FORTINET

Les quatre principaux éléments à prendre en compte lors de la conception d'une architecture de sécurité

Fortinet Security Fabric, pour une sécurité globale, intégrée et automatisée

Table des matières

Synthèse

Les organisations adoptent rapidement des initiatives d'innovation numérique (IN) pour accélérer leurs activités, réduire les coûts, améliorer l'efficacité et offrir une meilleure expérience aux clients. Pour obtenir des résultats en matière d'IN tout en minimisant la complexité et en gérant efficacement les risques, les organisations ont besoin d'adopter une plate-forme de cybersécurité offrant une visibilité sur l'ensemble de leur environnement et les moyens de gérer facilement à la fois la sécurité et l'exploitation du réseau.

La Fortinet Security Fabric de Fortinet relève ces défis grâce à des solutions étendues, intégrées et automatisées qui permettent une mise en réseau axée sur la sécurité, un accès réseau à vérification systématique, une sécurité cloud dynamique et des opérations de sécurité basées sur l'intelligence artificielle (IA). Les offres Fortinet sont optimisées par un écosystème de produits tiers intégrés et transparents qui minimisent les lacunes dans les architectures de sécurité des entreprises tout en optimisant le rendement du capital investi (RCI) en matière de sécurité.

84% des responsables de la sécurité estiment que le risque de cyberattaques va augmenter.[1]

L’innovation numérique transforme toutes les industries

Dans tous les secteurs économiques du monde, l’IN est considéré comme un impératif pour la croissance des entreprises et l’amélioration de l’expérience client.[2]

Pour les responsables informatiques et cybersécurité et les prestataires de services cloud, l’innovation numérique se traduit par une série de changements dans leurs environnements réseau. Les utilisateurs sont de plus en plus mobiles et ils accèdent au réseau à partir de sites et de points d’extrémité qui ne sont pas toujours sous le contrôle des services informatiques d’entreprise. Ils se connectent également directement aux clouds publics pour utiliser des applications professionnelles clés, telles qu’Office 365. Les dispositifs IoT largement distribués, souvent sur des sites distants et non surveillés, sont plus nombreux que les périphériques contrôlés par l’homme. Enfin, les empreintes commerciales des prestataires de services cloud se diffusent dans de nombreuses succursales distantes, dont la plupart se connectent directement aux services cloud et cellulaires, contournant les datacenters des entreprises.

Tous ces changements rendent le concept d’un périmètre réseau défendable obsolète, obligeant les prestataires de services cloud à adopter une nouvelle stratégie de défense en profondeur à plusieurs niveaux.

77% des professionnels de sécurité déclarent que leur entreprise a migré des applications ou des infrastructures vers le cloud malgré des problèmes de sécurité connus.[3]

Migration des applications et des charges de travail vers le cloud

Presque toutes les entreprises ont commencé à déplacer certaines charges de travail et applications vers le cloud, ou du moins prévoient de le faire. Ces décisions sont souvent motivées par le désir de réduire les coûts et d'améliorer l'efficacité opérationnelle ainsi que l'adaptabilité en tirant parti de la flexibilité que le cloud offre.

Les fournisseurs de services cloud offrent un large éventail de modèles de déploiement possibles, du Software-as-a-Service (SaaS) à la plate-form-as-a-service (PaaS).

Se méfiant de la dépendance exclusive à l'égard d'un prestataire de services cloud et visant à déployer chaque application et charge de travail dans le cloud le mieux adapté, de nombreuses entreprises ont adopté une infrastructure multicloud. L'inconvénient d'une telle liberté de choix est la nécessité de connaître les particularités de chaque environnement cloud. En outre, elles doivent utiliser différents outils pour gérer l'environnement et ses clauses de sécurité, ce qui réduit la visibilité et nécessite l'utilisation de consoles de gestion multiples pour la gestion des politiques, la création de rapports, etc.

