GESTION DE LA POLITIQUE DE SÉCURITÉ EN DATA CENTER DE NOUVELLE GÉNÉRATION

An AlgoSec Whitepaper

Introduction

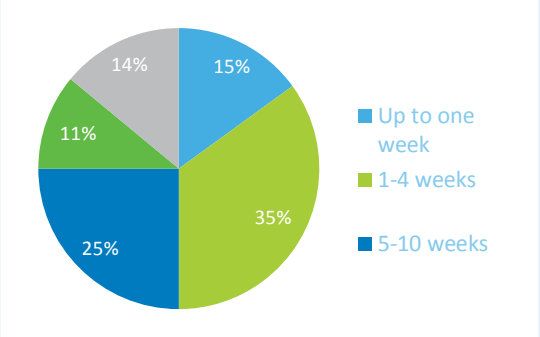
Les réseaux d'entreprise actuels doivent fournir des centaines d'applications d'entreprise stratégiques et rester suffisamment flexibles pour soutenir les innovations de productivité « à la vitesse des affaires », tout en évitant les cyberattaques et en assurant la conformité. Comme si cela ne présentait pas suffisamment de défis, l'environnement du réseau d'entreprise, lui-même, évolue rapidement à mesure que les entreprises étendent leurs data centers physiques pour adopter le cloud computing et les réseaux définis par logiciel afin de profiter de la flexibilité et des avantages économiques offerts par ces environnements.

Tout ceci entraîne une augmentation sans précédent de la taille et de la complexité de la politique de sécurité protégeant l'organisation, ce qui exclut toute possibilité de gestion manuelle. Le présent livre blanc examine la nouvelle réalité à laquelle sont confrontées les équipes de sécurité, de réseau et d'applications, les défis pour gérer la politique de sécurité dans un environnement en changement perpétuel et à complexité constante, ainsi que les solutions qui peuvent vous aider à gérer la sécurité à la vitesse de vos affaires.

Comprendre les défis à surmonter

Davantage d'applications et plus de complexité

Dans un récent sondage, AlgoSec a découvert que 32 % des participants géraient plus de 100 applications critiques en data center, tandis que 19 % en supervisaient plus de 200. Ces applications nécessitent généralement une architecture complexe, interconnectée et distribuée sur plusieurs niveaux, ainsi que des trajets de communication élaborés à travers d'autres applications, serveurs et bases de données, présents sur site ou sur des clouds privés et publics. De plus, cette infrastructure d'entreprise nécessite, aujourd'hui plus que jamais, davantage de pare-feu, de chiffrement et de points d'authentification, ce qui fait augmenter encore plus les demandes pesant sur les équipes de réseau et de sécurité.



Les équipes de réseau et de sécurité ne peuvent pas « juste » gérer les plus de 100 applications qu'elles ont à la fois et considérer qu'elles ont terminé. Il y a constamment des mises à jour et des changements à effectuer, de nouvelles applications à déployer, connecter et sécuriser pour les utilisateurs professionnels qui exigent qu'elles soient opérationnelles aussi vite que possible.

Ainsi, comme le sondage AlgoSec l'a montré, il faut plus de 5 semaines chez plus d'un tiers des entreprises pour mettre une nouvelle application en ligne et près de 60 % des entreprises ont déclaré qu'il leur fallait plus de huit heures pour traiter les changements de connectivité d'une application.

Figure 1 : Temps moyen pour déployer de nouvelles applications en data center. Extrait de l'enquête AlgoSec « Examining the Impact of Security Management on the Business ».

Des menaces plus coûteuses

Le nombre croissant d'applications complexes augmente la pression exercée sur les équipes IT, de même que la brusque augmentation du nombre des brèches dans les données, coûteuses et très médiatisées. Selon une récente enquête PwC, le coût moyen associé à une brèche dans les données pour une grande entreprise atteint 5,9 millions de dollars, ce qui place la sécurité en tête des préoccupations chez les cadres, les régulateurs et le conseil d'administration.

Dans le but de protéger le réseau et les données critiques contre les menaces internes et externes, de nombreuses organisations ont adopté une stratégie de défense en profondeur, une segmentation de leur réseau ou une combinaison de ces deux approches. La stratégie de défense en profondeur établit des couches de contrôle de la sécurité pour bloquer l'accès à différents endroits, tandis que l'approche par segmentation du réseau isole les dispositifs cruciaux et les données à haute sécurité dans des domaines séparés qui sont protégés avec des pare-feu spécialisés et une variété de points d'étranglement. Qu'une organisation choisisse une défense en profondeur ou une segmentation du réseau, une sécurité plus élevée signifie plus d'appareils sur le réseau, plus de complexité et plus de tracas pour la gestion chez les divisions IT.

