LA TRANSFORMATION NUMÉRIQUE DOIT INCLURE LA SÉCURITÉ

WHITE PAPER

Alors que les entreprises se réorganisent pour gagner en compétitivité sur le nouveau marché numérique, de nouvelles exigences relatives aux données rendent impératif un fonctionnement plus rapide et plus efficace de leurs réseaux. Collecter des données à partir de sources variées, y compris les nouveaux dispositifs IoT avec données cryptées, et les traiter pour produire et livrer des informations précieuses et concurrentielles, est la base de la nouvelle économie numérique.

Il n'est pas surprenant que les architectures réseau traditionnelles — basées sur les dispositifs réseau hérités accumulés au fil du temps et provenant de différents fabricants — ne soient pas conçues pour prendre en charge les exigences actuelles en termes de puissance, de flexibilité et d'efficacité. Si la plupart des entreprises ont à l'origine mis en place des solutions issues de dizaines de fabricants afin d'éviter un point de défaillance unique, cela dégrade aujourd'hui leur posture de sécurité en minimisant les capacités de corrélation des menaces et en rendant la gestion plus complexe.

Ces dernières années, les entreprises ont donc procédé au remplacement rapide de leur matériel réseau par des serveurs virtualisés et des infrastructures basées sur le cloud, et réduit le nombre de fournisseurs avec lesquels elles travaillent. Ce processus de consolidation permet non seulement de gagner en efficacité au niveau informatique et au niveau des datacenters, mais il réduit aussi les dépenses d'investissement et les coûts opérationnels. Moins de dispositifs achetés auprès de fournisseurs moins nombreux implique que des ressources informatiques limitées peuvent être concentrées sur la gestion des activités clés de l'organisation. La consolidation des fournisseurs réduit aussi le nombre de consoles de gestion à surveiller, améliore la visibilité et le contrôle, et permet une automatisation accrue.

Alors que de plus en plus d'appareils périphériques migrent vers le cloud, et que le réseau devient de plus en plus distribué et transitoire, les stratégies de sécurité traditionnelles, basées sur le périmètre, ont besoin d'évoluer. Paradoxalement, alors que la surcharge du réseau se réduit, le nombre de dispositifs de sécurité spécialisés ne cesse de se développer sur le réseau.

Deux facteurs entraînent l'expansion des dispositifs de sécurité et des fournisseurs dans l'entreprise.

Le premier est le fait que, tandis que le nombre de fournisseurs et de dispositifs physiques à gérer se réduit, le réseau lui-même devient plus complexe. Les données et les ressources s'étendent sur une variété de domaines, y compris les clouds public et privé, les terminaux mobiles et les bureaux à distance, et les réseaux eux-mêmes ne sont plus statiques. Les outils de sécurité traditionnels ont des difficultés à surveiller des réseaux dynamiques, réactifs et de plus en plus transitoires, sans parler de l'inspection et de la sécurisation d'un volume croissant de données, d'appareils et d'utilisateurs sur ces réseaux.

Le deuxième tient à l'évolution de la nature du cybercrime lui-même. Les attaques (avec le développement actuel des rançongiciels, par exemple) deviennent de plus en plus complexes et coûteuses. De plus, les nouvelles attaques en plusieurs étapes ont non seulement adopté l'apprentissage automatique et les techniques d'évasion sophistiquées, mais elles ciblent une variété de vecteurs d'attaque sur le réseau distribué, y compris une grande variété de terminaux et d'environnements cloud. Elles exploitent aussi les limitations inhérentes à beaucoup de déploiements actuels en se déplaçant latéralement dans toute l'organisation afin d'échapper à toute détection.

Pour répondre à ces difficultés, les organisations achètent et déploient des outils de sécurité spécialisés, conçus pour gérer les nouvelles menaces et pour fonctionner dans de nouveaux environnements, prenant en charge des éléments comme les hyperviseurs, les environnements cloud, les points d'accès et les terminaux. Cependant, ces solutions sont souvent plus ou moins les mêmes : des dispositifs isolés dont le déploiement, le réglage et la gestion requièrent des ressources supplémentaires.