Les environnements cloud sont dynamiques : 74% des entreprises ont migré une application vers le cloud et l'ont ensuite replacée sur site.[4]

Une abondance de points d'extrémité dans des environnements multiples

Les points d'extrémité sont sans doute les nœuds les plus vulnérables du réseau du prestataire de services cloud. Les fournisseurs plus grands comptent des milliers d'employés, chacun utilisant plusieurs appareils professionnels et personnels pour accéder aux ressources réseau. Garantir une bonne cyber-hygiène et une sécurité à jour des points d'extrémité sur tous ces appareils est une tâche ardue. La prolifération des appareils IoT est encore plus décourageante. À la fin de 2019, le nombre d'appareils actifs dépassait 26,66 milliards et, en 2020, les experts estiment que ce nombre atteindra 31 milliards.[5]

Les appareils IoT sont présents dans de nombreux environnements d'entreprise. Ils offrent des expériences personnalisées aux clients des secteurs de la vente au détail et de l'hôtellerie, permettent de suivre les stocks dans la fabrication et la logistique, et de surveiller les équipements dans les usines ou les centrales électriques.

Souvent robustes et économes en énergie, les appareils IoT mettent l'accent sur les performances, mais fréquemment au détriment des fonctions de sécurité et des protocoles de communication sécurisés. Et contrairement à la plupart des appareils connectés au réseau, les équipements IoT sont généralement déployés sur des sites distants, à l'extérieur ou dans des installations sans personnel ou presque (comme les centrales électriques). L'équipement transmet fréquemment des données critiques et sensibles à des datacenters sur site et des services cloud depuis ces lieux peu sûrs.

84% des entreprises ont une stratégie multicloud. 81% des entreprises considèrent la sécurité comme un défi majeur du cloud.[6]

Présence accrue de l'entreprise sur les marchés et les zones géographiques distribuées

À mesure que les entreprises étendent leur présence mondiale en ouvrant de nouvelles installations, succursales et d'autres sites satellites, elles sont confrontées à des contraintes grandissantes en matière de bande passante WAN (wide-area network). Bien que les applications SaaS, la vidéo et la voix sur IP (VoIP) augmentent la productivité et permettent de nouveaux services, elles contribuent également à une croissance exponentielle du volume de trafic WAN.

Très fiable, le MPLS (commutation multiprotocole par étiquette) est la technologie de connectivité WAN de choix depuis de nombreuses années. Cependant, avec le MPLS, il est difficile d'optimiser l'utilisation de la bande passante WAN et de varier les niveaux de qualité de service en fonction des besoins des différentes applications. C'est pourquoi l'expansion des succursales et l'amélioration des services peuvent rapidement entraîner une explosion des coûts WAN.

Les organisations se tournent par conséquent vers le SD-WAN, qui utilise efficacement les MPLS, les connexions Internet et même les liaisons de télécommunications. De plus, le SD-WAN achemine dynamiquement chaque type de trafic sur la liaison optimale. L'adoption du SD-WAN a créé le besoin d'avoir un SD-WAN sécurisé, et la meilleure façon est de le proposer dans une plate-forme intégrant à la fois, les fonctionnalités réseau et sécurité.

De 2017 à 2019, on a constaté une augmentation de 73% du nombre d'entreprises victimes de violations de données à cause des applications ou des appareils IoT non sécurisés.[7]

Le SD-WAN offre des performances et une sécurité supérieures pour un coût inférieur à celui du MPLS.[8]

Les quatre éléments à prendre en compte lors de la conception d'une architecture de sécurité

Lorsque les entreprises poursuivent avec enthousiasme leurs initiatives d'innovation numérique, les implications pour la sécurité réseau sont souvent négligées ou minimisées. En fait, près de 80% des entreprises ajoutent d'autres innovations numériques plus rapidement qu'elles ne peuvent les protéger contre les cybermenaces.[9]

Les responsables informatiques doivent donner la priorité à quatre éléments lorsqu'ils conçoivent des architectures sécurisées pour leurs entreprises innovant dans le domaine numérique :

