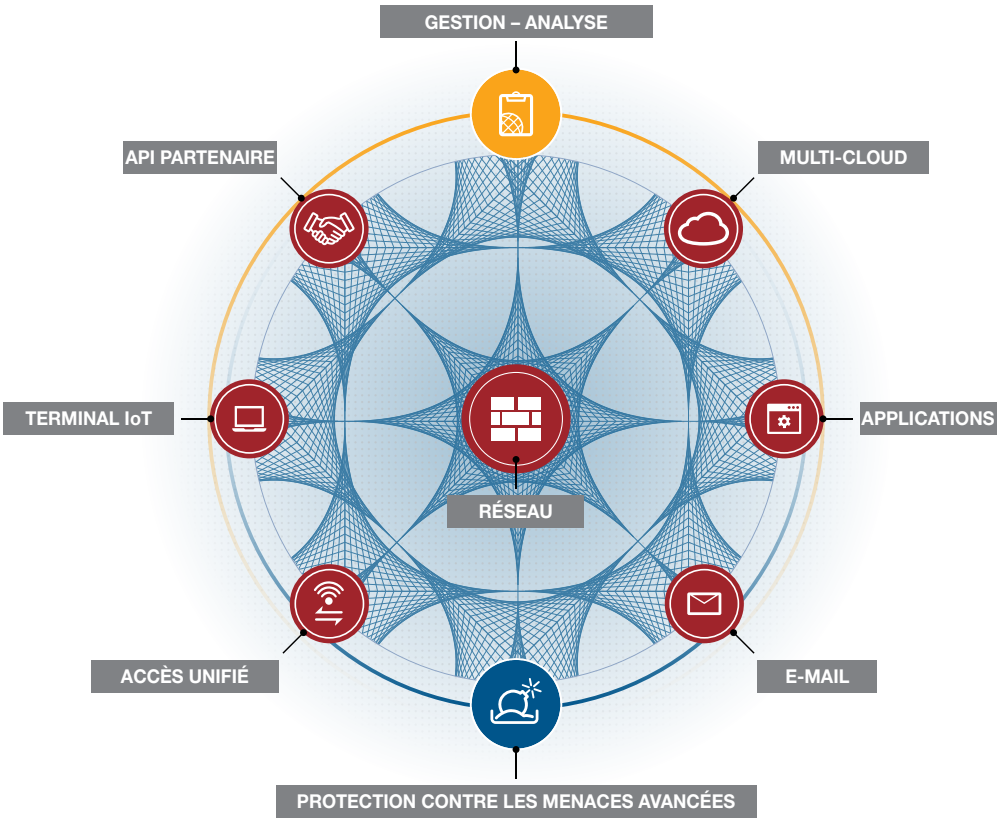
LA TRANSFORMATION DE LA SÉCURITÉ REQUIERT UNE SECURITY FABRIC

Ces dernières années, la croissance et l'adoption de nouvelles technologies ont transformé les entreprises, les gouvernements et même l'économie dans son ensemble. Elles affectent la façon dont les gens interagissent socialement, gèrent leurs finances, effectuent leurs achats, réalisent des transactions, reçoivent des informations et des divertissements, et même la façon dont ils s'orientent dans leur environnement. Cela a aussi radicalement modifié leurs attentes et leurs comportements dans leurs échanges avec les entreprises et les services, que ce soit en tant que clients ou en tant qu'employés.

Pour rester compétitives, les organisations ont dû répondre en redéfinissant la façon dont elles participent au nouveau marché numérique et satisfont aux demandes changeantes d'utilisateurs amateurs de technologie. Pour la plupart des organisations, la transformation numérique implique l'intégration de technologies numériques dans tous leurs domaines d'activité, ce qui entraîne des changements fondamentaux dans leur façon de fonctionner et d'offrir de la valeur à leurs clients.

Pour y parvenir, les sociétés doivent relier entre eux une variété de dispositifs, technologies et services, afin de créer un réseau unique intégré capable de s'étendre de façon dynamique et de s'adapter à l'évolution des exigences du marché et des utilisateurs. Cela signifie qu'elles doivent aborder des questions comme l'IoT, les SDN, l'OT et les environnements multi-clouds ; la prolifération des applications internes et tournées vers le client; une croissance sans précédent de la vitesse et du volume de données générées et consommées; l'expansion de charges de travail dépassant les limites du datacenter; et les attentes de la prochaine génération d'employés en termes d'agencement de leur vie personnelle et professionnelle sur les appareils mobiles de leur choix, associé à un accès instantané à toutes les données, à tout moment et depuis n'importe quel endroit.



