Livre blanc

Faire face aux menaces internes : Remodeler les déploiements de sécurité réseau

Introduction

Les brèches de sécurité IT touchent bon nombre d'entreprises. Le volume tout comme l'échelle et l'ampleur de ces cyberattaques forcent le monde de l'entreprise à repenser la façon de déployer, gérer et préserver la cybersécurité. Pour ce faire, il faudra totalement reconsidérer la perception et le modèle de fonctionnement de la cybersécurité.

Le modèle traditionnel fonctionnait sur la base de présomptions simples. Celles-ci ont abouti sur des modèles de déploiement qui, dans le monde actuel de la cybersécurité, s'avèrent lamentablement inadaptés à la lutte contre les logiciels malveillants et les brèches de sécurité. Certains de ces modèles sont exposés ci-dessous :

- **Sécurité en périphérie :** Le modèle de cybersécurité traditionnel était basé sur la présomption simple que tout ce qui se trouvait à l'intérieur du périmètre était protégé et que tout ce qui se trouvait à l'extérieur d'un réseau était exposé aux attaques externes. Ce périmètre de sécurité était composé en principe d'un pare-feu à la périphérie du réseau Internet et d'un logiciel de sécurité tel qu'un anti-virus au niveau du terminal de l'utilisateur. Cependant, la plupart des pare-feu et des logiciels de sécurité au niveau des terminaux identifient les logiciels malveillants à l'aide de règles et de signatures. A l'heure actuelle, bon nombre des cyberattaques exploitent des vulnérabilités zero-day. Pour ces vulnérabilités détectées, il n'existe pour l'instant aucun patch, signature ou règle. Par conséquent, il est de plus en plus difficile pour les solutions traditionnelles basées sur une défense en périphérie de repousser les logiciels malveillants ou les menaces.
- **Modèle simple basé sur la présomption de confiance :** Le modèle de cybersécurité traditionnel était simplement basé sur le fait que les employés étaient des utilisateurs de confiance et que toutes les autres personnes étaient proscrites. Cependant, à l'heure actuelle, les employés utilisent des ordinateurs personnels tels que les smartphones pour leurs besoins professionnels. La main d'œuvre est également composée d'employés, de consultants, d'entrepreneurs et de fournisseurs qui ont tous accès au réseau de l'entreprise et à ses ressources informatiques. C'est là que ce modèle simpliste s'écroule, sachant que la source d'une menace pourrait tout aussi bien être un employé ou un intérimaire. De plus, le modèle traditionnel reposait sur l'utilisation unique des équipements informatiques de l'entreprise. Cette notion supposait que ces équipements étaient dotés de la dernière version des logiciels et de l'anti-virus. Cependant, les employés d'aujourd'hui n'utilisent plus seulement les équipements informatiques de l'entreprise, mais également des équipements personnels tels que les ordinateurs portables, les tablettes, les smartphones et les téléphones afin d'améliorer leur productivité. En d'autres mots, la méthode « Apportez votre propre matériel » (BYOD) augmente la productivité, mais sonne le glas des modèles traditionnels.
- **Environnement statique :** Auparavant, les appliances de sécurité étaient déployées à des emplacements fixes. Cela inclut les pare-feu, les systèmes de détection d'intrusion/prévention (IDS/IPS) et d'autres systèmes de détection et de prévention des malwares. Ces systèmes prennent en charge un périmètre fixe ou surveillent un ensemble de goulots d'étranglement pour détecter des menaces là où l'on s'attend à du trafic. Cependant, avec la mobilité des utilisateurs, des dispositifs et des applications, les modèles de trafic sont beaucoup moins prévisibles. De plus, l'adoption du Cloud a repoussé les limites du périmètre étant donné la possibilité d'augmenter les capacités du Cloud sur demande. Cette nouvelle tendance fait du lieu de travail un environnement bien plus dynamique et bien moins prévisible, avec des limites et des goulots d'étranglement nettement moins prévisibles. De ce fait, il est beaucoup plus difficile d'identifier de façon cohérente et exhaustive les menaces grâce à des appliances de sécurité déployées de façon statique à des emplacements fixes.

Malgré l'effondrement des présomptions traditionnelles décrites ci-dessus, un grand nombre d'architectures de sécurité reposent encore sur celles-ci pour protéger les réseaux face aux risques de sécurité. En outre, la nature des cybermenaces a évolué de manière significative. Autrefois, quand un ver informatique ou un virus envahissait un réseau, la propagation était rapide et avait pour objectif de faire un maximum de dégâts en peu de temps. Cela permettait de détecter les vers et les virus plus rapidement compte tenu de l'empreinte et de la trace laissée par ces vers.

Les menaces d'aujourd'hui ont une envergure industrielle et sont beaucoup plus sournoises, plus sophistiquées et bien plus destructrices. On regroupe bon nombre d'entre elles sous l'appellation « Menaces persistantes avancées » (APT - Advanced Persistent Threats). Ces menaces sont la cause de nombreuses brèches de sécurité récentes. Elles ont tendance à utiliser une variété de méthodes sophistiquées pour compromettre le réseau et s'y installer pendant de longues périodes, d'où leur nom : Menaces persistantes avancées.

