Livre blanc

Sécurité à la vitesse de votre réseau

Introduction

Alors que le volume et la vitesse des données réseau ne cessent de s'accroître, les outils de sécurité s'avèrent incapables de suivre le rythme, avec pour conséquence une démultiplication des outils de sécurité, une dégradation des performances, des inefficacités et des dépenses inutiles. Cet ensemble de conséquences conduit à un temps accru en matière de détection des menaces et de réponse ainsi qu'un risque supérieur de brèche, en dépit de dépenses importantes en outils de sécurité.

La solution est donc d'établir une architecture de sécurité réseau efficace qui puisse faire face aux vitesses réseau croissantes actuelles, tout en augmentant le retour sur investissement des outils de sécurité, et en réduisant la complexité, les coûts et la surcharge des outils à travers l'infrastructure physique, virtuelle ou cloud. Ceci est accompli en utilisant l'approche architecturale d'un collecteur de paquets réseau conçu pour la sécurité afin de permettre le déploiement d'un ensemble diversifié de solutions de sécurité sous la forme d'une ferme d'outils de sécurité centralisée, réduisant ainsi significativement les frais généraux, la complexité et les coûts.

Ce livre blanc envisagera les problèmes de sécurité introduits par des volumes de données plus importants sur des réseaux plus rapides, la façon dont une approche architecturale peut résoudre ces problèmes et introduira la Plateforme de sécurité GigaSECURE®, le collecteur de paquets réseau de nouvelle génération leader, conçu pour que les outils de sécurité fonctionnement plus efficacement à travers les environnements physiques, virtuels et cloud. De fait, IHS Markit1 a désigné Gigamon comme l'entreprise leader du marché et le fournisseur le plus réputé dans ce secteur avec la première part de marché dans plusieurs industries : 36 % au total, et 59 % dans le secteur Gouvernement.

Le coût de volumes de données supérieurs à vitesses plus élevées

Alors que les données en mouvement à travers les environnements sur site et cloud continuent d'augmenter en volume, les entreprises répondent par des mises à niveau vers des réseaux à vitesse plus élevée, incluant des réseaux 40 Gb et 100 Gb. Bien que cela aide à adapter leurs opérations afin de répondre à la demande du marché, il existe certaines conséquentes coûteuses à envisager :

1. Lacunes de sécurité préoccuppantes

Le volume croissant de données sur des réseaux plus rapides dépasse la capacité et les performances des outils de sécurité et de surveillance, ce qui génère un écart majeur entre les données circulant au sein d'une entreprise et la capacité des outils de sécurité à traiter ces données à un moment précis. Par exemple, à des vitesses réseau de 100 Gb, l'écart inter-paquets de 6,7 nanosecondes ne constitue tout simplement pas un temps suffisant pour de nombreux outils de sécurité afin d'effectuer des analyses de sécurité et de prévenir les menaces, s'ils doivent traiter l'ensemble du trafic réseau au cours de cet intervalle.

En conséquence, les entreprises se voient contraintes de :

- Ralentir leurs activités en ralentissant leurs réseaux afin que les outils de sécurité puissent faire face.
- Désactiver certains de ces outils de sécurité, tels qu'IDS, IPS et pare-feux pour application Web, afin de maintenir leurs activités à pleine capacité lorsque la charge est trop élevée pour les outils.
- Échantillonner le trafic ou opérer en mode détection uniquement, deux options particulièrement risquées.

Quelque soit le choix, cela conduit à une couverture de sécurité moins qu'optimale. Entretemps, des outils directement connectés via taps ou ports SPAN (Switched Port Analyzer) parviennent aux limites de leur capacité de traitement, forçant du trafic à être écarté et compromettant par là même la sécurité organisationnelle. De plus, les outils de sécurité connectés à des points spécifiques du réseau peuvent ne pas voir le trafic issu d'autres parties du réseau, ou d'utilisateurs ou applications s'étant déplacés vers d'autres parties du réseau. Cette visibilité limitée suscite des conflits en matière de trafic entre les services.