Cette transformation numérique a simultanément beaucoup exigé des équipes informatiques jusqu'à un point de rupture et a élargi de façon exponentielle la surface d'attaque à protéger. Par exemple, les environnements multi-clouds signifient que les organisations doivent se préoccuper d'une surface d'attaque qui n'est pas toujours visible par leur service informatique, et la convergence des environnements informatiques et opérationnels expose désormais à de nouveaux risques des éléments comme les ateliers de fabrication, les systèmes de contrôle industriels et les infrastructures critiques. La prolifération des appareils liés à l'IoT dans ces environnements dont la sécurité repose exclusivement sur un réseau d'accès, complique les défis à relever.

Alors que les données commerciales critiques et propriétaires migrent vers le cloud ou sont gérées au moyen d'applications et de services basés sur le cloud, la croissance d shadow IT a tout simplement fait perdre à certaines organisations toute trace de l'endroit où se situent leurs données ou des mesures de sécurité en place pour les protéger. Le BYOD complique encore les questions de gouvernance des données puisqu'il permet aux utilisateurs d'accéder à des données critiques à partir d'emplacements publics et de les stocker sur leurs appareils personnels où leurs profils personnel et professionnel ne sont pas distincts.

LA TRANSFORMATION DE LA SÉCURITÉ

Alors que les forces commerciales et économiques entraînent une évolution rapide du réseau, les équipes de sécurité informatique peinent à suivre le rythme. Une part significative du problème tient au fait que la transformation numérique ne se produit pas sous la forme d'une seule activité intégrée. Au contraire, elle prend plutôt une forme organique de projets séparés qui déplacent les curseurs petit à petit. La tendance consiste à sécuriser chaque segment du réseau au fur et à mesure de son développement, à l'aide des outils de sécurité traditionnels plus facilement disponibles. Au final, cela aboutit à une infrastructure de sécurité complexe et largement hétéroclite, bâtie autour de solutions en silos issues de fournisseurs distincts.

Malheureusement, la complexité est généralement l'ennemie de la sécurité. Différents environnements exigeant différents formats de solution, il peut s'avérer difficile de se contenter d'un seul fournisseur, car les différences entre versions physique, virtuelle ou basée sur le cloud du même produit peuvent être importantes, quand elles sont tout simplement disponibles. En conséquence, les entreprises déploient aujourd'hui en moyenne plus de 30 solutions de sécurité différentes sur leurs réseaux distribués. Ces solutions de sécurité isolées, avec des interfaces de gestion séparées et aucun véritable moyen de rassembler ou de partager les renseignements sur les menaces avec les autres dispositifs du réseau, peuvent faire obstacle à la visibilité et limiter le contrôle.

La meilleure réponse à ces environnements réseau de plus en plus complexes est la simplicité. Cela exige une transformation de la sécurité capable de suivre le rythme de la transformation numérique. La transformation de la sécurité implique l'intégration de la sécurité dans tous les domaines de la technologie numérique, résultant en une architecture de sécurité cohérente et holistique qui permette un cycle de vie de la sécurité efficace, étendue à l'intégralité de l'écosystème des réseaux distribués. Cela inclut l'identification de la surface d'attaque, la protection contre les menaces connues, la détection des menaces inconnues, une réponse rapide et coordonnée aux cyber-incidents, et des évaluations en continu de la fiabilité.

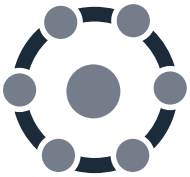
Pour être efficace, une stratégie de transformation de la sécurité doit inclure des informations collaboratives et une intégration système permettant le partage des renseignements sur les menaces locales et internationales entre les dispositifs et la coordination des réponses entre les solutions; l'orchestration de politiques de sécurité unifiées et de leur mise en œuvre ; une segmentation intelligente des environnements physique et virtuel pour une visibilité en profondeur du trafic passant latéralement sur le réseau, même

en cas d'environnements multi-clouds, et l'identification et la mise en quarantaine rapides des dispositifs infectés ; et l'automatisation du tri du bruit croissant sur le réseau, de la corrélation des informations sur les menaces, ainsi que la réponse en temps réel à toute menace repérée en tout point de la surface d'attaque étendue.