1. Comprendre l'expansion de la surface d'attaque

Les données sensibles peuvent potentiellement résider n'importe où, et elles peuvent circuler sur de nombreuses connexions hors du contrôle de l'entreprise. Les applications dans le cloud sont exposées à Internet de sorte que chaque nouvelle instance du cloud crée une nouvelle facette de la surface d'attaque de l'entreprise. Les appareils IoT étendent la surface d'attaque à des sites distants, sans ressources. Dans ces parties sombres de la surface d'attaque, les intrusions peuvent passer inaperçues pendant des semaines et des mois, et causer des dégâts dans le reste de l'entreprise. Les appareils mobiles et les périphériques appartenant aux utilisateurs apportent une certaine imprévisibilité à la surface d'attaque, car les utilisateurs se déplacent entre les sites de l'entreprise, dans les espaces publics et au-delà des frontières internationales. En fait, une vaste migration vers le cloud, ainsi que l'utilisation étendue des plates-formes mobiles et des appareils IoT sont des facteurs qui amplifient le coût d'enregistrement d'une violation de données de plusieurs centaines de milliers de dollars.[10]

61% des RSSI (déclarent avoir déjà mis en place d'importantes opérations cloud, IoT et mobiles.[11]

Jusqu’à 40% des nouveaux logiciels malveillants détectés un jour donné sont de type « zero-day » ou inconnus jusqu’alors.[12]

Cette surface d'attaque étendue et dynamique dissout le périmètre réseau autrefois bien défini et les protections de sécurité qui lui sont associées. Il est beaucoup plus facile pour les attaquants d'infiltrer le réseau, et une fois à l'intérieur, ils trouvent souvent peu d'obstacles pour se déplacer librement et sans être détectés vers leurs cibles. C'est pourquoi la sécurité dans les initiatives d'innovation numérique doit se faire à plusieurs niveaux, avec des contrôles sur chaque segment du réseau, si l'on part du principe que le périmètre sera violé tôt ou tard. L'accès aux ressources réseau doit, quant à lui, être basé sur le principe de privilège minimal et de vérification systématique.

Pour accompagner les initiatives d'innovation numérique, les équipes de sécurité des entreprises doivent déployer des protections pour 17 types de points d'extrémité différents.[13]

2. Il faut déterminer de quelle façon les cybermenaces évoluent

Le paysage des cybermenaces évolue rapidement, car les acteurs malveillants tentent de contourner et de vaincre les défenses traditionnelles de la cybersécurité. Jusqu'à 40% des nouveaux logiciels malveillants détectés un jour donné sont de type « zero-day » ou inconnus jusqu'alors.[14] Que ce soit en raison de l'utilisation accrue de logiciels malveillants polymorphes ou de la disponibilité de boîtes à outils de logiciels malveillants, l'augmentation des logiciels malveillants de type « zero-day » rend les algorithmes traditionnels de détection des logiciels malveillants basés sur les signatures moins efficaces. Par ailleurs, des acteurs malveillants continuent de recourir à l'ingénierie sociale en exploitant les méthodes de vérification statique utilisées dans les approches de sécurité traditionnelles. Des études révèlent que 85% des entreprises ont subi des attaques de phishing ou d'ingénierie sociale au cours de l'année écoulée.[15]

Les cybermenaces devenant de plus en plus sophistiquées, les incidents et les violations de données sont plus difficiles à détecter et à corriger. Entre 2018 et 2019, le temps nécessaire pour identifier et contenir une violation de données est passé de 266 à 279 jours.[16] Au-delà de la capacité à détecter et à prévenir une tentative d'attaque, les entreprises doivent également être capables d'identifier rapidement une attaque réussie et d'y remédier. Plus de 88% des entreprises ont déclaré avoir connu au moins un incident au cours de l'année écoulée, ce qui prouve que toutes les entreprises sont exposées à un risque d'attaque et que la cyber-résilience est essentielle.[17]

