Un nouvel avenir pour les réseaux

Un modèle de télétravail, de sécurité sans frontières et de budgets en baisse. Voici comment y faire face.

Gigamon®

Introduction

Le monde a changé. Dans un court laps de temps, des événements imprévus à l'échelle mondiale ont entraîné de vastes changements dans nos habitudes de travail et nos vies quotidiennes.

Dans le contexte de l'exploitation des réseaux et de la sécurité des informations, cela se traduit par la prise en charge de nouveaux process numériques et un personnel décentralisé avec un budget réduit. La plupart des infrastructures et outils réseau des entreprises ont été conçus pour supporter un personnel travaillant principalement au bureau. Du jour au lendemain, les services informatiques ont dû se réorganiser pour prendre en charge une main-d'œuvre à distance deux à trois fois plus importante que ce qui était prévu En outre, la sécurité doit être maintenue alors que le trafic réseau est passé d'un usage interne à un usage externe. Les changements rapides à l'échelle du réseau et des outils soulèvent des problèmes en matière de sécurité, de résilience et de performance. De même, les applications dont nous dépendons, qu'elles soient personnalisées, packagées ou Web, sont toutes utilisées à des extrêmes non testés au préalable.

Vue d’ensemble

Ce livre blanc examine les priorités informatiques que les entreprises doivent aborder dès maintenant et envisager pour le futur :

+ **AUJOURD’HUI**

  Il est impératif de garantir la sécurité et la continuité des opérations dans ce nouvel environnement bouleversé, tout en redéployant les ressources réseau afin de maintenir le plus haut niveau de satisfaction, à la fois pour les clients et les employés.

+ **UN NOUVEL AVENIR**

  Confrontées à l’incertitude à tous les niveaux, qu’il s’agisse de marchés de capitaux, de chaînes d’approvisionnement, de politique gouvernementale ou de la confiance des consommateurs, les entreprises ont besoin de l’agilité pour répondre de manière rapide et rentable aux défis et opportunités nouveaux et inattendus

Nous aimerions partager nos réflexions sur la façon dont les sociétés peuvent mieux avancer en ces terres inconnues selon les observations tirées de notre base de clients, composée d’entreprises majeures dans tous les secteurs.

Telefónica a acquis une plus grande visibilité sur l'ensemble de son réseau et a traité les problèmes au fur et à mesure des modifications apportées à ce dernier. Au cours du processus de déploiement, Gigamon a aidé à dépanner un problème de performance du parc DNS Cache Server, en le résolvant à distance afin d'éviter une panne de service potentielle, ce qui a permis de rationaliser la performance de l'ensemble du système DNS de Telefónica. Selon une étude ESG (Enterprise Strategy Group), cela aide ses clients à réduire les temps de coupure de 30 à 50 %.

Donner à Telefónica une visibilité pendant la transition.

Aujourd'hui

Les équipes informatiques doivent déployer des capacités et des services supplémentaires plus rapidement que jamais, tout en garantissant que ceux-ci répondent à trois exigences essentielles :

Un nouveau modèle de télétravail

Certains aspects de l'infrastructure et des applications font face à des défis d'adaptabilité, peut-être à des niveaux sans précédent. Le basculement soudain et rapide vers le télétravail a laissé peu de temps aux services informatiques pour étendre leur infrastructure d'accès à distance pour leurs employés. Alors qu'ils s'efforcent de mettre rapidement en ligne une capacité de travail à distance, en reconvertissant des infrastructures anciennes ou existantes, des problèmes tels que des défaillances et des goulets d'étranglement peuvent survenir dans les nouveaux segments et infrastructures de réseau. Détecter ces problèmes à temps est critique. Cependant, devant des ressources déjà surchargées, ces problèmes représentent un obstacle véritablement significatif.

En plus de prendre en charge les utilisateurs internes, les services informatiques sont confrontés à une augmentation de l'utilisation des applications externes. Les clients sont maintenant en contact avec des sociétés principalement par le biais d'applications mobiles ou en ligne.

Nos clients dans les secteurs des services financiers, des soins de santé, du divertissement et du commerce observent une augmentation significative du nombre d'utilisateurs et de la fréquence d'utilisation pour leurs applications grand public. Alors que de nouveaux conteneurs d'applications, microservices et machines virtuelles sont rapidement mis en œuvre pour répondre à la croissance soudaine de la demande des utilisateurs, les services IT risquent de se trouver dépassés par les équipes de DevOps et d'applications qui travaillent plus rapidement. Cette désynchronisation peut avoir de graves conséquences. Même si la capacité d'application peut augmenter, la capacité d'infrastructure peut se trouver en décalage, engendrant ainsi des problèmes de bande passante et d'expérience utilisateur amoindries, tandis que l'accès et l'utilisation des applications et données peuvent ne pas être surveillés de manière adéquate concernant les menaces.

