

SE PROTÉGER CONTRE L'ATTAQUE ULTIME

COMMENT LA VISIBILITÉ DU RÉSEAU PERMET D'ASSURER LA SÉCURITÉ DE
VOTRE ORGANISATION DANS UN CONTEXTE DE MENACES DE PLUS EN PLUS
PRÉGNANTES.



TABLE DES MATIÈRES

BIENVENUE DANS LE MONDE CONNECTÉ	3
CYBER-ATTAQUES : PLUS IMPORTANTES ET PLUS DESTRUCTRICES QUE JAMAIS	4
LE CONTEXTE DES MENACES	5
1. La convergence de l'IT et de l'OT amplifie les menaces	5
2. Le déploiement de la 5G comporte des risques qui changent la donne	5
3. Attaques DDoS : Plus graves, plus fréquentes	6
4. La cybercriminalité chapeautée par l'État	6
5. Un trafic latéral est-ouest	7
VISIBILITÉ OT ET IOT POUR UNE PRODUCTIVITÉ ET UNE SÉCURITÉ ACCRUES, ET DES TEMPS D'ARRÊT RÉDUITS.	9
LE DEPLOIEMENT DE NOZOMI NETWORKS AVEC GIGAMON	10
À PROPOS DE GIGAMON ET DE NOZOMI NETWORKS	11
NOUS CONTACTER	11



BIENVENUE DANS LE MONDE CONNECTÉ

Aujourd'hui plus que jamais, la connectivité définit nos vies. Alors que les appareils IoT connectés à Internet se multiplient de manière exponentielle et que la 5G promet de révolutionner la connectivité, les entreprises et les organisations doivent faire face à la convergence des technologies IT et OT et aux défis qui peuvent en découler.

LES CONDITIONS DE L'ATTAQUE ULTIME

Mais plus les organisations sont connectées, plus elles s'exposent à une exploitation numérique par des cybercriminels à une échelle sans précédent. L'augmentation inquiétante des attaques DDoS, des infiltrations est-ouest et de la cybercriminalité chapeautée par les États crée un contexte de menaces plus sombre et plus dangereux.

Le renforcement de la connectivité et l'augmentation des cyber-risques **pourraient-ils se combiner pour créer une attaque ultime ?** Ce livre blanc explore les menaces que représentent les dernières tendances et explique comment les outils de visibilité et de protection du réseau peuvent contribuer à assurer la sécurité de votre organisation et de votre personnel.

CYBER-ATTAQUES : PLUS IMPORTANTES ET PLUS DESTRUCTRICES QUE JAMAIS

UNE ATTEINTE AU TRAITEMENT DE L'EAU EN FLORIDE MENACE LA SANTÉ DE 15 000 RÉSIDENTS

Les pirates qui ont attaqué une station de traitement des eaux à Oldsmar, en Floride, ont pris le contrôle des niveaux d'hydroxyde de sodium, une substance hautement corrosive utilisée pour équilibrer l'acidité de l'eau. L'attaque de février 2021 a brièvement fait passer les concentrations de 100 parties par million (ppm) à 11 100 ppm, avant qu'un opérateur n'évite la catastrophe en prenant immédiatement les mesures nécessaires pour ramener les taux de produit chimique à la normale. **Si rien n'avait été fait, le piratage aurait mis en péril la santé de 15 000 habitants de la région.**

LES CONSÉQUENCES DU PIRATAGE DE SOLARWINDS FINANCÉ PAR LA RUSSIE SE CHIFFRENT À 100 MILLIARDS DE DOLLARS.

En 2020, des hackers ont exploité des brèches de sécurité dans les logiciels Microsoft, SolarWinds et VMware pour procéder à des milliers de violations de données au sein de l'OTAN, de Microsoft, du Parlement européen, des gouvernements américain et britannique et de nombreuses autres organisations. Identifiée comme l'œuvre de pirates informatiques russes agissant avec l'aval de l'État, l'attaque est passée inaperçue pendant des mois et a causé des milliards de dollars de dommages dans le monde entier, engendrant des coûts supérieurs à **100 milliards de dollars pour les entreprises et les services gouvernementaux américains.**