2. Escalade des coûts

Les entreprises ont déjà investi des sommes colossales dans des outils supportant 10 Gb et 40 Gb (tels que pare-feux, IPS/IDS, DLP, etc.) et continueront à le faire. Cybersecurity Ventures prévoit que les dépenses globales en produits et services de cybersécurité excéderont mille milliards USD cumulés au cours des cinq prochaines années, de 2017 à 2021.[2]

[1]https://www.gigamon.com/content/dam/gated/AR-IHS-Technology-Gigamon-Market-Leader.pdf
[2]Steve Morgan, "Cybersecurity Market Report," Cybersecurity Ventures, May 30, 2017. https://cybersecurityventures.com/cybersecurity-market-report/

Néanmoins, avec les volumes accrus de trafic générés par les réseaux 100 Gb, il existe une disparité entre les capacités d'investissement d'une entreprise en outils de sécurité actuels, et le volume de trafic devant être surveillé et analysé. Ceci se voit davantage aggravé par le fait que tous les outils de sécurité (voire la majorité) d'une entreprise (particulièrement les outils passifs) ne sont pas capables d'opérer à 100 Gb, et ces derniers sont généralement très chers.

Alors que les entreprises achètent de plus en plus d'outils de sécurité, les mettent à niveau ou les remplacent, les réseaux deviennent plus lourds et complexes, et les coûts s'envolent.

3. Compromis douloureux

Comme les entreprises cherchent à sécuriser des volumes de trafic supérieurs de façon à pouvoir passer à des réseaux plus rapides, allant jusqu'à 40 Gb et 100 Gb sans que les outils ne deviennent un problème, elles doivent faire des compromis entre sécurité, performances et coût. Les tentatives d'utiliser des outils de sécurité plus lents sur des réseaux plus rapides requièrent l'échantillonnage du trafic, qui augmente le risque de brèche. Ou bien encore, elles permettent aux outils de sécurité plus lents d'effectivement ralentir le réseau. Dans les deux cas, il ne s'agit pas d'une option intéressante, aussi les fournisseurs d'outils font la promotion d'une approche « arracher et remplacer » afin de mettre à niveau. Les fournisseurs incapables de répondre à des charges plus élevées encouragent la multiplication des outils, avec un équilibreur de charge, une autre option aussi coûteuse qu'inefficace. De telles approches peuvent finir par représenter des dépenses de plusieurs millions de dollars USD, et n'aident aucunement les entreprises à profiter pleinement des avantages de la mise à niveau de leurs réseaux. Pas plus qu'elles n'offrent d'avantages supplémentaires, tel que par exemple être en mesure d'ajouter ou retirer facilement des outils Inline, et d'analyser plus de segments du réseau sans avoir à acheter plus d'outils.

Pour résumer, les équipes de sécurité sont confrontées à une complexité accrue, des coûts plus élevés, et une perte de contrôle croissante alors que les volumes de données et les vitesses de réseau augmentent. Les contrôles de sécurité et de gestion sur les réseaux haute performance requièrent une nouvelle approche.

Une approche architecturale de la sécurité résout le problème de la vitesse et du volume

Afin de répondre aux lacunes de sécurité, à l'escalade des coûts et aux compromis suscités par des volumes de données supérieurs sur des réseaux plus rapides, les entreprises se tournent vers une approche architecturale afin d'aider à :

- Améliorer la posture de sécurité.
- Réduire les coûts.
- Éliminer les compromis.

Cette approche architecturale permet le déploiement d'un ensemble diversifié de solutions de sécurité sous la forme d'une ferme d'outils de sécurité centralisée, réduisant ainsi significativement les frais généraux, la complexité et les coûts. Une telle approche est au cœur d'une plateforme de sécurité, laquelle se trouve en mesure d'équilibrer la charge des sessions grâce à des ensembles d'outils de moindre capacité. Elle fournit ainsi non seulement la capacité requise, mais elle y parvient aussi en utilisant l'ensemble d'outils actuel, ce qui réduit les coûts.

De plus, une plateforme de sécurité renforce la résilience du réseau en permettant une architecture N+1 pour l'équilibrage de charge des outils de sécurité, de sorte que dans l'éventualité d'une défaillance, un outil de sécurité peut être mis hors service et remplacé sans interruption ni amoindrissement de la sécurité. Les outils de sécurité Inline peuvent affecter négativement la résilience et les performances