Les difficultés qui en résultent sont prévisibles.

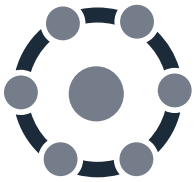
- **Une surcharge pour le service informatique** — Les dispositifs de sécurité exigent des réglages, des mises à jour et une gestion, et alors que les environnements réseau changent automatiquement pour s'adapter à des charges de travail, des volumes de données et des exigences de trafic fluctuants, les règles de sécurité doivent être mises à jour et modifiées pour assurer la sécurité de ces paradigmes réseau évolutifs. Le fait est que cela ne peut plus être fait manuellement. Chaque nouvel outil exige un technicien familiarisé avec ses configurations et son système d'exploitation, capable d'en adapter les réglages au segment de réseau qu'il est chargé de protéger, et de maintenir à jour ses données de sécurité et ses renseignements sur les menaces. Cela nécessite souvent un ajout de personnel que la plupart des organisations n'ont pas les moyens de s'offrir. Les outils de sécurité sont donc bien souvent sous-exploités, certaines données et certains segments de réseau sont souvent mal sécurisés et des cycles de mise à jour erratiques et imprévisibles laissent les dispositifs vulnérables ou moins efficaces.
- **Une gestion complexe** — Chaque solution de sécurité possède généralement sa propre console de gestion qui fournit uniquement un aperçu des outils et données qu'elle est est supposée contrôler. Multipliez ceci par une dizaine de fournisseurs de sécurité, ou plus, et vous obtenez un cauchemar de gestion logistique. Plus compliqué encore, ces dispositifs n'ont jamais été conçus pour partager leurs renseignements sur les menaces. Les équipes informatiques sont donc obligées de corréler manuellement les informations afin de découvrir les menaces plus sophistiquées d'aujourd'hui. Cela signifie que le temps entre la compromission de votre réseau et la découverte de la menace se mesure plus souvent en semaines qu'en minutes ou secondes qui vous permettraient de défendre efficacement vos actifs.
- **Des dispositifs isolés ne peuvent pas réagir comme un système** — Une fois la menace découverte, vous devez savoir d'où elle provient, depuis combien de temps elle est présente, quels dispositifs ont été compromis et comment l'éliminer. Cela signifie que vos solutions de sécurité doivent être capables de synchroniser une réponse coordonnée à toute menace détectée. Malheureusement, des dispositifs isolés ne peuvent pas faire cela; certains segments de votre réseau peuvent ainsi être négligés. Bien trop souvent, les environnements de cloud public ou privé demeurent une zone d'ombre en matière de sécurité.
- **Un manque de compétences en sécurité** — Pire encore, tout cela se produit à un moment où les professionnels chevronnés possédant la formation et les compétences en sécurité dont vous avez besoin, se font de plus en plus rares. Les experts estiment qu'il y a aujourd'hui dans le monde un million de postes non pourvus dans la cybersécurité, et ce nombre pourrait passer à 1,5 million en 2019.

UNE SÉCURITÉ AUTOMATISÉE À TOUS LES NIVEAUX

Comme les réseaux qu'elle doit protéger, la sécurité doit être repensée et modernisée. Pour prendre en charge les réseaux dynamiques d'aujourd'hui, la sécurité doit avoir une vue de tous les appareils présents sur le réseau, établir une politique au point d'accès et surveiller et protéger les données et les ressources qui se déplacent dans un environnement distribué, de l'IoT au Cloud, en passant par le réseau. Cela exige une approche architecturale ou structurée de la sécurité qui permet une intégration croisée, une collaboration sans faille et une adaptabilité automatisée.

Pour ce faire, vous devez commencer par remplacer vos dispositifs et plateformes de sécurité isolés hérités, par des outils conçus pour fonctionner ensemble, soit à l'aide d'un système d'exploitation commun, soit intégrés à partir de normes communes. Dans la mesure du possible, choisissez un fournisseur unique qui vous permette de disposer d'une gestion unifiée, de contrôler et de gérer de façon simplifiée les solutions déployées physiquement, virtuellement, dans le cloud et à des endroits distants, pour une orchestration et une application harmonieuses de vos politiques. Si ce n'est pas possible, recherchez des solutions qui prennent en charge les normes ouvertes, afin de pouvoir les intégrer en toute transparence dans votre cadre de gestion et de sécurité.