Plus de cloud computing

Pour satisfaire la demande en termes de débit, capacité et diminution des dépenses, de nombreuses entreprises commencent à utiliser des plates-formes sur cloud pour leurs applications d'entreprise.

Si deux tiers des organisations récemment sondées par AlgoSec ont déployé ou prévoient de déployer des applications d'entreprise sur une plate-forme en cloud public au cours des 3 prochaines années, la majorité d'entre elles ont déclaré que l'extension de leur politique de sécurité d'entreprise au cloud public soulève d'importants défis. 80 % des participants ont indiqué qu'ils avaient besoin d'avoir une meilleure visibilité sur leur environnement sur site et sur le cloud public. Enfin, la plupart des entreprises n'ont qu'une très vague idée des contrôles de sécurité dont elles ont besoin, ainsi que de la façon de les intégrer et de les gérer dans leurs environnements hybrides.

Même si la division IT est préoccupée par les problèmes de sécurité sur le cloud, les développeurs et détenteurs d'applications d'entreprise adoptent souvent le cloud, en défiant la vigilance des équipes de sécurité et de réseau. Cette « IT de l'ombre » augmente la vulnérabilité de l'entreprise et place sur la division IT la responsabilité de limiter les risques liés à des applications dont elle ne connaît pas l'existence. Pour mettre fin à cette activité de l'ombre, la division IT doit évoluer de sa position de point d'étranglement pour devenir un facilitateur des affaires, capable de répondre rapidement aux requêtes des utilisateurs tout en conservant la sécurité.

Surmonter les défis posés par la gestion de la politique de sécurité

Dimensionnement de connectivité à prévoir pour les applications de data center

À mesure que de nouvelles applications sont ajoutées, ou que les besoins en connectivité de celles existantes évoluent, les administrateurs de la sécurité et de l'exploitation du réseau doivent pouvoir évaluer les règles sous-jacentes du pare-feu et les changements nécessaires et initier le bon flux de tâches à mettre en place pour la gestion des changements.

Toutefois, bien trop souvent, la documentation relative aux besoins en connectivité des applications fait défaut (ou n'existe pas), et de nombreuses organisations s'appuient encore sur des tableurs, des bases de données rarement mises à jour et sur la mémoire des membres de l'équipe. Ceci rend pratiquement impossible la tenue de discussions sérieuses concernant les changements nécessaires entre les détenteurs d'applications et les autres, qui ne parlent généralement pas la langue des ports et des protocoles.

Adopter une approche axée sur l'application pour la gestion de la politique de sécurité vous permettra de surmonter ces défis. Une analyse axée sur l'application et totalement intégrée à une solution de gestion de la sécurité peut automatiser les tâches liées aux changements et surmonter des problèmes classiques, tels que:

- Identifier l'impact des modifications du réseau proposées (migrations de serveur, nouveaux modèles de segmentation et de routage, par exemple) sur les applications de l'organisation.
- Identifier précisément et retirer les règles d'accès liées aux applications mises hors service, sans affecter l'accessibilité des autres applications.
- Déterminer l'impact des changements proposés des règles d'accès (en réponse à des menaces ou des vulnérabilités récemment découvertes, par exemple) sur les applications de l'organisation.
- Utiliser les exigences en matière de connectivité d'une application comme une couche d'abstraction pour masquer la complexité croissante des politiques de sécurité actuelles.
- Refermer le fossé de communication entre les différentes parties constituant le domaine IT

Garder le rythme de l'évolution des exigences commerciales

Les exigences commerciales évoluent à une vitesse effrénée dans l'environnement mondial actuel et les applications d'entreprise des organisations, ainsi que leur connectivité sous-jacente, doivent être modifiées dans leur lignée afin de soutenir les besoins commerciaux, tout en gardant une position de sécurité et en réduisant les risques.

Étant donnée l'extrême complexité d'un réseau et d'une infrastructure de sécurité, tout manquement à une gestion adéquate de ces changements peut entraîner des coupures et faire peser des risques sur la sécurité et les affaires. Parmi les facteurs contribuant à créer ce problème :

- Le manque de processus formel pour la gestion du changement.
- Une mauvaise communication entre les principaux responsables.
- Un manque de compréhension des risques commerciaux associés.

