabric pour Azure comprend des solutions destinées à protéger ce genre d'applications critiques pour l'entreprise contre les attaques connues et de type zero-day en tirant parti de solutions Security Fabric telles que FortiWeb, FortiMail et FortiSandbox. L'entreprise évite ainsi de devoir constamment appliquer des correctifs aux serveurs. Cette solution assure également la conformité aux normes réglementaires et de sécurité telles que la norme de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard ou PCI DSS) et la loi américaine sur l'assurance maladie (Health Insurance Portability and Accountability Act ou HIPAA). De plus, FortiSandbox permet de protéger les sites Web de collaboration contre les risques associés aux menaces persistantes avancées (APT, Advanced Persistent Threats) résultant du téléchargement de fichiers malveillants.
3. **VPN d'accès sécurisé.** Fortinet Security Fabric offre des performances hors pair en matière de sécurisation du trafic VPN pour l'accès à distance au VPN dans Azure. En tirant parti de l'infrastructure mondiale multirégionale d'Azure, les entreprises peuvent instantanément dimensionner leurs services à l'échelle mondiale et proposer une terminaison VPN d'accès à distance proche de l'utilisateur final. Le VPN d'accès à distance permet aussi bien d'accéder à des applications cloud qu'à des applications locales connectées au cloud par le biais d'autres formes de liaisons privées ou de VPN.
4. **Hub de services cloud (vNET).** La connectivité des fournisseurs de cloud surpasse de loin celle d'une entreprise de taille moyenne classique. Un réseau virtuel Azure (vNET) permet aux entreprises de partager des services de sécurité au sein de plusieurs réseaux à travers le monde. En tirant parti de l'étendue des solutions Fortinet, notamment la visibilité sur le réseau, la connectivité VPN, le pare-feu NGFW (Next-Generation Firewall), le pare-feu avancé pour applications Web, un outil sandbox et la sécurité de la messagerie, Security Fabric propose une palette de services bien plus grande tout en tirant parti de l'élasticité du cloud et de l'évolutivité à la demande pour un rapport prix/performance optimisé.
5. **Sécurisation d'Office 365.** En raison du taux d'attachement élevé entre Office 365 et les déploiements de cloud Azure, parallèlement au fait que la plupart des menaces s'insinuent dans les entreprises par le biais de la messagerie électronique, la nécessité de sécuriser les applications métiers et de messagerie basées sur Office 365 est plus forte que jamais. La combinaison de FortiMail, FortiSandbox et FortiCASB permet de bénéficier de fonctionnalités essentielles dans le cadre de la sécurisation d'Office 365. Security Fabric offre notamment une visibilité approfondie sur les messages électroniques à des fins de protection contre les menaces de type zero-day et de surveillance de la couche d'API Office 365.

COMPLÉMENTARITÉ ENTRE LA SECURITY FABRIC ET LES FONCTIONS DE SÉCURITÉ D'AZURE

La Security Fabric offre une protection multicouche approfondie et des avantages opérationnels en matière de sécurisation des applications contre les menaces connues et inconnues d'Azure, et sur le plan de la gestion des infrastructures de sécurité mondiales à partir du cloud. La Security Fabric pour Azure présente les fonctionnalités clés suivantes :

Contrôle et gestion via une interface unique. La Security Fabric permet de gérer de façon centralisée les fonctionnalités de sécurité cloud et locales à partir d'Azure, ce qui contribue à éviter les erreurs humaines tout en réduisant la charge de travail des services informatiques limités en ressources.

Visibilité et contrôle directement dans le cloud. Les entreprises gagnent en visibilité sur leurs déploiements d'applications Azure grâce à La Security Fabric. Elles n'ont plus besoin de planifier des configurations de déploiement spécifiques, mais peuvent désormais appliquer des politiques davantage orientées sur l'intention. Grâce à l'utilisation de groupes d'adresses dynamiques et à l'attribution de noms logiques aux ressources cloud, il est possible d'étendre les politiques de sécurité en tant que montée en puissance des ressources Security Fabric dans toute l'infrastructure cloud.

Contrôle du Shadow IT. La tendance est à la rationalisation des opérations informatiques et à la consolidation des contrôles de sécurité dans les entreprises. C'est pourquoi dans de nombreux secteurs d'activité, ces dernières s'approvisionnent elles-mêmes directement en services cloud. Security Fabric offre aux services informatiques une meilleure visibilité sur l'utilisation des infrastructures Azure et la possibilité de mettre en œuvre des contrôle plus stricts des modèles d'utilisation afin de lutter contre les risques.