Anatomie d'une menace persistante avancée

Bon nombre des brèches de grande envergure passent par plusieurs phases et s'étendent sur de longues périodes qui vont de plusieurs semaines à plusieurs mois. Certains de ces modèles sont exposés ci-dessous:

1. **Reconnaissance :** Pendant cette phase, l'auteur de la menace ou le pirate passe un certain temps à comprendre l'activité en ligne de ses cibles potentielles et essaie d'identifier les moyens d'injecter le logiciel malveillant en fonction de cette activité. Par exemple, l'auteur de l'attaque identifie les sites Web bancaires ou les réseaux sociaux qu'un utilisateur visite régulièrement, les groupes d'intérêt auxquels il s'abonne, ainsi que ses habitudes en ligne. En fonction de ces informations, l'auteur en question établit un profil de la cible potentielle.
2. **Brèche initiale :** C'est la phase pendant laquelle l'utilisateur ou la cible est attaquée. Un email ou un article de blog invite un utilisateur ou un blogueur à cliquer sur un URL en lien avec ses habitudes et son profil. Une fois que l'utilisateur a cliqué sur le lien, il est redirigé vers un site Web où une vulnérabilité zero-day est téléchargée sur le système de l'utilisateur. C'est ce que l'on appelle un hameçonnage. Les attaques telles que les téléchargements furtifs (drive-by) sont également fréquentes. L'objectif est simplement d'injecter un logiciel malveillant dans le système de l'utilisateur. Dans bien des cas, l'empreinte de ce logiciel malveillant est assez réduite et n'est destinée qu'à créer une porte dérobée (backdoor) servant de canal de communication.
3. **Accès backdoor :** Une fois le système de l'utilisateur compromis par le logiciel malveillant initial, ce logiciel malveillant explore les accès cachés qui permettront de traverser le pare-feu, dans le but d'ouvrir un canal de communication avec un centre de commande et de contrôle situé n'importe où dans le monde. Une fois la communication établie, le téléchargement de logicielsmalveillants et/ou d'instructions peut commencer.
4. **Mouvement latéral :** Le logiciel malveillant se met ensuite à sonder et à se propager en interne, en recherchant d'autres systèmes vulnérables. Cependant, ce processus est sournois et maquille méthodiquement l'activité du logiciel malveillant tout en minimisant son empreinte. Cette activité peut prendre des semaines voire même plusieurs mois. En d'autres mots, la propagation latérale du logiciel malveillant est très lente et très discrète. Durant cette phase, d'autres "portes dérobées" peuvent être ouvertes dans l'éventualité où l'accès initial serait détecté et fermé.
5. **Collecte des données :** Une fois que le logiciel malveillant s'est propagé et a accédé à des ressources critiques dans l'infrastructure, il commence par identifier les données critiques pour filtrer ou enregistrer les données en vue de les exfiltrer
6. **Exfiltration :** Les données collectées sont ensuite exfiltrées en masse par les différentes portes dérobées. À ce stade, les informations de l'organisation sont gravement compromises. Le pirate peut demander une rançon, dévoiler des données confidentielles ou secrètes ou vendre des informations aux enchères.

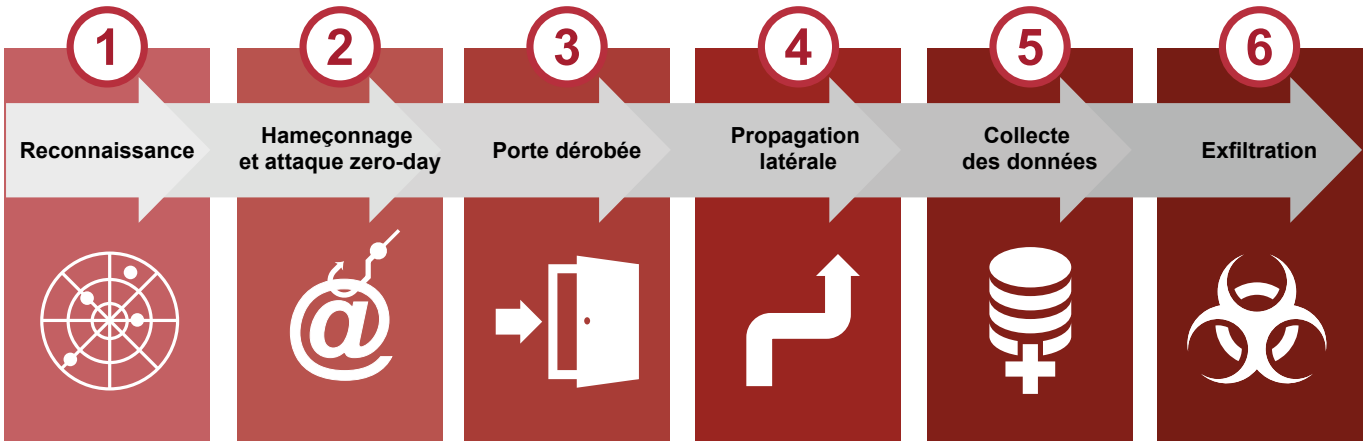

Figure 1 : Anatomie d'une menace persistante avancée

Dans bien des cas, l'organisation reste compromise même après l'exfiltration, ce qui la rend vulnérable à des attaques ou des brèches supplémentaires. Dans bien des cas, même lorsque la brèche a été détectée et la quasi-totalité des systèmes compromis a été nettoyée, certains systèmes restent compromis et indétectés. Ces systèmes compromis sont ensuite vendus sur des sites de vente de malware (Malware-as-a-service) où des individus ou des groupes peuvent acheter ces équipements infectés. Ce genre de service est devenu une industrie bien rodée, et fournit aux individus et aux organisations un moyen facile et bon marché de tirer parti de systèmes compromis pour lancer des attaques Dos, par exemple.

Une étude récente[1] auprès de 1200 entreprises dans 63 pays a révélé que 97 % des répondants avaient été piratés pendant la période d'étude. Parmi ces organisations, 75 % exerçait une activité de commande et de contrôle actifs. Une autre étude[2] indique que le nombre moyen de jours entre l'intrusion initiale et la détection de la brèche est de134 jours, ce qui indique que la brèche peut évoluer pendant des mois sans être détectée.