Un tiers des entreprises ont subi une violation de données critiques au cours de l'année dernière, pouvant entraîner des sanctions réglementaires.[18]

3. Simplifier un écosystème informatique de plus en plus complexe grâce à l'automatisation

Selon près de la moitié des DSI, la complexité accrue est le plus grand défi d'une surface d'attaque en expansion.[19] Cette complexité accrue est due au fait que de nombreuses entreprises s'appuient sur un ensemble de produits de sécurité individuels non intégrés. En fait, l'entreprise moyenne utilise plus de 75 solutions de sécurité distinctes.[20]

En raison de ce manque d'intégration de la sécurité, ces entreprises ne peuvent pas tirer parti de l'automatisation dans leur déploiement de sécurité. En fait, 30% des DSI considèrent le nombre de processus manuels comme un problème de sécurité majeur dans leur entreprise.[21] Sans automatisation de la sécurité, les DSI ont besoin de professionnels de cybersécurité plus qualifiés pour surveiller et sécuriser leur réseau.

Cependant, de nombreuses entreprises ne sont pas en mesure d'acquérir les talents dont elles ont besoin en matière de cybersécurité. Selon les estimations, plus de 4 millions de postes dans le domaine de la cybersécurité sont actuellement vacants, et ce nombre ne cesse de croître.[22] Ce manque d'accès aux talents nécessaires met les entreprises en danger, 67% des DSI déclarant que le manque de compétences en matière de cybersécurité les empêche de suivre le rythme du changement. [23]

Les attaquants comprennent bien ces défis et les utilisent à leur avantage.

4. Garder une longueur d'avance sur les exigences réglementaires croissantes

Le règlement général sur la protection des données (RGPD) de l'Union européenne (UE) et la loi californienne sur la protection de la vie privée des consommateurs (California Consumer Privacy Act ou CCPA) sont deux des réglementations les plus connues en matière de protection des données. Cependant, elles sont loin d'être les seules. Chaque État américain dispose actuellement d'une loi sur la notification des violations de données, et nombre d'entre eux adoptent des mesures de protection supplémentaires de la vie privée des consommateurs. Sous l'effet de la pression politique et sociale, les réglementations devraient se développer dans les années à venir, et les sanctions en cas de non-respect sont de plus en plus lourdes et fréquentes.

Les entreprises doivent également se conformer aux normes de l'industrie, et beaucoup ont du mal à le faire. Moins de 37% des entreprises réussissent par exemple leur audit de conformité provisoire à la norme de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard ou PCI DSS).[24] Comme la norme PCI DSS est remplacée par l'infrastructure de sécurité logicielle de l'industrie des cartes de paiement (PCI SSF), ces entreprises sont susceptibles de rencontrer des obstacles encore plus importants pour rester conformes.

La nécessité d'assurer et de maintenir la conformité réglementaire a des répercussions importantes sur la capacité d'une entreprise à atteindre ses objectifs de transformation de la sécurité — et donne également des informations sur la manière dont les organisations investissent dans les solutions technologiques. Par exemple, sur les 71% d'entreprises qui ont rapatrié des applications cloud vers des datacenters sur site, 21% l'ont fait pour maintenir leur conformité réglementaire.[25]

La Fortinet Security Fabric

La Fortinet Security Fabric relève les quatre défis de sécurité mentionnés ci-dessus en offrant une visibilité et un contrôle étendus de l'ensemble de toute la surface d'attaque numérique d'une entreprise afin de minimiser les risques. La Fortinet Security Fabric est une solution intégrée qui réduit la complexité créée par la prise en charge de plusieurs produits individuels et automatise le flux de travail pour augmenter la vitesse d'exploitation, tout en maintenant la productivité et la résilience des activités commerciales.