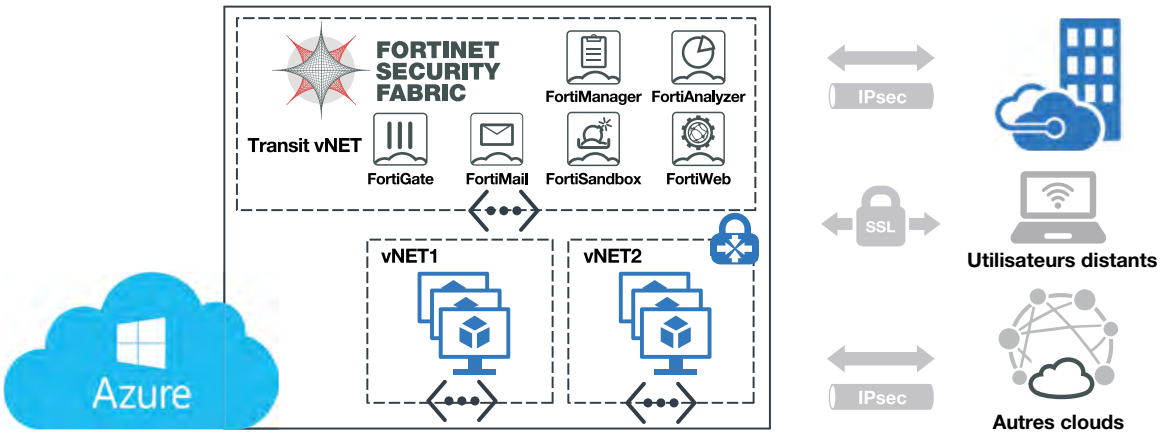

SCHÉMA 1 : SOLUTION FORTINET SECURITY FABRIC POUR MICROSOFT AZURE

Protection contre les attaques de type Zero-Day. Pour contrer les attaques de type Zero-Day, les solutions Fortinet Security Fabric offrent une protection hautement évolutive, entièrement intégrée à l'infrastructure cloud. L'entreprise réduit ainsi considérablement son exposition aux menaces persistantes avancées et se sent plus en confiance pour déployer des applications à n'importe quelle échelle dans le cloud.

Mise en conformité. Les solutions Security Fabric offrent une protection incomparable destinée à garantir la mise en conformité des entreprises avec les normes du secteur en vigueur (PCI DSS, par ex.) et la législation récente sur la confidentialité des données, notamment le Règlement général sur la protection des données (RGPD) de l'UE.

DÉFENSES INTÉGRÉES COUVRANT TOUT LE SPECTRE DES ATTAQUES

Les différentes solutions qui composent Fortinet Security Fabric pour Azure ont été conçues pour augmenter la confiance de l'utilisateur final dans les environnements cloud Azure. Ces solutions reposent toutes sur des formats de machine virtuelle (VM) Fortinet. Les licences acquises auprès d'un partenaire revendeur Fortinet pour machines virtuelles sont transférables d'une plate-forme à l'autre. Par exemple, une licence VM pour FortiGate-VM sur VMware fonctionne aussi sur la plate-forme FortiGate pour Azure via l'utilisation du modèle BYOL. En outre, il est possible de consommer FortiGate, FortiMail et FortiWeb à l'aide du **modèle d'utilisation à la demande (PAYG)** directement depuis la Marketplace Azure.

Les solutions suivantes font partie de Fortinet Security Fabric pour Azure :

- **FortiGate-VM NGFW** propose l'un des jeux de fonctionnalités de protection contre les menaces les plus performants du secteur pour lutter contre les cyberattaques connues et inconnues les plus avancées. FortiGate-VM dimensionne la solution en fonction des exigences du client et se décline en plusieurs tailles pour s'adapter à une variété de cas d'utilisation pris en charge.
- **FortiMail** propose des passerelles de sécurité de la messagerie qui font appel aux technologies et services les plus récents mis au point par FortiGuard Labs. Ces passerelles offrent une protection de haut niveau constante contre les menaces courantes et avancées tout en intégrant de puissantes fonctionnalités permettant d'éviter la perte de données.
- **FortiSandbox** propose une puissante combinaison de détection avancée, de réduction des risques automatisée, d'informations exploitables et de flexibilité de déploiement pour empêcher les attaques ciblées et la perte de données qui s'ensuit.
- **FortiWeb** comprend des firewalls pour applications Web (WAF) destinés à protéger les applications Web hébergées contre les attaques qui ciblent les failles connues et inconnues. À l'aide de méthodes de détection multicouches et corrélées, FortiWeb défend les applications contre les vulnérabilités connues et les menaces de type zero-day.
- **FortiManager** propose un tableau de bord de gestion unique et des contrôles de politiques étendus à toute l'entreprise pour offrir un aperçu des menaces et du trafic à l'échelle du réseau. Elle comprend des fonctions de lutte contre les attaques avancées, ainsi qu'une évolutivité permettant de prendre en charge jusqu'à 10 000 périphériques Fortinet.
- **FortiAnalyzer** collecte, analyse et corrèle les données des produits Fortinet afin de garantir une visibilité accrue et de solides informations sur les alertes de sécurité. Associée à un abonnement au service Indicator of Compromise (IOC) FortiGuard, cette solution propose également une liste hiérarchisée des hôtes compromis pour permettre une intervention rapide.
- **FortiCASB** propose un service d'abonnement dans le cloud à CASB (Cloud Access Security Broker). Ce service prend en charge la visibilité, la conformité, la sécurité des données et la protection contre les menaces. Il fournit des informations analytiques sur les utilisateurs, les comportements et les données stockées dans le cloud via des outils de reporting complets.
- **Fabric Connectors** comprend des connecteurs qui permettent l'intégration ouverte de Fortinet Security Fabric de façon à automatiser l'insertion des fonctions de pare-feu et de sécurité réseau dans des flux réseau dynamiques incluant plusieurs composants existants au sein de l'écosystème d'un client.

PROTECTION MULTICOUCHE QUI LIMITE LES RISQUES

Fortinet élimine les obstacles qui entravent la visibilité et la gestion de la sécurité sur tous les types de plates-formes cloud (privé, public et hybride). Il permet aux responsables sécurité de s'assurer que leurs réseaux couvrent la totalité de la surface d'attaque.

Grâce à Fortinet Security Fabric pour Azure, les entreprises disposent d'une solution de sécurité uniforme au sein d'un modèle à responsabilité partagée, du local au cloud. Cette solution offre une sécurité multicouche complète et une prévention des menaces aux utilisateurs Azure. Dans le même temps, elle simplifie les opérations, l'administration des politiques et la visibilité pour une gestion du cycle de sécurité améliorée.

FORTINET

www.fortinet.fr

mai 24, 2019 11:37 AM

279230-0-1-FR Solution-Brief-Azure-A4_FR