Tout ceci montre bien qu'il faut repenser les modèles de sécurité. Les entreprises ne peuvent plus se contenter de se protéger face aux menaces externes. Elles doivent au contraire renforcer leurs systèmes de détection des systèmes piratés et de confinement de malwares. Il est de plus en plus difficile d'identifier les systèmes compromis compte tenu des tendances IT actuelles.

Tendances IT affectant la sécurité

Évolution de la main d'œuvre et BYOD

Plusieurs nouvelles tendances IT affectent la capacité des entreprises à assurer sa sécurité interne. Comme nous l'avons mentionné plus haut, la nature même de la main d'œuvre a changé. En effet, les employés, consultants et sous-traitants sont tous considérés comme faisant partie de la main d'œuvre de l'entreprise. Cela complique le travail des équipes IT, qui ne peut plus aujourd'hui baser ses contrôles sur les rôles. La tendance du BYOD et la consumérisation de l'IT ont largement affaibli les contrôles stricts que les équipes IT effectués sur les PC, ordinateurs portables, téléphones mobiles et autres dispositifs utilisés par la main d'œuvre pour améliorer sa productivité.

Augmentation du trafic est-ouest

L'autre changement majeur s'opère actuellement dans le centre de données, où le trafic évolue à présent d'est en ouest, étant donné que les serveurs et les machines virtuelles communiquent entre eux et avec les systèmes de base de données, les systèmes de stockage et les autres applications résidant dans le centre de données. Le trafic est-ouest n'atteint normalement jamais le cœur du réseau où l'inspection de sécurité peut détecter les malwares ou les menaces présentes dans ce trafic, par exemple les systèmes IPS/IDS. De plus, le volume de trafic est-ouest prend aujourd'hui le pas sur le trafic nord-sud, qui correspond au trafic entrant et sortant de l'Internet. Cela permet à un malware qui a pénétré un serveur plus ancien ou non mis à jour de se déplacer latéralement dans le centre de données sans être détecté par les systèmes de sécurité visant à intercepter et inspecter le trafic nord-sud (voir la figure 2).

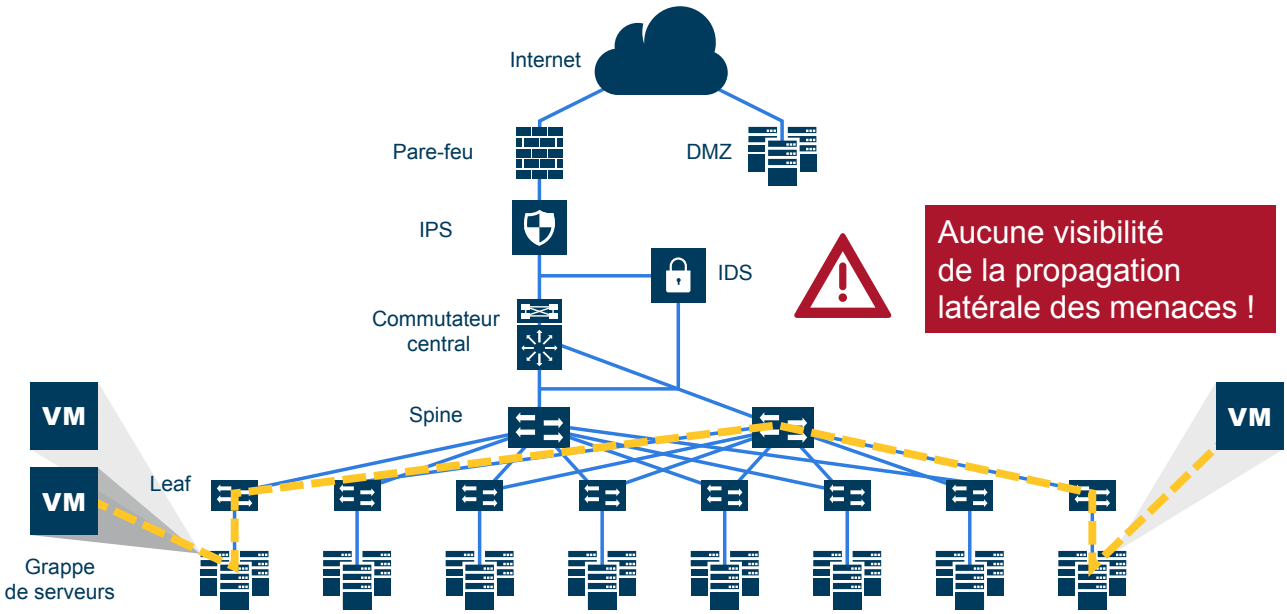

Figure 2 : Trafic est-ouest dans les centre de données

[1]FireEye. 2015. Maginot revisited: More Real-World Results from Real-World Tests. https://www2.fireeye.com/WEB-2015RPTMaginotRevisited.html
[2]Trustwave. 2014. Global Security Report. https://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf
[3]Wiener, Janet and Bronson, Nathan. "Facebook's Top Open Data Problems." Web blog post. research.facebook.com, Sept. 2014.

A titre d'exemple, Facebook exécute 1 million de tâches MapReduce par jour.3 Cela signifie qu'un trafic réseau significatif demeure dans le centre de données. Si la plupart des entreprises sont bien loin d'un tel volume, c'est l'utilisation croissante des Big Data par les grandes ou moyennes entreprises qui est la cause de ce changement dans les modèles de trafic des centres de données. Autre exemple, l'adoption de l'infrastructure de bureau virtuel (VDI - Virtual Desktop Infrastructure) par plusieurs entreprises, dont les systèmes d'exploitation de bureau sont à présent hébergés dans le centre de données. En conséquence, le trafic serveur-client qui représentait auparavant du trafic nord-sud et traversait le cœur du réseau ainsi que des goulots d'étranglement bien définis est devenu un trafic est-ouest entre les bureaux virtuels et les applications, tous désormais hébergés dans le centre de données. Tout ce trafic échappe au contrôle des appliances de sécurité qui n'ont pas accès à ce trafic de réseau.