Sécurité sans frontières au-delà du réseau

Toute activité utilisateur supplémentaire dans de nouveaux segments de réseau peut devenir une source de menaces, notamment en matière de fuite de données ou de ransomware. Les personnes malveillantes exploitent rapidement la paranoïa et l'incertitude régnantes dans le but de compromettre les systèmes des utilisateurs. Ces menaces utilisent des injecteurs, qui sont ensuite utilisés pour télécharger des logiciels malveillants sur les systèmes de l'utilisateur afin de compromettre leurs informations d'identification, résultant en des attaques de ransomware et des fuites potentielles de données. (Consultez des exemples ici[1] et ici[2].)

Le fait que les travailleurs distants utilisent leur réseau domestique et/ou leurs équipements personnels pour travailler ajoute à ce problème d'externalisation. Il n'est pas certain que chaque travailleur respecte les protocoles de sécurité recommandés. Même l'utilisation obligatoire des VPN peut ne pas résoudre le problème, surtout si les points de terminaison n'ont pas été récemment corrigés. Par exemple, des vulnérabilités sont détectées et signalées concernant divers fournisseurs de VPN et de pare-feu, qui permettent à différentes menaces de type Mirai botnet de prendre le contrôle des équipements[3]. Afin d'augmenter leur capacité, les entreprises doivent s'assurer que, s'ils utilisent des équipements plus anciens, ceux-ci sont adaptés à l'usage prévu et peuvent être corrigés et sécurisés.

Travailler avec des budgets réduits

À mesure que de nombreux secteurs de l'économie commencent à ralentir, les entreprises prévoient déjà une récession potentielle. Les secteurs des

[1] https://www.forbes.com/sites/thomasbrewster/2020/03/18/coronavirus-scam-alert-covid-19-map-malware-can-spy-on-you-through-your-android-microphone-and-camera/#37bf4a0a75fd

[2] https://www.businessinsider.com/hackers-are-using-fake-coronavirus-maps-to-give-people-malware-2020-3

[2] https://krebsonsecurity.com/2020/03/zxyel-flaw-powers-new-mirai-iot-botnet-strain/

voyages, du divertissement et de services sont tous gravement impactés. Les retombées de cet effet sur l'économie à plus grande échelle sont planifiées par les entreprises sous forme de restrictions budgétaires, d'arrêt temporaire des recrutements et de contrainte en matière de dépenses. Les équipes informatiques et applicatives en sont particulièrement impactées, alors qu'on leur demande d'accroître l'étendue du réseau sans étendre leurs ressources; la nécessité de faire plus avec moins n'a jamais été aussi importante.

Un nouvel avenir

Restez concentré sur vos objectifs tout en évaluant vos options

Alors que l'économie absorbe l'impact des semaines récentes, de nombreuses entreprises prévoient déjà une récession potentielle. Les chaînes d'approvisionnement mondiales ont d'abord été interrompues en Asie et ces effets se cumulent et s'amplifient à présent en raison des changements drastiques observés dans les économies européennes et américaines. Ces transformations affectent profondément les secteurs du voyage, de l'hôtellerie, du commerce, du divertissement et des services. De plus, pour ceux qui ne sont pas directement touchés par des fermetures forcées, les retombées de celles-ci sur l'économie à plus grande échelle obligent la majorité des entreprises informatiques à réexaminer leurs budgets et priorités en matière de dépenses.

Alors que les entreprises et les entreprises informatiques évaluent leurs priorités, celles-ci sont confrontées à une incertitude : Combien de temps durera la crise? Quelle capacité de bande passante réseau et combien d'applications et de services supplémentaires devront être ajoutés? Comment gérer les problèmes et, dans certains cas, les opportunités liés à cette crise? Est-ce que le télétravail deviendra un modèle permanent pour leurs entreprises?

L'une des approches pour répondre à nombre de ces obstacles consiste à tirer parti des informations du réseau en temps réel pour la détection d'applications, d'utilisateurs et d'équipements, le dépannage, les performances applicatives, le suivi de l'expérience utilisateur et la sécurité.