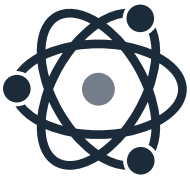
LA FORTINET SECURITY FABRIC

La solution Fortinet Security Fabric est une approche architecturale qui unifie les technologies de sécurité déployées sur le réseau numérique, y compris multi-cloud, les terminaux, les applications e-mail et Web, et les points d'accès réseau, en un seul système de sécurité intégré, grâce à la combinaison de normes ouvertes et d'un système d'exploitation commun. Ces solutions sont ensuite améliorées par l'intégration de technologies de protection contre les menaces et par l'unification de la corrélation, de la gestion, de l'orchestration et du système d'analyse.

Cette approche basée sur un tissu de sécurité s'articule autour de trois pièces maîtresses :



La largeur La visibilité et la protection doivent s'étendre à l'intégralité de la surface d'attaque numérique. Les données et les charges de travail passant par une variété de formats d'appareils et d'écosystèmes de réseau, les équipes informatiques doivent disposer d'une vue holistique des dispositifs, du trafic, des applications et des événements et avoir la possibilité de stopper une menace en tout point de sa chaîne d'attaque. Cette approche doit englober et unifier les réseaux physiques, l'IoT, les appareils et utilisateurs mobiles, ainsi que les environnements multi-clouds de plus en plus complexes, et ce pour des solutions IaaS et SaaS.



L'intégration. L'intégration des dispositifs à l'aide de normes ouvertes, de systèmes d'exploitation communs et de plateformes de gestion unifiées permet le partage et la corrélation des renseignements sur les menaces en temps réel. Ce cadre commun prend aussi en charge la détection coordonnée des menaces avancées grâce à des capacités d'analyse centralisées sophistiquées, difficiles voire impossibles à obtenir au moyen des déploiements de sécurité isolés traditionnels.

L'automatisation. Aujourd'hui, comme les activités commerciales, le cybercrime se développe à la vitesse du numérique. Le temps entre une violation du réseau et la compromission de ses données ou systèmes devra bientôt être mesuré en microsecondes. Les systèmes de sécurité doivent automatiquement fournir une évaluation continue de la fiabilité et apporter une réponse immédiate et coordonnée aux menaces détectées. Les environnements réseau actuels étant largement élastiques, la sécurité doit aussi pouvoir s'adapter de façon dynamique aux changements d'exigences et de configurations du réseau.

Pour proposer ces fonctionnalités, la solution Fortinet Security Fabric s'articule autour d'un certain nombre d'éléments clés :

- La sécurité du réseau. Alors que les réseaux continuent d'évoluer au-delà de leurs limites traditionnelles, les cyber-attaques sophistiquées s'en prennent à leur surface d'attaque étendue, à la recherche de fragilités et de points faibles. La gamme de firewalls Fortinet hautes performances, bâtie autour d'un ensemble consolidé et intégré de solutions de sécurité avancées, est la première ligne de défense essentielle de toute organisation.
- La sécurité multi-cloud. La majorité des organisations ont adopté une stratégie multi-cloud qui comprend de multiples fournisseurs IaaS et plus d'une dizaine de solutions SaaS différentes. L'expansion des données et des charges de travail dans un environnement cloud distribué complique prévention et détection dans le cadre d'une sécurité consolidée. Les solutions cloud physiques et virtuelles intégrées de Fortinet, alimentées par Fortinet Security Fabric, étendent la sécurité homogène à tout le déploiement de votre cloud distribué, y compris en étant les premières à fournir des solutions de sécurité avancées pour les cinq principaux fournisseurs de services cloud actuels.
- La sécurité des applications Web. Les applications Web non protégées ou vulnérables deviennent des points d'entrée courants sur votre réseau. Le Web application firewall de FortiWeb utilise les technologies de détection et de protection les plus récentes et les renseignements les plus avancés pour protéger vos applications Web des attaques sophistiquées.
- La sécurité des e-mails. Les e-mails restent le point d'entrée principal des logiciels malveillants pour infecter votre réseau. Les auteurs de spams et de phishing par e-mail utilisent des pièces jointes infectées, des liens malveillants et des fraudes sophistiquées pour tromper les utilisateurs et les pousser à exécuter un logiciel malveillant. En fait, l'e-mail a été le premier vecteur de rançonlogiciel en 2017. La passerelle de messagerie sécurisée FortiMail inspecte les e-mails entrants et sortants, bloque les messages et pièces jointes malveillants et empêche la violation d'informations sensibles.
- Un accès unifié sécurisé. La plupart des points d'accès sans fil offrent une connectivité, mais pas vraiment de sécurité. De plus en plus de dispositifs exigeant un accès sans fil au réseau, sécuriser les communications professionnelles, les données personnelles identifiables (DPI), les appareils mobiles et une variété d'utilisateurs, exige bien plus qu'un simple contrôle d'accès. Les solutions d'accès sécurisé de Fortinet offrent un accès haute performance associé à une sécurité et un contrôle des applications complet, pour un Wi-Fi plus sûr, totalement intégré à vos politiques et protocoles de sécurité réseau.