Mobilité

La mobilité accentue la difficulté de protéger les réseaux modernes. Les utilisateurs, les dispositifs et les applications sont aujourd'hui tous mobiles. Par exemple, une application conditionnée comme une machine virtuelle peut être déplacée par un simple clic de souris, et même de manière complètement automatique entre des baies, des rangées, des pods ou même sur plusieurs centres de données. Tout cela sans aucune intervention de l'équipe de sécurité. Une appliance de sécurité telle que le système IDS ou IPS connectée directement à un centre de données via un simple lien et centrée sur l'inspection du trafic applicatif peut être inefficace si l'application proprement dite est déplacée vers un emplacement qui n'est pas connu de l'équipe de sécurité. En d'autres mots, l'emplacement devient de moins en moins important quand on déploie des solutions de sécurité. Il en va de même à la périphérie du site, où les utilisateurs et les dispositifs sont mobiles.

Usage croissant du chiffrage

Enfin, les technologies de chiffrage comme le SSL sont de plus en plus utilisées dans les entreprises. Même si le chiffrage des données mobiles peut offrir une protection contre les regards indiscrets, il crée en parallèle des canaux de communication protégée qui peuvent également être utilisés par les malwares sous couvert de confidentialité. Bon nombre d'appliances de sécurité ne décèlent pas le trafic chiffré et le chiffrage est donc de plus en plus utilisé par les pirates informatiques. Parallèlement, les appliances de sécurité capables d'inspecter le trafic chiffré SSL voient leurs performances diminuer, étant donné les nombreuses ressources nécessaires au déchiffrage SSL. Un rapport de Gartner4 prévoit que d'ici 2017, plus de 50 % des attaques réseau utiliseront le trafic chiffré pour contourner les contrôles.

La combinaison de ces facteurs, c'est-à-dire la nature sophistiquée et évoluée des menaces, l'évolution des modèles de trafic réseau, la mobilité, l'utilisation croissance des technologies SSL et de chiffrage de la part des malwares, ainsi que l'utilisation de modèle de sécurité obsolètes contribue à créer un climat propice aux brèches.

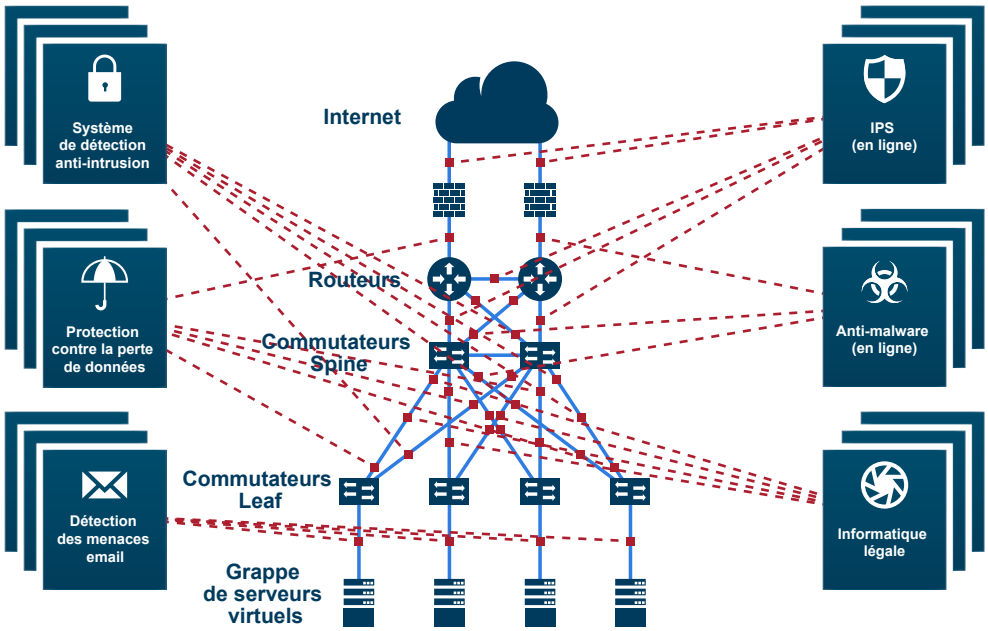

Figure 3 : Approche ponctuelle et non structurée du déploiement de la sécurité

[4]FD'Hoinne, Jeremy and Hils, Adam. 'Security Leaders Must Address Threats From Rising SSL Traffic'. Gartner Report, 9 Dec 2013..

Comment relever le défi

Pour mieux relever ce défi croissant, il faut revoir les hypothèses de confiance traditionnelles en matière de cybersécurité. Les stratégies de sécurité modernes doivent être basées sur l'hypothèse que ces brèches sont inévitables. En d'autres mots, il faut insister davantage sur la détection et le confinement des brèches provenant de l'intérieur, en marge d'une prévention bien rodée. Le réseau étant le principal moyen de relier l'environnement physique, virtuel et Cloud, le trafic réseau s'impose à présent comme une fenêtre permettant aux entreprises de détecter les malwares et les menaces informatiques. De nombreux fournisseurs de solutions de sécurité l'ont bien compris, et analysent le réseau pour détecter les menaces, les anomalies et le mouvement latéral des malwares. Cependant, aussi sophistiquées ces solutions soient-elles, leur performance n'équivaut qu'au type de trafic réseau qu'elles détectent.