Les données du réseau constituent l'unique source fiable concernant les performances et la sécurité de votre réseau. Si ces données sont fiables et à jour, les équipes n'auront pas à modifier en continu les niveaux de journalisation sur les serveurs, à rappeler aux développeurs d'instrumenter les applications ou à ajouter de nouvelles applications de surveillance.

Afin de garantir que ces données sont suffisamment fiables pour former une source unique de vérité, il est impératif qu'elles comprennent des données en circulation provenant des environnements physiques, cloud et virtuels, des systèmes d'enregistrement, des fichiers log et d'autres sources de données. Une bonne pratique consiste à utiliser un modèle de raccord unique, par lequel toutes les informations en circulation sont immédiatement accessibles aux outils de sécurité et de surveillance des performances à mesure que de nouveaux segments réseau sont mis en ligne. La fourniture d'un accès aux données du réseau doit être rapide, avec un minimum d'intervention humaine et peu, voire aucune dépendance envers les équipes applicatives, de DevOps, etc.

Under Armour avait besoin d'une visibilité complète sur les performances et la sécurité de ses applications numériques. Cette fiabilité était essentielle pour répondre aux attentes de leurs clients en matière d'expérience utilisateur et de confiance. Selon un rapport ESG, Gigamon a permis une visibilité 75 % plus significative du trafic réseau.

« Disposer d'une visibilité complète des performances et de la sécurité de nos applications numériques est essentiel pour répondre aux attentes en matière d'expérience utilisateur et de confiance exprimées par nos clients. »

Aider Under Armour à protéger leurs clients.

Restez concentré sur vos objectifs tout en évaluant vos options

Bien que l'issue de la crise actuelle reste inconnue, voici nos recommandations sur la manière dont vous pouvez préparer le succès de votre entreprise.

EXPÉRIENCE UTILISATEUR RELATIVE À L'APPLICATION.

Plus que jamais, il est évident que les applications numériques sont essentielles aux organisations : la nécessité de garantir les meilleures expériences client et utilisateur possibles n'a jamais été aussi importante.

Pour ce faire, il est important d'utiliser des outils qui surveillent et visualisent l'utilisation des applications et l'expérience utilisateur, mais qui peuvent également prendre des mesures en fonction de la performance et du comportement de ces applications.

Par exemple, les hausses du trafic de visioconférence en raison de l'utilisation intensive d'applications telles que Cisco Webex, GoTomeeting, Skype et Zoom peuvent très rapidement submerger les outils de sécurité hors bande, notamment en matière de détection d'intrusion. Les équipes informatiques doivent être en mesure de visualiser rapidement les applications à l'origine de ces pics de trafic, de décider s'ils doivent analyser ce trafic et a quel niveau, puis de filtrer le trafic sûr ou à faible risque afin de préserver la bande passante pour d'autres applications.

SÉCURITÉ RÉSEAU SANS FRONTIÈRES.

Face à des cyberattaques plus fréquentes et plus sophistiquées, la pandémie COVID-19 a dévoilé une nouvelle vague de personnes malveillantes cherchant à tirer parti des équipes InfoSec et des utilisateurs en quête d'informations sur le virus à la fois à l'échelle mondiale et locale. Ainsi, disposer des bons outils de sécurité et d'un réseau de données riches n'a jamais été aussi important.

Voici quelques exemples d'outils à même d'offrir une assistance à court et à long terme :

+ **DÉTECTION DES MENACES ET RÉPONSE AUX MENACES**
  Devant la hausse d'attaques et de vulnérabilités résultant du basculement vers le télétravail sur des architectures VPN étendues rapidement, il est impératif que les entreprises disposent d'outils puissants pour détecter ces nouvelles menaces et y répondre. Par exemple, les outils de pointage fonctionnant au niveau des liens d'entrée/sortie et derrière les concentrateurs VPN fournissent une approche ciblée permettant de réduire les risques potentiels.

+ **DÉCHIFFREMENT DU TRAFIC CENTRALISÉ**
  Bien que de nombreux outils puissent déchiffrer le trafic encrypté, le déploiement d'une solution centralisée pour déchiffrer et inspecter celui-ci constitue souvent l'option la plus efficace pour de nombreuses organisations. La centralisation des capacités de déchiffrement TLS permet au trafic d'être décrypté et inspecté une fois avant d'être réencrypté et partagé sur plusieurs outils. La capacité à analyser le trafic chiffré entrant et sortant des applications peut être importante pour déterminer si l'accès aux applications et aux données est légitime ou illégitime. À mesure que la capacité d'application augmente de manière dynamique, l'architecture des applications est rapidement réorganisée et de nouvelles applications sont élaborées.