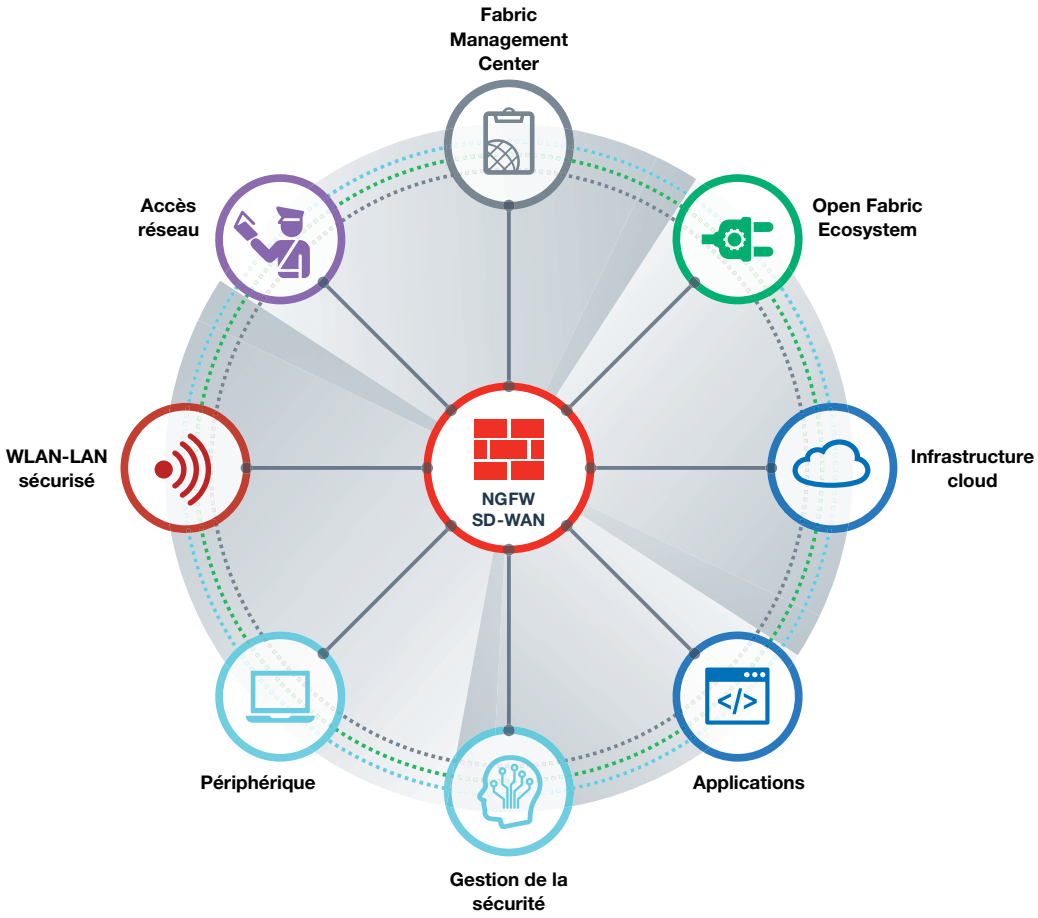

Schéma 1. La Fortinet Security Fabric permet à de multiples technologies de sécurité de fonctionner ensemble de façon transparente, dans tous les environnements, en exploitant une source unique de renseignements sur les menaces, via une console unique. Cela permet d'éliminer les failles de sécurité sur le réseau et d'accélérer les réponses aux attaques et aux violations de données.

Près de la moitié des RSSI considèrent l'intégration de la sécurité et l'amélioration de l'analyse comme une priorité majeure de leur stratégie technologique en matière de cybersécurité.[26]

Avec la Fortinet Security Fabric, les équipes peuvent :

Avoir une visibilité étendue et profonde de la surface d'attaque

Avec la plus large gamme de solutions de réseau haute performance et sécurisé pour les datacenters, les succursales et les petites entreprises, et pour les principaux prestataires de services cloud, la Fortinet Security Fabric s'adapte pour protéger chaque segment du réseau. Tous les composants sont configurés, gérés et surveillés à partir d'un seul système de gestion centralisé. En plus d'éliminer les silos associés aux infrastructures de sécurité des produits ponctuels, l'interface unique pour tous les composants de sécurité réduit la charge de formation d'un personnel en sous-effectif. Le système de gestion facilite également le déploiement sans contact des composants à distance, ce qui permet d'économiser des interventions sur place et de réduire davantage les coûts d'exploitation.