L'approche de surveillance héritée

L'approche traditionnelle consistait à connecter les appliances de sécurité directement au réseau au moyen d'un port TAP ou d'un miroir/port SPAN sur un commutateur/routeur de réseau. Fournir un meilleur accès au trafic réseau revenait à déployer des appliances de sécurité réseau supplémentaires dans plus d'emplacements sur le réseau. Cependant, la nature multi-dimensionnelle de la sécurité se prête à l'utilisation de différents types de solutions de sécurité réseau destinées à améliorer la couverture réseau. Ce procédé pose plusieurs problèmes lors du déploiement de ces solutions de sécurité (voir la Figure 3), qui incluent notamment :

- Opposition entre les différentes appliances de sécurité tentant chacune d'accéder au trafic à partir des mêmes points du réseau. En d'autres mots, connecter directement une appliance au réseau TAP ou à un port miroir/SPAN restreint l'accès au trafic à une seule appliance.
- Déséquilibre entre la capacité de traitement des appliances de sécurité et le volume de trafic que l'appliance de sécurité doit traiter.
- Zones d'ombre et visibilité partielle du trafic Il se peut que les appliances de sécurité connectées à des points spécifiques du réseau ne puissent pas voir le trafic d'autres parties du réseau, ou le trafic des utilisateurs ou applications déplacées sur ces parties du réseau.
- Augmentation du nombre de faux positifs. Davantage d'appliances de sécurité signifie davantage de faux positifs pour les applications de sécurité sujettes à ce problème
- Les coûts des outils augmentent rapidement tandis qu'ils prolifèrent sur le réseau avec pour résultat une gestion de plus en plus complexe.
- Perturbations du réseau à cause des nouveaux déploiements passant du mode de monitoring hors bande au mode de protection en ligne.

Une plateforme de sécurité en guise de nouveau modèle pour les déploiements de sécurité

Alors que l'industrie tend à converger vers la détection de malwares à l'intérieur des réseaux, la sophistication des solutions de sécurité devient un problème majeur. Il n'y a pas eu beaucoup de réflexions quant à l'architecture de déploiement de ces solutions, raison pour laquelle nous sommes aujourd'hui confrontés aux différents défis décrits ci-dessus. C'est un domaine qui a été extrêmement négligé. Pourtant, la détection de malwares et de brèches dans le réseau est essentielle. Pour venir à bout des problèmes ci-dessus, une approche structurée reposant sur une plateforme est nécessaire. Elle doit offrir la visibilité du trafic nécessaire à une multitude d'appliances de sécurité selon un modèle évolutif, pervasif et rentable. La solution doit englober les composants suivants :