+ **UTILISER DES MÉTADONNÉES POUR STIMULER L'EFFICACITÉ SIEM**
  Lorsque les entreprises utilisent des solutions telles que Splunk ou d'autres SIEM pour la surveillance active de leur sécurité, fournir des métadonnées au système et aux applications peut constituer une méthode efficace afin de garantir la conformité, tout en offrant de nouvelles applications et capacités en ligne. Les entreprises doivent s'efforcer de s'assurer que seules des métadonnées précises et pertinentes sont envoyées à ces outils afin d'optimiser le contexte fourni tout en minimisant la quantité de données envoyées. Ceci est particulièrement important pour les outils SIEM, dans lesquels le modèle de facturation est basé sur le volume de données traitées ou stockées.

+ **ZERO TRUST**

  De nombreuses entreprises avaient déjà entamé un processus d'apprentissage, de planification ou de mise en œuvre en matière d'initiative Zero Trust. Cette crise peut se révéler être le point de basculement dans l'accélération de ces initiatives. Les principes fondamentaux de Zero Trust sont d'éliminer la confiance implicite associée à la localité d'accès et de déplacer le périmètre défensif d'une organisation des extrémités du réseau vers les actifs utilisant le réseau, c'est-à-dire les utilisateurs, les périphériques, les données et les applications.

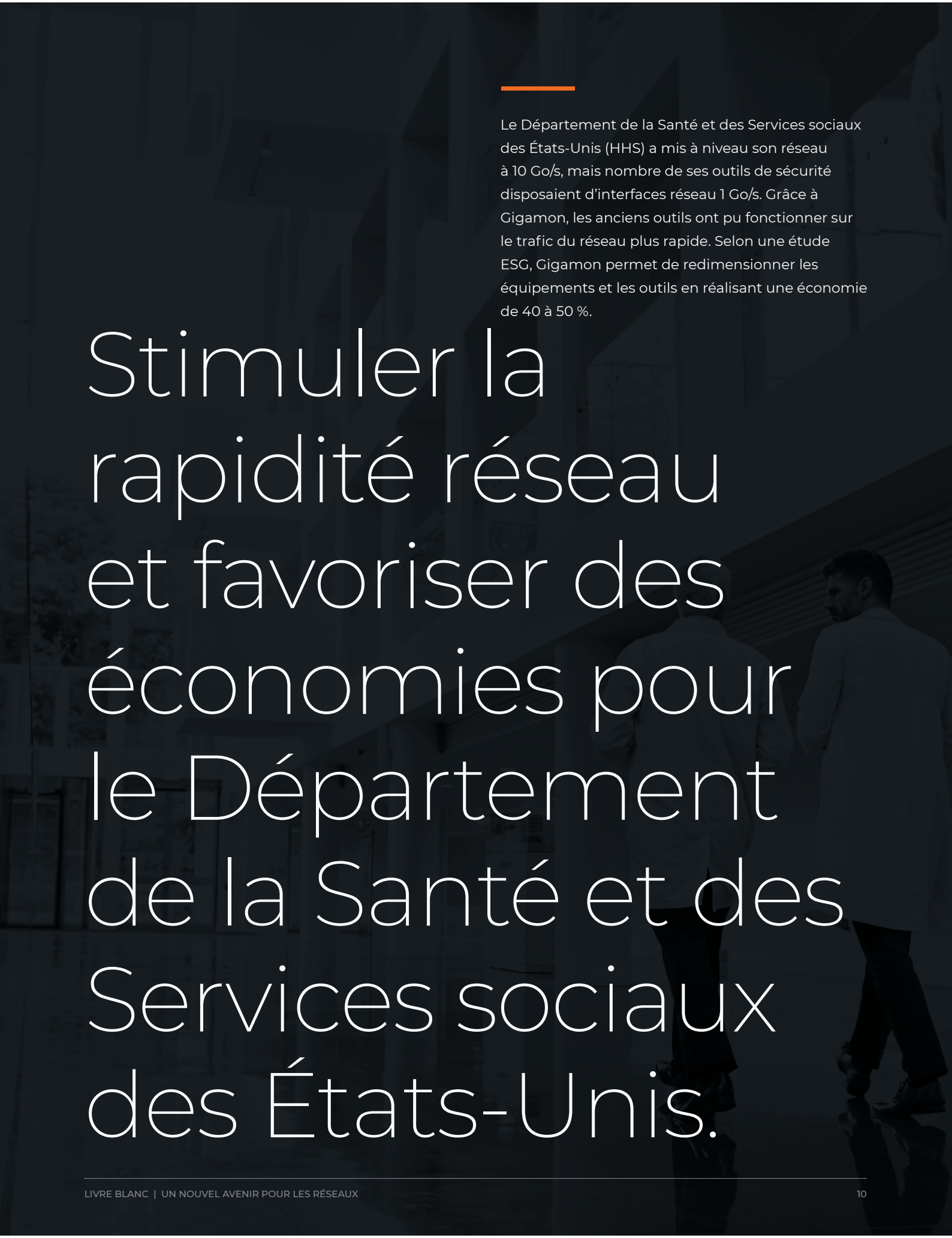
Dans un monde où la main-d'œuvre, suite à la crise du COVID-19 ou à des changements planifiés dans le modèle d'entreprise, évolue vers un modèle de type «travailler partout, à tout moment», basculer vers une architecture Zero Trust devient une évidence. La visibilité de toutes les informations sur le réseau est essentielle pour garantir une solution Zero Trust exhaustive.