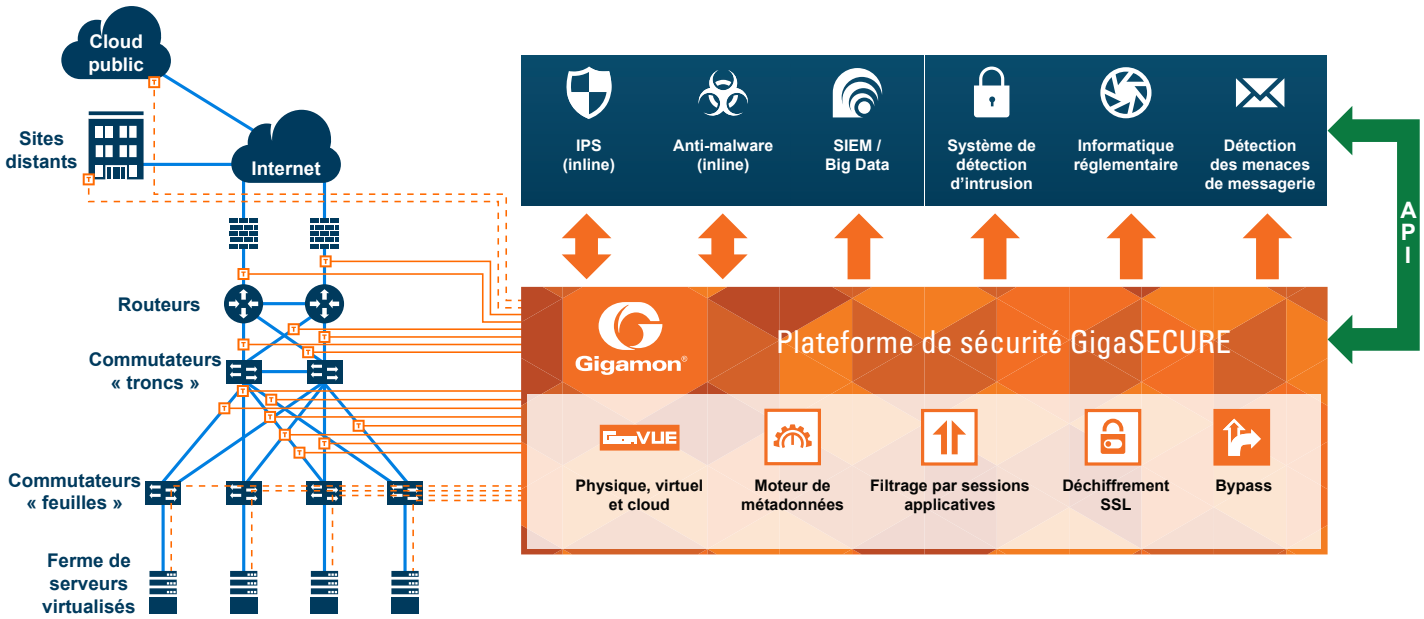

Figure 1 : Une approche architecturale de la sécurité

d'un réseau, parce qu'ils constituent des points de défaillance potentiels sur le réseau, et opèrent souvent à des vitesses considérablement inférieures à celle du réseau. Que la raison soit une défaillance matérielle, un dysfonctionnement logiciel ou un goulot d'étranglement de traitement, des outils Inline défaillants ou lents peuvent perturber les applications et services qu'ils sont pourtant supposés protéger. Le mécanisme de bypass inline physique et logique d'une plateforme de sécurité apporte la solution à ce problème.

En centralisant les outils de sécurité, la sécurité peut être étendue à travers les environnements physiques, virtuels et cloud en acquérant le trafic depuis les appareils et applications présents dans le centre de données à travers les sites physiques, virtuels et distants, de même que dans les clouds privés et publics. Cette approche offre une vue de l'infrastructure dans son intégralité à tout outil opérationnel nécessitant des enregistrements du trafic et des flux issus du trafic réseau, elle élimine également les angles morts et fournit un accès rapide à l'ensemble du réseau.

« De plus, de par sa nature, la plateforme de sécurité fournit une base importante pour l'amélioration de la cybersécurité. Par exemple, elle permet aux équipes SecOps d'intégrer de nombreuses solutions de sécurité disparates, incluant outils en ligne et hors bande, au sein d'une plateforme intégrée unique qui simplifie le déploiement, les opérations et la gestion entre ces produits. La plateforme de sécurité agit également en tant que « chambre de compensation » pour le trafic afin de garantir que le trafic approprié est dirigé vers l'outil de sécurité adéquat. Ceci non seulement optimise les performances de ces dispositifs ou logiciels, mais contribue également à réduire le nombre d'instances inutiles de ces produits, lesquels peuvent s'avérer particulièrement coûteux. »[3]