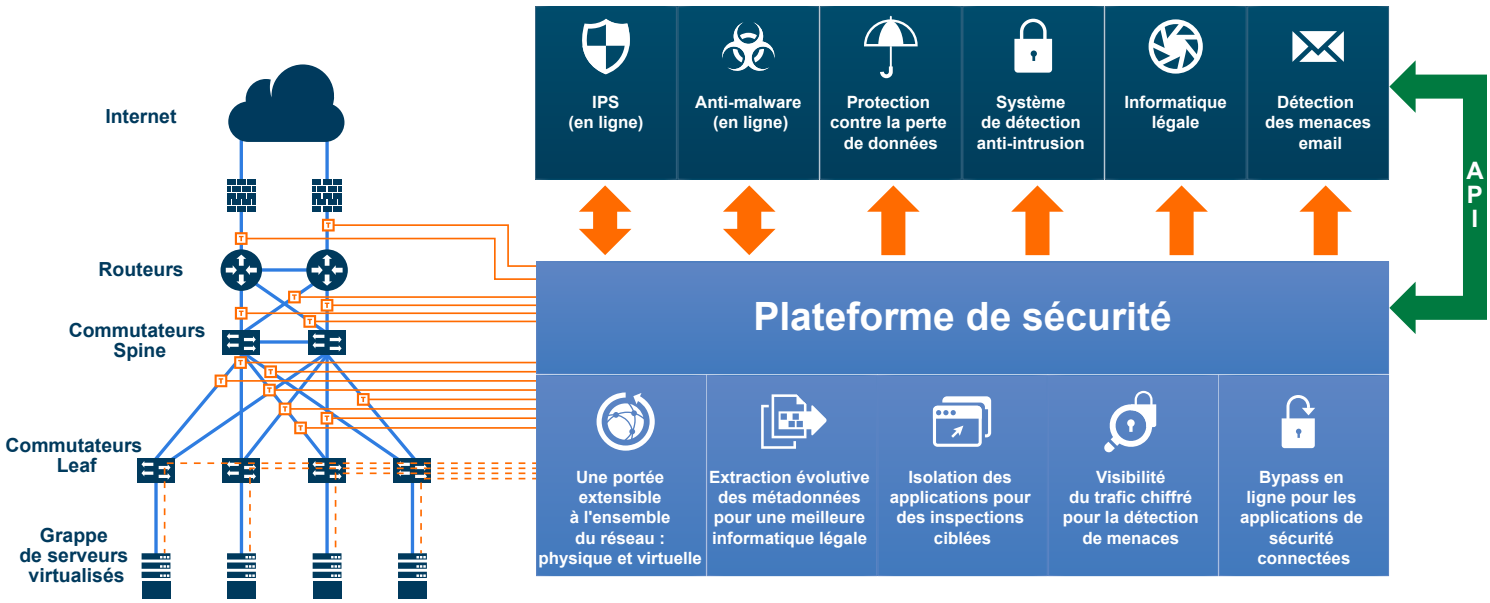

Figure 4 : Composants clés d'une plateforme de sécurité

- Offrir en permanence une parfaite visibilité du trafic dans des environnements physiques et virtuels, même lorsque les utilisateurs, les appareils et les applications sont mobiles.
- Éliminer les hésitations quant à l'emplacement adéquat des solutions de sécurité, en réduisant la dépendance liée à l'identification des goulots d'étranglement au sein du réseau, en particulier dans les environnements dynamiques d'aujourd'hui, caractérisés par l'utilisateur/le dispositif/l'application.
- Fournir une solution capable de crypter les communications chiffrées de manière à ce que les outils de sécurité puissent détecter les malwares qui exploitent les canaux de communication chiffrées, tout en veillant à ce que les informations sensibles ne soient pas compromises.
- Offrir la capacité d'envoyer uniquement les flux de trafic pertinents à chaque appliances de sécurité spécifique. Par exemple, une solution de sécurité de messagerie n'a pas besoin de voir le trafic YouTube. N'envoyer que le trafic pertinent permet aux solutions de sécurité de fonctionner de manière plus efficace et de ne pas utiliser inutilement de la largeur de bande et des ressources.
- Générer des renseignements de flux et de sessions détaillés sur la base du trafic réel et non pas seulement sur un échantillon du trafic.
- Prendre en charge les déploiements de sécurité réseau en ligne et hors bande à partir de la même plateforme, tout en étant capable d'équilibrer la charge des appliances de sécurité à la fois en ligne et hors bande ainsi que de contourner les appliances de sécurité en cas de panne.

Une plateforme de sécurité capable de résoudre les problèmes ci-dessus offre une solution puissante capable de déployer un vaste panel de solutions de sécurité et de transcender les modèles de déploiement traditionnels. Une telle plateforme permet de visualiser le mouvement latéral des malwares, accélérer la détection des activités d'exfiltration, et réduire ainsi les frais généraux, la complexité et les coûts associés aux déploiements de sécurité (Voir la figure 4). Face aux cybermenaces sophistiquées qui touchent aujourd'hui le monde de l'entreprise, il ne suffit plus de se concentrer exclusivement sur les applications de sécurité. Il faut dorénavant veiller à déployer ces solutions de façon optimale et à bénéficier d'un accès permanent aux données pertinentes. A cet égard, une plateforme de sécurité est la pierre angulaire de toute stratégie de cybersécurité.

GigaSECURE en tant que plateforme de sécurité

GigaSECURE® est la plateformede sécurité signée Gigamon. La plateforme GigaSECURE se connecte au réseau, aux infrastructures physiques et virtuelles et envoie du trafic à toutes les applications qui le demandent. Les appliances de sécurité se connectent à la plateforme GigaSECURE, quelle que soit la vitesse de connexion de l'interface, et reçoivent en conséquence un flux de trafic haute-fidélité et pertinent provenant de l'infrastructure du réseau. GigaSECURE prend également en charge l'extraction des métadonnées du trafic réseau, et est capable d'exporter des données de flux vers différents outils de sécurité à des fins d'analyse. Voir la Figure 5.

GigaSECURE prend en charge un éventail de solutions de sécurité pouvant être hébergées hors du réseau de production pour détecter les malwares et leur propagation latérale, détecter les activités d'exfiltration, publier des résultats d'analyse, et mener diverses initiatives de sécurité. Elle permet également de déployer diverses solutions de sécurité devant être alignées dans le réseau afin de protéger celui-ci face aux menaces détectées. Les solutions de sécurité en ligne sont habituellement capables de prendre des mesures préventives en temps réel afin de détecter les menaces, les malwares et les comportements irréguliers. GigaSECURE est capable de prendre en charge les déploiements en ligne et hors bande. GigaSECURE fournit une protection complète contre les défaillances et des fonctions de distribution de charge. Elle est compatible avec plusieurs modes de déploiement en ligne.