Une gestion efficace des changements dans la sécurité requiert une solution automatisée, axée sur l'application et associée à des processus formels. Il faut disposer de politiques et de procédures bien définies et clairement documentées, soutenues par des contrôles techniques automatisés qui fournissent visibilité, gestion et mise en application. La standardisation et l'automatisation du processus de changement de la politique de sécurité permet aussi d'obtenir un processus de gestion du changement plus fluide et assure la bonne entente de toutes les parties, plutôt que de supposer que tout le monde connaît ce dont les autres ont besoin ou ce qu'ils veulent. Au bout du compte, l'automatisation de la majeure partie du processus de changement de la sécurité réduit les erreurs, limite les risques et permet à la division IT de répondre « à la vitesse des affaires », et pas 11 semaines plus tard.

Comprendre les risques dans leur contexte commercial

Suite aux brèches de sécurité récentes qui ont fait la une de la presse, la sécurité est à présent la priorité numéro 1 des acteurs des entreprises. Pour adresser ce problème, les responsables de la sécurité et leurs équipes doivent trouver le moyen de faire prendre conscience aux acteurs des entreprises des risques liés à la sécurité IT pesant sur leur domaine d'affaires, et de les responsabiliser.

Les pratiques classiques de gestion des risques sont généralement très techniques et présentent les risques pour les serveurs, les adresses IP et d'autres éléments qui ne veulent pas dire grand chose aux responsables d'entreprise. Ici encore, les organisations auraient avantage à adopter une approche axée sur les applications, en associant et en hiérarchisant les risques selon le domaine des affaires.

Une méthode consiste à intégrer la gestion de la politique de sécurité aux analyseurs de vulnérabilité qui sont déjà en place dans l'organisation. Les organisations peuvent cartographier leurs vulnérabilités selon les applications de data center associées, y compris leurs serveurs et exigences complexes de connectivité. On peut alors attribuer un score aux vulnérabilités et à leur sévérité selon le serveur d'application et les regrouper par application pour fournir une vision globale du risque pesant sur l'entreprise. Ces scores doivent être mis à jour quand les flux de connectivité d'une application changent afin de garantir une vision à jour des risques liés à l'application, à tout moment.

Simplifier les audits et assurer une conformité continue

Plus de 400 réglementations avec 10 000 éléments de contrôle se chevauchant gouvernent la sécurité du réseau dans le monde. De plus, les organisations disposent de leurs propres directives internes, ainsi que de celles établies avec leurs partenaires, clients et sur leur secteur.

De nombreuses organisations doivent généralement passer plusieurs audits chaque année, ce qui utilise une portion significative des ressources IT de l'entreprise. Près des trois quarts des participants au sondage AlgoSec ont déclaré qu'ils avaient dépensé plus d'une semaine de travail d'un employé par an sur les audits de pare-feu et 17 % ont indiqué que les audits de pare-feu prenaient plus d'un mois de travail d'un employé chaque année. Des solutions qui fournissent une visibilité sur le réseau et les applications, qui vous permettent de réaliser l'audit, de démontrer ou de documenter votre sécurité et votre niveau de conformité à tout moment rendent le processus d'audit beaucoup plus simple et plus court.

Maintenir une politique de sécurité du réseau optimale

Quand une application est déployée, l'équipe de sécurité définit les droits d'accès et crée les règles du pare-feu. Quand une application est mise hors service, l'inverse se produit rarement. Ceci entraîne des surcharges de politiques, qui peuvent à leur tour ralentir les performances du pare-feu et rendre difficile le dépannage des problèmes de connectivité, mais surtout, exposer votre entreprise à des risques. Une solution automatisée de la gestion de la politique de sécurité, qui montre la topologie du réseau et présente une analyse du trafic et des flux d'accès au réseau selon les applications, peut rapidement identifier les règles inutilisées, inutiles, trop permissives et en double, ainsi que les problèmes de connectivité engendrés par un pare-feu spécifique.

Unifier la gestion des politiques de sécurité à travers les data centers d'un cloud hybride

Les organisations recherchent de plus en plus à étendre leurs data centers sur site vers des plates-formes IaaS (Infrastructure-as-a-Service, c.-à-d. infrastructure en tant que service) sur un cloud public pour optimiser leur agilité et réduire les dépenses. Toutefois, garantir l'accès du réseau dans un cloud public est un véritable défi en raison de la nature fragmentée et diverse des contrôles de la sécurité sur un réseau en cloud et du manque de visibilité sur l'ensemble de l'environnement hybride.