L'Enterprise Strategy Group (ESG) a récemment écrit au sujet de l'approche architecturale en matière de consolidation des outils de sécurité. « Ainsi que clairement démontré par les données de recherche d'ESG, la plupart des entreprises peuvent améliorer leur visibilité réseau et réduire leurs vulnérabilités en matière de sécurité. Néanmoins, elles doivent procéder à des investissements intelligents. L'ajout d'outils ponctuels supplémentaires à un environnement de sécurité et de surveillance déjà fragmenté ne fera qu'aggraver la situation plutôt que de produire des résultats meilleurs. Au contraire, il est plus probable que l'entreprise typique puisse obtenir de meilleurs résultats en matière de sécurité en investissant dans du personnel (probablement trop dispersé aujourd'hui) ou en consolidant les outils par le biais d'une approche, basée sur une plateforme, de la visibilité, dans laquelle les données, analyses et rapports issus de divers outils peuvent être agrégés et consommés via un panneau de contrôle unique. Cette méthodologie architecturale est une solution particulièrement intéressante, car elle permet aux entreprises de préserver leurs investissements dans les outils existants, en les rendant plus performants, tout en donnant le contrôle au personnel. Améliorer l'utilisation des ressources informatiques et humaines existantes au sein de l'organisation est une façon prudente de répondre à ces défis. »[4]

Présentation de la Plateforme de sécurité GigaSECURE

La Plateforme de sécurité GigaSECURE™ constitue un collecteur de paquets de nouvelle génération, conçu afin de permettre aux outils de sécurité d'opérer plus efficacement à travers les environnements physiques, virtuels et cloud. Pour les outils de prévention des menaces Inline, elle renforce la posture de sécurité, simplifie l'informatique et réduit les coûts. Elle offre également une visibilité complète de l'ensemble des activités survenant dans le périmètre d'une entreprise, de sorte que l'ensemble des outils de sécurité peuvent détecter, analyser et bloquer les cyberattaques rapidement. Elle élimine visibilité partielle et angles morts en obtenant le trafic réseau depuis tout point dans l'entreprise, et en appliquant l'intelligence du trafic avant de transmettre des données précises aux outils de sécurité spécifiques dans et à travers l'entreprise.

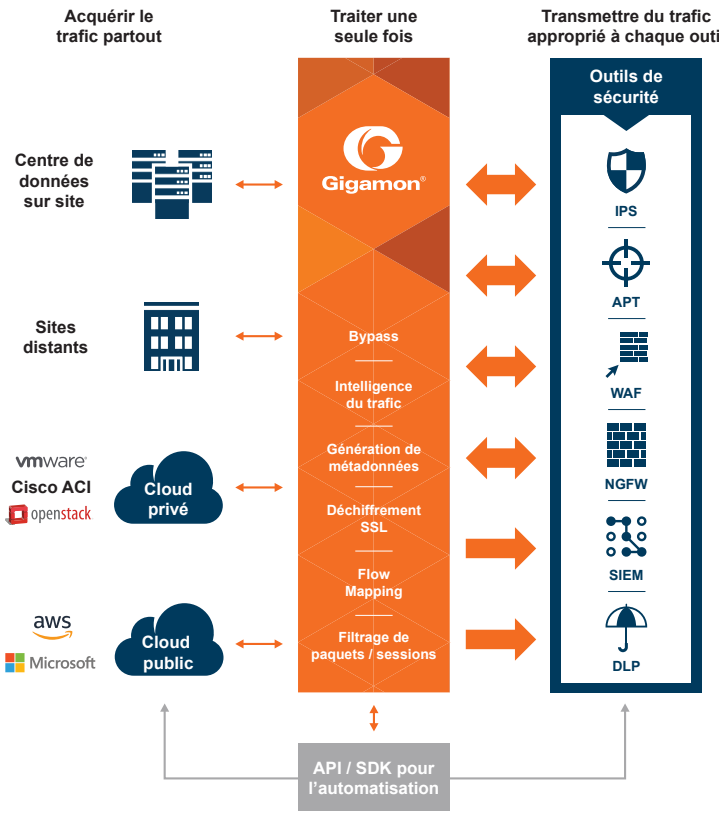

Figure 2 : La Plateforme de sécurité GigaSECURE® de Gigamon

[3]IDG Tech Dossier, "A Security Delivery Platform Benefits the Entire Organization." (Dossier technique IDG : Une plateforme de sécurité bénéficie à l'ensemble de l'entreprise) https://www.gigamon.com/content/dam/gated/wp-security-delivery-platform-benefits-entire-organization.pdf

[4]Dan Conde, "Understanding the State of Network Security Today," (« Comprendre l'état de la sécurité réseau aujourd'hui »), The Enterprise Strategy Group, Inc., Janvier 2017. https://www.gigamon.com/content/dam/gated/wp-esg-research-insights-gigamon-state-of-network-security.pdf

Avantages de la Plateforme de sécurité GigaSECURE

Bien qu'il existe de nombreux avantages à la Plateforme de sécurité GigaSECURE, concentrons-nous sur les trois principaux en ce qu'ils ont trait aux problèmes posés par des volumes de données supérieurs sur des réseaux plus rapides.