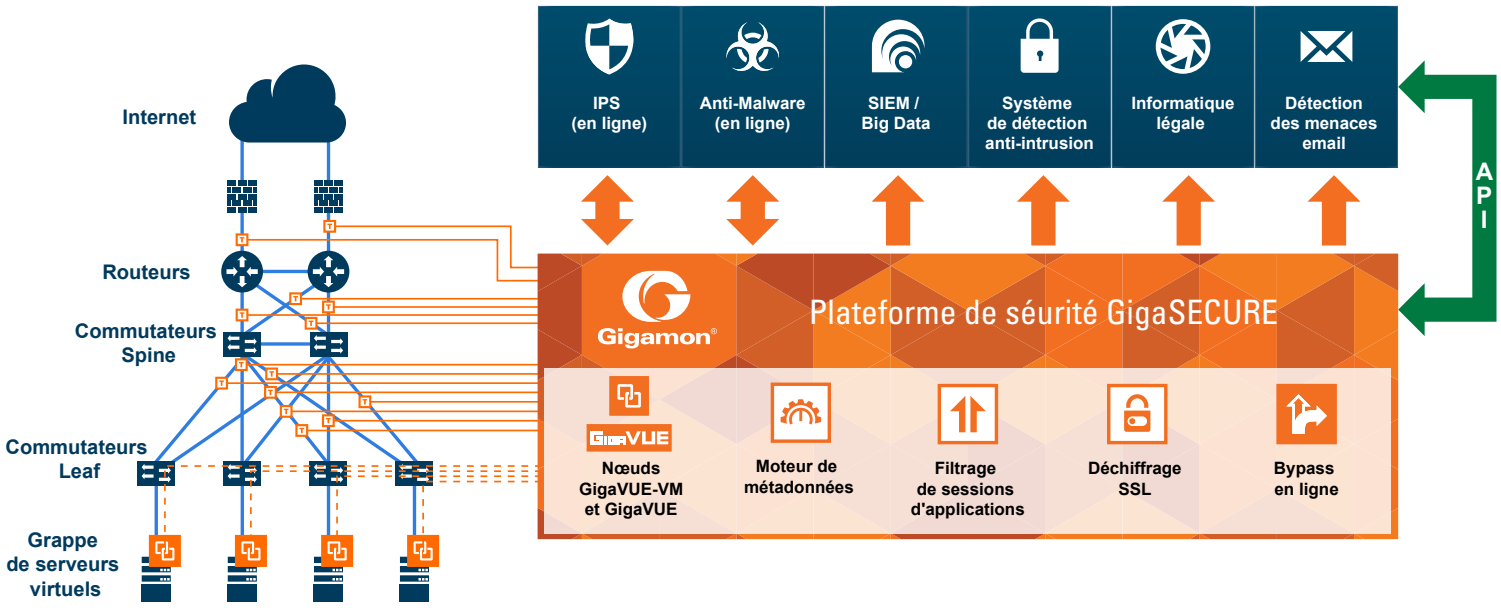

Figure 5: GigaSECURE Security Delivery Platform

Composants de la plateforme

GigaSECURE est composée de nœuds de visibilité et est basée sur la technologie GigaVUE OS™ associée à la technologie Flow Mapping® brevetée, aux fonctions d'intelligence de trafic optimisées par GigaSMART® et à un contrôleur de grille (GigaVUE-FM). Ces fonctions sont décrites ci-dessous :

- **Nœuds de visibilité virtualisés :** GigaVUE-VM est un nœud virtualisé et un outil de visibilité qui représente le trafic sous forme de charges de travail virtuelles. La solution GigaVUE-VM est capable de surveiller des machines virtuelles tandis qu'elles se déplacent d'un serveur à l'autre, et d'appliquer des politiques Follow-the-VM (Suivre la machine virtuelle) afin de veiller à ce que le trafic applicatif soit toujours envoyé aux outils de sécurité, même lorsque les machines virtuelles se déplacent.
- **Évolutivité et nœuds de visibilité rentables :** La gamme de nœuds de visibilité GigaVUE TA ainsi que le système d'exploitation GigaVUE-OS, utilisés en conjonction avec les commutateurs Ethernet Whitebox, offrent un moyen rentable de bénéficier d'une visibilité horizontale. Grâce à la technologie Flow Mapping®, ces nœuds fournissent des fonctions de recoupement, de filtrage et de réplication sophistiquée à un prix rentable pour aboutir à un modèle de déploiement où le trafic de l'infrastructure peut être ré-acheminé vers des appliances de sécurité spécifiques.
  La combinaison des solutions GigaVUE-VM et GigaVUE TA fournit une visibilité du trafic est-ouest, du site interne et des réseaux du centre de données. Elles apportent également une solution aux problèmes liés à la mobilité et fournissent une source constante de trafic haute-fidélité aux appliances de sécurité, qui sont désormais capables de surveiller la propagation latérale des menaces et de contrôler l'infrastructure de manière pervasive.
- **Renseignements sur le trafic fournis par GigaSMART :** Alors que les gammes GigaVUE-VM et GigaVUE TA offrent des appliances de sécurité capables de prendre en charge des flux de trafic hautement pertinents dans toute l'infrastructure de façon rentable et extensible, les plateformes GigaVUE H reposant sur la technologie GigaSMART permettent d'agir sur ces flux de trafic et de prendre toute une série de mesures susceptibles d'alléger et d'optimiser diverses solutions de sécurité. Parmi les fonctions GigaSMART avancées prises en charge par des solutions de sécurité, on peut citer :
  - **Génération de Netflow haute performance (IPFIX) et de métadonnées :** IPFIX est une technologie puissante basée sur des normes qui prend de l'ampleur dans le secteur de la sécurité réseau comme outil d'informatique légale, d'analyse de données et de détection d'irrégularités. IPFIX analyse le contenu brut des paquets du réseau et en extrait des métadonnées sophistiquées basées sur les flux comme des enregistrements de conversation entre terminaux, la durée de ces échanges et les canaux de communication, etc. GigaSECURE centralise les fonctions qui permettent de générer ces enregistrements de flux de manière homogène dans des infrastructures pourtant hétérogènes et disparates. Les enregistrements de flux peuvent être transférés à plusieurs solutions de sécurité qui analysent les métadonnées. La génération des métadonnées de flux se fait à débit très élevé agin de générer des enregistrements haute-fidélité essentiels pour une bonne analyse de sécurité. La solution permet également de définir des modèles personnalisés afin que les informations extraites du trafic puissent être personnalisées aux catactéristiques spécifique de l'environnement de déploiement.
  - **Déchiffrage SSL :** Avec la croissance du volume de malwares qui utilisent à fond les canaux de communication chiffrées, la nécessité de surveiller les canaux chiffrés se fait plus pressante. Le déchiffrage des canaux de communication chiffrés est plus efficace et ne se fait qu'une fois au sein de la plateforme applicative protégée GigaSECURE, avec une performance élevée qui élimine les angles morts pour les appliances qui n'ont pas l'habitude de traiter des communications chiffrées. Pour ces appliances de sécurité qui n'ont pas la capacité de traiter des communications chiffrées, cela permet de décharger chacune de ces appliances de sécurité de cette tâche de calcul intensive.
  - **Filtrage de session :** De nombreuses solutions de sécurité n'ont pas besoin d'analyser entièrement les flux de confiance ou les flux qu'elles ne sont pas aptes à traiter. Grâce à l'outil de filtrage de sessions d'applications, la plateforme de sécurité est capable d'inspecter les paquets au niveau de la couche d'application, d'identifier les flux applicatifs basés sur un quelconque modèle arbitraire au sein des paquets et de diriger des sessions entières (c'est-à-dire tous les paquets appartenant à cette session, même si les paquets suivants ou précédents ne correspondent pas au modèle) vers une solution de sécurité spécifique ou d'ignorer la session entière. Cette capacité puissante permet de contrôler précisément les types de données de trafic envoyés aux outils de sécurité sur les couches L4-L7 et de mettre en correspondance des contenus plus sophistiqués. Elle garantit que les solutions de sécurité ne géreront que le trafic réseau le plus pertinent tout en allégeant leur charge de traitement, en ignorant des volumes importants de données non pertinentes. Il est possible de personnaliser ce qui est pertinent et non pertinent en fonction de chaque appliance de sécurité.
- **Protection en ligne et équilibrage de charge :** Bon nombre d'appliances de sécurité fonctionnent en ligne avec le trafic réseau pour le protéger en temps réel des activités malveillantes et des malwares. Bon nombre d'autres appliances de sécurité fonctionnent en mode hors bande et dans la bande passante à des fins de détection et de génération d'incidents. La plateforme de sécurité GigaSECURE offre une plateforme commune pour envoyer les flux de trafic aux solutions déployées en ligne et hors bande. Pour les solutions de sécurité déployées en ligne, la plateforme GigaSECURE permet de répartir la charge sur les diverses solutions de sécurité en ligne, et de mettre en série les différentes appliances de sécurité en ligne pour qu'elles fournissent chacune