Disposer d'une architecture de sécurité véritablement intégrée

Avec tous les composants pilotés par le même système d'exploitation réseau FortiOS, la Fortinet Security Fabric permet une configuration et une gestion des politiques cohérentes ainsi qu'une communication en temps réel et sans effort à travers l'infrastructure de sécurité. Cela minimise les temps de détection et de réduction des risques des menaces, réduit les risques de sécurité résultant des erreurs de configuration et de la compilation manuelle de données, et facilite une réponse rapide et précise aux audits de conformité. Outre l'intégration des produits et des solutions Fortinet, la Fortinet Security Fabric comprend des API préconstruites pour plus de 70 partenaires « Fabric Ready », qui assurent une intégration complète à travers tous les éléments de la Security Fabric.

Les pare-feux nouvelle génération NGFW FortiGate offrent le meilleur rapport qualité-prix dans les évaluations tierces, tout en analysant le trafic chiffré. Ils atteignent des performances d'inspection SSL de 5,7 Gbits/s et bloquent 100% des fraudes.[27]

La réduction du temps de détection et de réponse peut entraîner une diminution de 25% des coûts globaux d'une violation de données.[28]

Disposer d'opérations et de réponse automatisées

En plus d'une intégration transparente, la Fortinet Security Fabric se place en tête du secteur en appliquant des technologies d'apprentissage automatique (AA) pour suivre l'évolution rapide du paysage des cybermenaces. La Fortinet Security Fabric comprend des fonctionnalités avancées d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR), ainsi que la détection proactive des menaces, la corrélation des menaces, les alertes de partage de renseignements, ainsi que la recherche et l'analyse des menaces.

Pour les opérations de réseau, la Fortinet Security Fabric fournit des flux de travail et des opérations automatisées pour aider à réduire les complexités dans l'ensemble de l'organisation et des déploiements, qu'ils soient sur site, dans le cloud ou dans les succursales.

Gestion des risques et poursuite des opportunités

L'innovation numérique permet aux entreprises d'accroître leur efficacité, de réduire leurs coûts et d'améliorer l'expérience de leurs clients. Cependant, les initiatives d'innovation numérique étendent et modifient également la surface d'attaque des entreprises, créant ainsi de nouveaux vecteurs d'attaque pouvant être exploités par les cybermenaces.

Pour les chefs de file de l'innovation numérique, il est primordial de reconnaître, d'accepter et de gérer correctement les risques. La Fortinet Security Fabric en est la base. Elle unifie les solutions de sécurité dans une interface unique, rend visible la surface d'attaque numérique croissante, intègre la prévention des violations basée sur l'intelligence artificielle, et automatise les opérations, l'orchestration et la réponse. En résumé, elle permet aux entreprises de créer de la valeur avec l'innovation numérique sans compromettre la sécurité, pour plus d'agilité, de meilleures performances et une plus grande simplicité.

[1] Nick Lansing, « Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources (Faire des choix difficiles : comment les RSSI gèrent des menaces croissantes et des ressources limitées) », Forbes et Fortinet, 2019.

[2] « The CIO and Cybersecurity: A Report on Current Priorities and Challenges (Le DSI et la cybersécurité : un rapport sur les priorités et les défis actuels) », Fortinet, 23 mai 2019.

[3] Jeff Wilson, « The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments (L'autoroute des clouds bi-directionnels : attitudes des utilisateurs sur la sécurisation des environnements hybrides et multi-clouds) », IHS Markit, 2019.

[4] Idem.

[5] Gilad David Maayan, « The IoT Rundown For 2020: Stats, Risks, and Solutions (Le bilan de l'IoT pour 2020 : statistiques, risques et solutions) » Security Today, 13 janvier 2020.