- La sécurité des terminaux. Les réseaux doivent prendre en charge un personnel hautement mobile et une diversité croissante de terminaux personnels connectés au réseau. Il n'est donc pas surprenant que ces dispositifs soient un autre point d'entrée couramment utilisé par les menaces. La difficulté tient dans le fait que les solutions de protection des terminaux ne partagent en général pas leurs renseignements sur les menaces avec le reste du réseau, ce qui peut faire obstacle à la détermination de l'infection ou non d'un appareil et ralentir la réponse à la menace s'il commence à se comporter bizarrement. FortiClient permet aux équipes informatiques d'intégrer une couche de sécurité des terminaux automatisée dans la Security Fabric, pour une protection du réseau plus rapide et plus complète.
- Une protection contre les menaces avancées. Aujourd'hui, les menaces avancées sont conçues pour échapper à la détection au moyen d'attaques en plusieurs étapes, de vecteurs d'attaque complexes et en observant et imitant les applications et le trafic légitimes. FortiGuard Threat Intelligence aide les sociétés à combattre ces menaces avancées en fournissant directement à ses solutions de sécurité, automatiquement et en temps réel, des renseignements sur les nouvelles menaces détectées, tandis que les solutions de Sandbox Fortinet détectent les menaces inconnues et isolent et inspectent tout fichier suspect détecté par les dispositifs de la solution Security Fabric.
- Gestion et analyse. Sur un réseau vaste et largement élastique, visibilité et contrôle sont plus importants que jamais. Les équipes informatiques doivent être en mesure de voir et de comprendre les menaces et les événements, quel que soit l'endroit où ils apparaissent sur le réseau distribué. Mais cela peut s'avérer extrêmement difficile pour les entreprises qui ont déployé des produits de sécurité isolés. Les solutions Fortinet d'enregistrement et de rapport, SIEM et de gestion centralisée de la sécurité recueillent et corrèlent les données à partir de vos produits de sécurité Fortinet et Fabric-Ready, vous procurant la visibilité et le contrôle granulaire indispensables à une gestion efficace des processus de sécurité et à l'orchestration de réponses automatisées.

UNE SOLUTION CONÇUE POUR L'ENTREPRISE NUMÉRIQUE D'AUJOURD'HUI

La transformation numérique est le plus gros challenge auquel les équipes de sécurité informatique aient jamais eu à faire face. Alors que l'évolution de l'informatique et des réseaux continue à remodeler les infrastructures commerciales critiques, les architectures et les pratiques, les organisations ont besoin d'une approche de transformation de la sécurité innovante, qui leur permette de prendre tous ces changements à bras le corps.

Une fois les solutions de sécurité traditionnellement isolées combinées dans un cadre Security Fabric unifié, les organisations peuvent examiner en profondeur leur réseau distribué afin de détecter les menaces avancées, s'adapter de façon dynamique à l'évolution de leur architecture réseau et au paysage des menaces, et profiter de l'évaluation en continu de la fiabilité dont toute entreprise numérique d'aujourd'hui a besoin, du cœur de leur système jusqu'au cloud.

Cliquez ici pour plus d'informations sur ce que Fortinet Security Fabric peut apporter à votre organisation.

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

WP-268377-0-0-FR
juillet 27, 2018 2:02 PM
Macintosh HD:Users:djarzabek:Documents:projekty:Fortinet:P-268377:05_DTP:fr-FR:wp-fortinet-security-fabric-A4_fr-FR