Comme on le dit souvent, Zero Trust est un parcours qui nécessite beaucoup de réflexion afin d'assurer une mise en œuvre réussie. La planification ou le lancement de ce parcours a été retardé pour de nombreuses entreprises. Cependant, avec les innovations forcées par la pandémie de COVID-19, la nécessité de rationaliser et d'unifier l'infrastructure de sécurité n'a jamais été aussi urgente qu'à présent.

ÉCONOMIES PAR OPTIMISATION DE VOS INVESTISSEMENTS DANS LES OUTILS.

La plupart des entreprises ont investi significativement dans les outils réseau et de sécurité qu'ils utilisent pour gérer et protéger leurs réseaux et applications. À mesure que le trafic passe du LAN au WAN, il est essentiel que le flux de données de ces outils ne cause pas de surcharge, d'angles morts au niveau de la visibilité ou d'autres problèmes liés à l'augmentation du trafic.

Afin d'optimiser l'efficacité (et le ROI) des outils au sein des entreprises, il est essentiel que le trafic réseau des environnements physiques, virtuels et cloud soit optimisé avant de le fournir à ces outils. Sans cela, de nombreux problèmes pourraient survenir : surcharge des outils, interventions manuelles des équipes dans des processus automatisés, non-disponibilité du réseau, problèmes de fiabilité et de sécurité.



Le Département de la Santé et des Services sociaux des États-Unis (HHS) a mis à niveau son réseau à 10 Go/s, mais nombre de ses outils de sécurité disposaient d'interfaces réseau 1 Go/s. Grâce à Gigamon, les anciens outils ont pu fonctionner sur le trafic du réseau plus rapide. Selon une étude ESG, Gigamon permet de redimensionner les équipements et les outils en réalisant une économie de 40 à 50 %.

Stimuler la rapidité réseau et favoriser des économies pour le Département de la Santé et des Services sociaux des États-Unis.

Conclusion

La série d'événements récents à l'échelle mondiale a changé notre réalité du jour au lendemain. Les équipes NetOps et InfoSec doivent gérer une perturbation massive en raison du télétravail des utilisateurs et se préparer pour un avenir incertain. Dans cette situation, la visibilité et l'agilité de l'infrastructure sont devenues des facteurs clés de réussite concernant la capacité d'une organisation à répondre à ces défis.

À propos de Gigamon

Gigamon est la première entreprise à offrir une visibilité sur le réseau et des analyses unifiées relatives à toutes les données en mouvement, des paquets bruts aux applications, qu'il s'agisse d'infrastructures physiques, virtuelles ou cloud. Nous regroupons, transformons et analysons le trafic réseau afin de résoudre vos besoins critiques en matière de performances et de sécurité, notamment en ce qui concerne la détection rapide des menaces et leur résolution. Ainsi, votre entreprise peut se consacrer à l'innovation numérique.

Gigamon a obtenu plus de 75 brevets technologiques, bénéficie du niveau de satisfaction client le plus élevé du secteur et compte plus de 3 000 entreprises partenaires dans le monde entier, notamment plus de 80 entreprises du Fortune 100.

Pour obtenir une présentation complète de la manière dont Gigamon peut vous aider, rendez-vous sur www.gigamon.com.

Nous vous invitons à rejoindre notre communauté en ligne et en particulier notre Groupe collaboratif de télétravail, au sein duquel vous pouvez partager vos préoccupations, pensées et idées avec des homologues du secteur et les experts de Gigamon.

Gigamon®

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