1. Améliorer la posture de sécurité

La Plateforme de sécurité GigaSECURE constitue un moyen rapide et économique d'améliorer l'efficacité des outils de sécurité existants. Elle s'adapte parfaitement aux environnements IT existants et élimine le besoin d'avoir à intégrer chaque nouvel outil de sécurité avec de multiples équipements réseau.

La Plateforme de sécurité GigaSECURE permet aux outils de sécurité existants de réaliser leur plein potentiel en :

- Leur fournissant une visibilité complète du trafic réseau circulant à travers l'entreprise, en éliminant les angles morts produits par des réseaux complexes et segmentés, le trafic Est-Ouest et les environnements virtuels.
- Leur fournissant une visibilité du trafic chiffré, même à 100 Gb.
- En rendant chaque outil de sécurité plus efficace en déchargeant les tâches gourmandes en ressources processeur, telles que le déchiffrement SSL et la génération de métadonnées.
- En réduisant le nombre de dispositifs requis et en simplifiant l'infrastructure de sécurité à l'aide de techniques telles que : intelligence du trafic et déduplication.

Grâce à ces avantages, les organisations informatiques peuvent optimiser les performances de leurs outils de sécurité existants indépendamment des vitesses réseaux : à savoir améliorer la posture de sécurité sans démultiplication des outils ou coûts supplémentaires.

2. Réduire les coûts

Une étude mandatée en 2016 « Total Economic Impact™ » (impact économique total) conduite par Forrester Consulting, au nom de Gigamon, a estimé que l'adoption de la Plateforme de sécurité GigaSECURE® par une entreprise composite, comptant 5 000 employés, pouvait économiser 1,1 millions USD en logiciel et matériel de sécurité, et 1,5 millions USD supplémentaires en personnel au cours de trois ans.[5] D'autres avantages incluent :

- 153 pour cent de retour sur investissement grâce aux économies en logiciel et matériel.
- Retour en sept mois de l'investissement.
- Plus de 50 pour cent de réduction des coûts de sécurité.
- Durée d'interruption réduite en raison d'un nombre inférieur de fenêtres de maintenance lorsque la maintenance des outils de surveillance ou des changements opérationnels sont requis.

Simon Gibson, ancien RSSI de Bloomberg, membre et RSSI de Gigamon, explique plus avant comment les entreprises peuvent réduire leurs coûts avec la Plateforme de sécurité GigaSECURE :

> « La Plateforme de sécurité GigaSECURE peut réduire significativement le coût de la sécurité sans rendre l'entreprise moins sûre. Sans la Plateforme de sécurité GigaSECURE, les équipes de sécurité achètent des outils de sécurité haute performance onéreux à déployer sur chaque point critique du réseau. Par exemple, s'il existe six points d'entrée, il est fort probable que l'entreprise fournisse une douzaine de pare-feux nouvelle génération (deux à chaque emplacement aux fins de redondance). Une fois en place, le trafic issu de chaque point peut être agrégé en un point unique. Aussi plutôt que d'avoir à en acheter 12, elle en achètera une paire uniquement. De même, vous pouvez envoyer le trafic uniquement à l'outil de sécurité qui en a véritablement besoin, réduisant significativement les exigences en matière de performance. La norme est de dépenser à outrance en outils de sécurité, or la Plateforme de sécurité GigaSECURE permet aux entreprises d'acheter exactement ce dont elles ont besoin, de plus, elle dispose de l'équilibrage de charge de session, afin qu'une capacité en outils de sécurité supplémentaire puisse être ajoutée au besoin, plutôt que d'avoir à suivre l'approche « arracher et remplacer » traditionnelle. »[6]