De plus, les mêmes défis rencontrés par la gestion de la sécurité du réseau sur site (mauvaises configurations, processus de gestion des changements manuel et sujets aux erreurs, conformité, pour n'en nommer que quelques uns) doivent également être surmontés dans l'environnement du cloud public.

Des solutions qui étendent la visibilité et qui sont capables d'unifier et d'automatiser la gestion de la politique de sécurité sur l'ensemble d'un data center hybride sont donc plus critiques que jamais pour assurer à leur organisation une sécurité et une conformité totales.

Améliorer la sécurité, la conformité et l'agilité des entreprises avec AlgoSec

Utilisée chez plus de 1,500 organisations dans le monde, AlgoSec Security Management Suite offre une solution intégrée et complète pour gérer les politiques complexes de sécurité du réseau, depuis la couche application d'entreprise jusqu'à l'infrastructure du réseau. Grâce à une visibilité puissante à travers les environnements physiques, virtuels et sur le cloud, la suite AlgoSec automatise et simplifie le processus complet de gestion des changements de la sécurité pour accélérer la mise à disposition des applications tout en assurant sécurité et conformité. Grâce à AlgoSec Security Management Suite, les utilisateurs peuvent:

- Comprendre et dimensionner facilement la connectivité d'une application pour accélérer la mise à disposition de l'application et minimiser les coupures.
- Traiter les changements de pare-feu 4 fois plus rapidement et éviter les mauvaises configurations et les remaniements.
- Évaluer de façon proactive l'impact des changements sur le réseau pour assurer la sécurité et la conformité continue.
- Simplifier et automatiser les audits de pare-feu internes et réglementaires, réduire leur durée et leurs coûts jusqu'à 80 %.
- Rationaliser la communication entre les équipes d'application, de réseau et de sécurité.
- Assurer une politique de sécurité plus étroite qui fournit une meilleure protection contre les cyberattaques.

AlgoSec Security Management Suite est composée de trois produits séparés, bien qu'étroitement intégrés: AlgoSec BusinessFlow, AlgoSec FireFlow et AlgoSec Firewall Analyzer.

AlgoSec BusinessFlow permet de dimensionner, entretenir et mettre hors service, en toute sécurité, la connectivité des applications d'entreprise. En cartographiant automatiquement les besoins en connectivité des applications sur l'infrastructure du réseau sous-jacent, BusinessFlow accélère la mise à disposition des applications, minimise les coupures et applique les politiques de sécurité et de conformité pour les data centers physiques, virtuels et sur le cloud.

AlgoSec FireFlow automatise le processus complet de changement de la politique de sécurité, depuis la conception jusqu'à la soumission, l'analyse proactive des risques, la mise en œuvre, la validation et l'audit. En éliminant toute spéculation grâce à un processus intelligent de gestion des changements, FireFlow permet aux équipes de sécurité et d'exploitation de gagner du temps, d'éviter les erreurs manuelles et de réduire les risques.

AlgoSec Firewall Analyzer donne une visibilité et une analyse complète des politiques complexes de sécurité sur le réseau à travers les environnements physiques, virtuels et en cloud. Il automatise et simplifie les opérations de sécurité, notamment le dépannage, l'audit et l'analyse des risques. Grâce à Firewall Analyzer, les équipes de sécurité et d'exploitation peuvent optimiser la configuration des pare-feu, routeurs, proxys Internet et l'infrastructure du réseau en liaison pour garantir la sécurité et la conformité.

À propos d'AlgoSec

AlgoSec permet aux organisations professionnelles et aux prestataires de services de gérer la sécurité à la vitesse des affaires. Grâce à son approche axée sur l'application, AlgoSec automatise et simplifie la gestion de la politique de sécurité à travers les environnements physiques, virtuels et en cloud afin d'accélérer l'accès aux applications tout en assurant la sécurité.

Plus de 1 500 organisations parmi les plus importantes du monde, dont 15 du classement Fortune 50, s'appuient sur AlgoSec pour rationaliser la gestion des changements, optimiser les configurations d'accès au réseau et les pare-feu, limiter les risques et assurer une conformité continue.

AlgoSec est une société profondément engagée dans le succès de chaque client et propose la seule garantie de remboursement du secteur.

Global Headquarters
65 Challenger Road,
Suite 320
Ridgefield Park
NJ 07660, USA
+1-888-358-3696

EMEA Headquarters
80 Coleman Street
London EC2R 5 BJ
United Kingdom
Tel: +44 207-099-7545

APAC Headquarters
10 Anson Road, #14-06
International Plaza
Singapore 079903
+65-3158-2120

AlgoSec.com