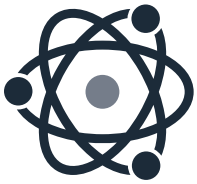
Des outils qui peuvent être combinés pour former une Security Fabric offriront toujours une meilleure visibilité et un meilleur contrôle que ceux qui fonctionnent uniquement de manière isolée. Ils peuvent activement collecter et partager des informations sur les menaces, afin d'améliorer la visibilité et les renseignements, améliorer la vision d'ensemble de la situation et permettre une réponse synchronisée aux attaques partout sur le réseau. Ce type d'approche permet aux organisations de répondre aux trois exigences de sécurité fondamentales des réseaux d'aujourd'hui :



LARGE

Tout déploiement de sécurité efficace doit couvrir l'intégralité de la surface d'attaque et répondre en temps réel à la fois aux menaces détectées et aux changements dynamiques du réseau. Les administrateurs réseau doivent avoir une visibilité sur l'ensemble de l'environnement, y compris les terminaux, les points d'accès, les dispositifs associés à l'IoT, les éléments du réseau, le datacenter, le cloud, et même les applications et les données elles-mêmes, au moyen d'un tableau de bord unique.

Une vue unifiée de l'entreprise étendue et de plus en plus élastique ne peut pas être bâtie autour de dispositifs isolés. Un cadre de sécurité basé sur des normes ouvertes permet aux solutions de fonctionner en tant que système unifié. Cette approche aide les administrateurs à relier les données, les applications, les dispositifs et les flux de travail, afin de repérer et de répondre aux menaces les plus sophistiquées d'aujourd'hui, qui pèsent sur l'entreprise distribuée.



INTEGRÉ

Beaucoup des menaces avancées d'aujourd'hui sont conçues pour échapper à la détection. Elles contournent les passerelles de sécurité en périphérie en se dissimulant dans le trafic crypté, en utilisant des attaques en plusieurs étapes qui semblent au départ inoffensives, en trompant les utilisateurs en les amenant à télécharger et à lancer des fichiers exécutables malveillants, ou en étant introduites directement dans le réseau par l'intermédiaire d'un appareil mobile infecté. Une fois à l'intérieur, elles se diffusent latéralement sur l'ensemble du réseau en observant et en imitant les modèles de trafic. Elles peuvent aussi rester dormantes pendant de longues périodes, attendant une commande ou des circonstances précises pour s'activer. Ainsi une infiltration réussie peut rester indétectée au sein d'un réseau compromis pendant des semaines, voire des mois, tout en rassemblant et exfiltrant des données sensibles.

Le fait que nombre d'outils de sécurité utilisés par les organisations sur leur réseau fonctionnent de manière isolée, est l'un des facteurs qui contribuent à ces difficultés. Ils ne voient que le trafic qui passe devant eux et ne peuvent pas partager ni corréler les renseignements sur les menaces pour avoir la vue d'ensemble nécessaire pour détecter ces menaces avancées.

Ce problème s'aggrave lorsque les données et les flux de travail se déplacent, par exemple entre des domaines traditionnels et multi-clouds. Bien trop souvent, les spécialistes de la sécurité sont obligés d'examiner des journaux sur des consoles séparées, puis de corréler manuellement les données afin de détecter les menaces avancées. Mais avec en moyenne plus de 30 produits dédiés différents fonctionnant sur un réseau d'entreprise, l'ampleur du défi dépasse les ressources dont disposent la plupart des équipes informatiques.