3. Éliminer les compromis

Avec la Plateforme de sécurité GigaSECURE, aucun besoin de faire de compromis pour la sécurisation de volumes de trafic supérieurs sur des réseaux plus rapides, du fait qu'aucun compromis n'est requis entre sécurité, performances et coût. La Plateforme de sécurité GigaSECURE offre une visibilité intelligente et complète à travers l'intégralité de l'infrastructure, permettant ainsi aux équipes de sécurité de disposer d'une visibilité exhaustive et uniforme du réseau. En plus du trafic réseau, la Plateforme de sécurité GigaSECURE peut être personnalisée afin d'extraire des sessions applicatives, des métadonnées, et du trafic déchiffré spécifiques. Dans cette architecture, les outils de prévention peuvent opérer avec des performances optimales sans compromettre la résilience du réseau, ni entraîner de ralentissement du réseau. Le résultat est une infrastructure de sécurité réseau plus efficace, avec un retour sur investissement (ROI) considérablement amélioré.

[5] Shaheen Parks, "The Total Economic Impact™ of Gigamon Cost Savings and Business Benefits Enabled by Gigamon," (L'impact économique total des économies et avantages opérationnels permis par Gigamon), Forrester Research, Inc., Avril 2016. https://insight.gigamon.com/forrester-tei-report.html

[6] Zeus Kerravala, "How CIOs can relieve the tension between security and network operations," (Comment les DSI peuvent soulager la tension entre opérations de sécurité et réseau), CIO, 30 novembre 2017. https://www.cio.com/article/3239167/leadership-management/how-cios-can-relieve-the-tension-between-security-and-network-operations.html

Récapitulatif

Alors que les données en mouvement circulant à travers les environnements sur site et cloud continuent à gagner en volume, des entreprises de dimension internationale souhaitant rester compétitives doivent répondre par une mise à niveau vers des réseaux à vitesse plus élevée, opérant à 40 Gb et 100 Gb. Néanmoins, cette évolution suscite des lacunes de sécurité préoccupantes, entraîne une escalade des coûts et des compromis douloureux, conséquences qui doivent être traitées afin de profiter pleinement des avantages d'une mise à niveau vers des réseaux à vitesse plus élevée. Afin de résoudre ces problèmes critiques, les entreprises prévoyantes font le bon choix en adoptant l'approche architecturale d'une plateforme de sécurité, permettant le déploiement d'un ensemble diversifié de solutions de sécurité, sous la forme d'une ferme d'outils de sécurité centralisée, réduisant significativement les frais généraux, la complexité et les coûts associés. La plateforme de sécurité de choix pour les entreprises cherchant à protéger à l'avenir leurs opérations de sécurité est la Plateforme de sécurité GigaSECURE, qui intègre une large variété de solutions de sécurité réseau, telles que détection, prévention, analyses de sécurité, informatique réglementaire, et d'autres outils. La Plateforme de sécurité GigaSECURE permet aux équipes de sécurité informatique de répondre aux nouvelles menaces en temps opportun, tout en éliminant la démultiplication des outils de sécurité, en améliorant la sécurité et en réduisant les coûts. Le résultat est une infrastructure de sécurité réseau bien plus efficace, avec un retour sur investissement considérablement amélioré.

Prochaines étapes

- Arrêtez la démultiplication des outils de sécurité Établissez une architecture de sécurité réseau efficace qui augmente le retour sur investissement des outils de sécurité, tout en réduisant la complexité, les coûts et la surcharge des outils à travers l'infrastructure physique, virtuelle ou cloud à l'aide de la **Plateforme de sécurité GigaSECURE**.
- Découvrez la raison pour laquelle Gigamon constitue le meilleur choix pour votre entreprise : **Parlez à un expert Gigamon**, **demandez une démonstration** ou **inscrivez-vous dès aujourd'hui pour une évaluation gratuite** !

À propos de Gigamon

Gigamon fournit une visibilité active du trafic réseau physique, virtuel et cloud, permettant une sécurité renforcée et des performances supérieures. La Plateforme de visibilité de Gigamon et GigaSECURE - première plateforme de sécurité du secteur - offrent une intelligence avancée de sorte que les solutions de gestion des performances applicatives, réseau et de sécurité sur les réseaux d'entreprises, de gouvernements et de fournisseurs de services opèrent plus efficacement. Découvrez-en davantage sur **www.gigamon.com**, le **blog Gigamon**, ou suivez Gigamon sur **Twitter**, **LinkedIn**, ou **Facebook**. See what matters.™ (Voyez ce qui compte.)

3256-01 01/18

Gigamon®

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