[6] « Rightscale 2019 State of the Cloud Report (Rapport sur l'état des clouds à l'échelle des droits 2019) », Flexera, 2019.

[7] Larry Ponemon, « Third-party IoT risk: companies don't know what they don't know (Risque d'IoT de tiers : les entreprises ne savent pas ce qu'elles ne savent pas) », ponemonsullivanreport.com, consulté le 4 février 2020.

[8] Nirav Shah, « SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019 (SD-WAN face à MPLS : pourquoi le SD-WAN est un meilleur choix en 2019) », Fortinet, 9 septembre 2019.

[9] Kelly Bissell, et coll., « The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study (Le coût de la cybercriminalité : neuvième étude annuelle sur le coût de la cybercriminalité) », Accenture Security et Ponemon Institute, 2019.

[10] « 2019 Cost of a Data Breach Report (Rapport sur le coût d'une violation de données en 2019) », IBM Security et Ponemon Institute, 2019.

[11] « The CIO and Cybersecurity: A Report on Current Priorities and Challenges (Le DSI et la cybersécurité : un rapport sur les priorités et les défis actuels) », Fortinet, 23 mai 2019.

[12] Selon les données internes de FortiGuard Labs.

[13] « 6 Obstacles to Effective Endpoint Security: Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders (6 obstacles à une sécurité efficace des terminaux : la désagrégation nuit à la visibilité et à la gestion des responsables de l'infrastructure informatique) », Fortinet, 8 septembre 2019.

[14] Selon les données internes de FortiGuard Labs.

[15] Kelly Bissell, et coll., « The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study (Le coût de la cybercriminalité : neuvième étude annuelle sur le coût de la cybercriminalité) », Accenture Security et Ponemon Institute, 2019.

[16] « 2019 Cost of a Data Breach Report (Rapport sur le coût d'une violation de données en 2019) », IBM Security et Ponemon Institute, 2019.

[17] Basé sur la recherche interne de Fortinet.

[18] Selon les données de recherche internes de Fortinet.

[19] « The CIO and Cybersecurity: A Report on Current Priorities and Challenges (Le DSI et la cybersécurité : un rapport sur les priorités et les défis actuels) », Fortinet, 23 mai 2019.

[20] Kacy Zurkus, « Defense in depth: Stop spending, start consolidating (La défense en profondeur : arrêter de dépenser, commencer à consolider) », CSO, 14 mars 2016.

[21] « The CIO and Cybersecurity: A Report on Current Priorities and Challenges (Le DSI et la cybersécurité : un rapport sur les priorités et les défis actuels) », Fortinet, 23 mai 2019.

[22] « Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019 (Stratégies pour la création et le développement d'équipes de cybersécurité solides : (ISC)² Étude sur la main-d'œuvre dans le domaine de la cybersécurité, 2019) », (ISC)², 2019.

[23] « CIO Survey 2019: A Changing Perspective (Enquête du DSI pour 2019 : une perspective en évolution) », Harvey Nash et KPMG, 2019.

[24] « 2019 Payment Security Report (Rapport sur la sécurité des paiements en 2019) », Verizon, 2019.

[25] Jeff Wilson, « The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments (L'autoroute des clouds bi-directionnels : attitudes des utilisateurs sur la sécurisation des environnements hybrides et multi-clouds) », IHS Markit, 2019.

[26] « Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources (Faire des choix difficiles : comment les RSSI gèrent des menaces croissantes et des ressources limitées) », Forbes et Fortinet, août 2019.

[27] « Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests (Validation indépendante de Fortinet Solutions : tests du groupe NSS Labs dans le monde réel) », Fortinet, janvier 2020.

[28] « 2019 Cost of a Data Breach Report (Rapport sur le coût d'une violation de données en 2019) », IBM Security et Ponemon Institute, 2019.

www.fortinet.fr

664959-0-0-FR

septembre 24, 2020 3:27 PM

ebook-considerations-security-architect