Ce dont les organisations ont besoin, c'est de dispositifs de sécurité conçus pour voir, partager, corréler et répondre aux menaces. Cela signifie que les outils de sécurité doivent être sélectionnés non seulement pour leurs performances et leurs fonctions, mais aussi pour leur capacité à fonctionner au sein d'un système de sécurité intégré. Pour ce faire, ils doivent utiliser un système d'exploitation commun ou être intégrés autour de normes ouvertes. Ils doivent aussi pouvoir fonctionner par l'intermédiaire d'un système d'analyse et de gestion centralisé, capable de corréler les données et d'orchestrer une réponse automatisée en cas de détection de menace. La sécurité conçue autour d'un cadre de dispositifs intégrés permet aux modèles et comportements complexes des menaces d'être plus facilement identifiés, d'isoler et de rétablir de façon dynamique les dispositifs ou segments de réseau compromis, de tracer les logiciels malveillants tout au long de la chaîne d'attaque, jusqu'à leur origine, et de faire fonctionner les outils de sécurité distribuée au sein d'un système offrant une évaluation de la fiabilité en continu sur l'ensemble de l'environnement réseau distribué.

AUTOMATISÉ

Étant donné qu'une attaque peut compromettre un réseau en quelques minutes, la visibilité à elle seule ne suffit pas. Une architecture de sécurité intégrée, qui relie les solutions de sécurité au sein d'une solution holistique, permet de répondre rapidement et de manière coordonnée aux menaces. Cela permet non seulement aux éléments de sécurité d'échanger rapidement des renseignements locaux et mondiaux sur les menaces, mais aussi de synchroniser automatiquement une réponse coordonnée afin d'isoler et de rétablir les dispositifs infectés, de mettre à jour les politiques, de rechercher des manifestations de menaces similaires, de renforcer automatiquement certains segments et points d'accès du réseau, de relever les indicateurs de violation de sécurité et de supprimer les logiciels malveillants.

Dans les environnements réseau actuels élargis, les solutions de sécurité doivent s'adapter automatiquement à des configurations réseau changeantes, en établissant et en appliquant de nouvelles politiques lorsque l'environnement protégé s'adapte à des besoins commerciaux fluctuants. En même temps, les mesures et contremesures de sécurité supplémentaires doivent être mises à jour ou fournies automatiquement lorsque de nouveaux dispositifs, charges de travail et services sont déployés. Cela nécessite aussi que la conformité, tout en restant cohérente, inclue des ajustements d'audit et de sécurité lorsque les réseaux changent.

LES AVANTAGES D'UNE SOLUTION SECURITY FABRIC

Les avantages d'une sécurité consolidée sont similaires à ceux qui résultent de la consolidation des ressources de votre réseau : une réduction des Opex et des Capex, une visibilité et un contrôle renforcés, une réduction de l'ampleur de vos déploiements de sécurité, une récupération plus rapide en cas d'incident et une conformité simplifiée et évolutive par rapport aux exigences réglementaires.

La solution Fortinet Security Fabric est la première qui offre une approche architecturale complète de la sécurité. Elle vous permet de connecter des solutions de sécurité distribuée au sein d'un cadre unifié afin qu'elles puissent s'adapter de façon dynamique à l'évolution de votre infrastructure informatique et défendre sa surface d'attaque en évolution constante et de plus en plus distribuée. De plus, sa conception autour de normes ouvertes vous permet d'intégrer des logiciels et des solutions issus de différents fournisseurs et vous fournit une protection homogène et des renseignements sur les menaces utiles en tous points de votre réseau, de l'IoT au Cloud.

FORTINET

France
TOUR ATLANTIQUE
11ème étage,
1 place de la Pyramide
92911 Paris La Défense
Cedex
France
Ventes: +33-1-8003-1655

SIÈGE SOCIAL INTERNATIONAL
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
États-Unis
Tél. : +1.408.235 7700
www.fortinet.com/sales

SUCCURSALE EMEA
905 rue Albert Einstein
06560 Valbonne
France
Tél. : +33 4 8987 0500

SUCCURSALE APAC
300 Beach Road 20-01
The Concourse
Singapour 199555
Tél. : +65 6513 3730

AMÉRIQUE LATINE — SIÈGE SOCIAL
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tél. : +1 954 368 9990

90833-0 0 FR

juillet 27, 2018 2:07 PM

Macintosh HD:Users:djarzabek:Documents:projekty:Fortinet:P-268377:05_DTP:fr-FR:wp-ent-fw-digital-transformation-A4_fr-FR