des niveaux de protection différents. Le trafic peut être envoyé vers les appliances de sécurité en fonction de plusieurs critères. tout en veillant à ce que le trafic inverse et de réacheminement d'un flux spécifique soit toujours envoyé vers la même appliance de sécurité. La plateforme fournir la résilience et la protection nécessaires en cas de défaillance de la sécurité en ligne, tant en mode d'équilibrage de charge que lorsque les appliances en ligne sont installées en série, pour éviter les perturbations dans le trafic réseau. Les appliances de sécurité peuvent également être déplacées sans problèmes d'un mode hors bande à un mode en ligne et vice versa, sans perturbation au niveau du réseau. C'est un outil performant qui unifie et simplifie le déploiement d'un éventail de solutions de sécurité en ligne et hors bande, tout évitant les problèmes de résilience et de défaillance de manière très efficace.

- **Contrôleur centralisé (GigaVUE-FM) :** GigaVUE-FM sert de contrôleur centralisé et est capable d'unifier les différents composants de la plateforme de sécurité GigaSECURE. Elle agit en tant que point de définition de polices centralisé pour les nœuds de visibilité virtualisés et physiques. GigaVUE-FM offre un ensemble d'API vers le nord qui permettent aux solutions de sécurité d'affiner quasiment en temps réel les flux de trafic qu'elles reçoivent pour ajuster leur visibilité du réseau et des infrastructures IT en fonction des irrégularités, des menaces et des conditions décelées, elles aussi en temps réel. En d'autres mots, les API permettent un certain degré d'automatisation qui permet aux outils de sécurité de contrôler les flux de trafic qu'ils reçoivent de la plateforme de sécurité, sur la base des conditions dynamiques analysées en temps réel ou presque.

La plateforme de sécurité GigaSECURE répond aux exigences souvent délaissées, mais essentielles, d'évolutivité et de rentabilité capables d'étendre la portée des différentes appliances de sécurité. Elle permet également de résoudre les problèmes d'opposition, de réduire les coûts et de simplifier les architectures de déploiement. L'approche améliore de manière significative le modèle de couverture pour la sécurité réseau tout en offrant une meilleure visibilité des menaces internes et de la propagation latérale des menaces.

Avantages

Il y a plusieurs avantages à choisir cette approche architecturale orientée sur la plateforme pour déployer des appliances de sécurité. La solution:

- Fournit des renseignements complets et immédiates sur le trafic réseau d'une entreprise ainsi qu'une visibilité de la propagation latérale des malwares.
- Envoie le trafic aux appliances de sécurité, élimine les incertitudes quant aux meilleurs sites d'implantation des appliances de sécurité pour obtenir les flux de trafic pertinents.
- Permet des mises à jour, des modifications ou des changements hors bande/en ligne sans affecter les solutions de sécurité du réseau.
- Réduit de manière significative les faux positifs grâce à la consolidation de plusieurs solutions de sécurité en un ensemble centralisé plus petit, plus à même d'exploiter la plateforme de sécurité.
- Élimine les zones d'ombre associéss à la mobilité et au chiffrage
- Fournit une source cohérente de paquets et de données de flux pour toutes les appliances de sécurité.
- Élimine les oppositions au sein du trafic - le trafic pertinent est répliqué et envoyé à toutes les solutions de sécurité.
- Augmente l'efficacité des solutions de sécurité en éliminant les flux de trafic non pertinents.

Summary

L'évolution des cybermenaces requiert un changement fondamental dans les modèles de sécurité traditionnels. Puisque les organisations reconnaissent le caractère inévitable des brèches, elles se tournent vers les architectures de sécurité pour détecter les malwares et les menaces au sein de l'organisation tout en atténuant les risques. Il faut pour cela des connaissances plus approfondies et une couverture plus grande que ne le permettent les modèles traditionnels et il faut donc un nouveau modèle de déploiement des solutions de sécurité. Ce modèle doit apporter une solution au problème des menaces intrusives, à l'explosion des volumes de trafic et aux oppositions créées par les différents outils. Une approche structurée et architecturale de la visibilité réseau fournit aux solutions de sécurité les accès nécessaires et permet de réduire les coûts. Grâce à sa sécurité renforcée et à sa meilleure rentabilité, la plateforme de sécurité est devenue la pierre angulaire du déploiement des solutions de sécurité. GigaSECURE est la plateforme de sécurité de Gigamon, qui associe pour la toute première fois des outils de calcul et de filtrage de paquets. Elle constitue l'avenir de la sécurité réseau, en leur fournissant les outils de détection et d'intervention nécessaires.

Rejoignez notre écosystème de partenaires afin de lutter vous aussi contre les cybercriminels à wefightsmart.com

3163-02 09/16

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com