L'ATTAQUE WANNACRY COÛTE AUX ORGANISATIONS PLUS DE 6 MILLIARDS DE DOLLARS DANS LE MONDE ENTIER

En 2017, la cyberattaque WannaCry est devenue l'incident de ransomware le plus grave au monde, ayant touché plus de **200 000 ordinateurs** dans 150 pays. Les cibles comprenaient le NHS britannique, Telefonica en Espagne, FedEx aux États-Unis et la compagnie ferroviaire allemande Deutsche Bahn. Au sein du NHS anglais, au moins 80 des 236 trusts et 603 organisations de soins de santé primaire ont été infiltrés. Des systèmes informatiques et téléphoniques essentiels ont été désactivés, entraînant l'annulation de milliers d'opérations et de rendez-vous de patients, pour **un coût supérieur à 92 millions de dollars.**

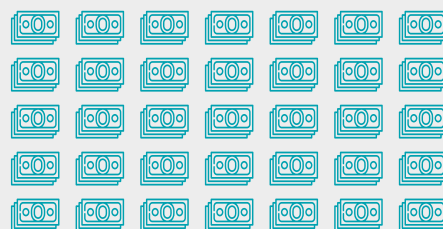
2021

15,000



2020

\$100B



2017

200,000



LE CONTEXTE DES MENACES

1. LA CONVERGENCE DE L'IT ET DE L'OT AMPLIFIE LES MENACES

Dans tous les secteurs industriels, la convergence des environnements **OT** (*technologie opérationnelle*) et **IT** (*technologie de l'information*) s'accélère.

Si la cyber-sécurité informatique est aujourd'hui un secteur bien établi, doté de solutions sophistiquées pour dissuader les cybercriminels, la cyber-sécurité de l'OT n'en est qu'à ses débuts, ce qui en fait **une cible relativement facile pour les pirates**.

Il fut un temps où l'OT était relativement isolée de l'Internet et à l'abri des cyber-menaces. Mais maintenant qu'un nombre accru de processus de fabrication est piloté par des appareils IoT et le cloud computing, la confluence des technologies qui en résulte a fait exploser la surface d'attaque, **permettant aux logiciels malveillants de migrer facilement entre l'IT et l'OT**.

Les violations de l'OT passent souvent inaperçues pendant un certain temps et entraînent une perturbation de la production, des défauts de fabrication ou une interruption des services, avec des **dommages évidents à la réputation de la marque, aux revenus financiers et à la confiance des clients**.

Pour protéger l'OT, il convient d'adopter une approche à deux volets :

- + **identifier et éliminer** les vulnérabilités des technologies à long cycle de vie existantes
- + **intégrer** la cyber-sécurité à la conception des nouveaux systèmes OT

2. LE DÉPLOIEMENT DE LA 5G ENTRAÎNE DES RISQUES QUI CHANGENT LA DONNE

Nombreux sont ceux qui prédisent que la 5G pourrait permettre à des pirates informatiques malveillants de semer le chaos à une échelle encore jamais vue **pour les particuliers et au sein des entreprises et des organismes publics du monde entier**.

Les applications de la 5G seront infinies et offriront de nouveaux modes de gestion des infrastructures, des ressources et des organisations - pensez aux villes intelligentes, aux soins de santé, aux transports, à la planification urbaine ou à la sécurité publique.

Mais l'efficacité accrue et la plus grande évolutivité s'accompagne de la « connectivité totale » tant attendue de la 5G, reliant des milliards d'appareils IoT connectés à l'Internet, et qui offre aux pirates de nombreuses possibilités de mettre hors service des infrastructures essentielles dans les domaines de l'électricité, de la santé et de la sécurité. Au niveau individuel, la 5G offre aux pirates une plus grande marge de manœuvre pour s'infiltrer partout, qu'il s'agisse des appareils portables personnels, des appareils médicaux, des systèmes de contrôle de véhicules ou des systèmes de sécurité domestique.

La 5G verra la croissance exponentielle du déploiement de petites antennes dans les zones urbaines, créant un vaste éventail de cibles "physiques". Par ailleurs, le routage numérique et la gestion du réseau définis par logiciel de la 5G constituent un point vulnérable pour les pirates informatiques.

3. ATTAQUES DDOS : PLUS GRAVES, PLUS FRÉQUENTES



Les attaques par déni de service distribué (DDoS) gagnent en ampleur, en durée et en fréquence. La prolifération des appareils IoT est un facteur contributif majeur et la super-connectivité à haut débit et à méga-bande passante de la 5G crée une porte d'entrée attrayante pour des attaques DDoS plus importantes, plus rapides et plus graves.

L'amplification DNS permet à un simple acteur de lancer une **attaque DDoS à grande échelle, très efficace et peu coûteuse, en exploitant un énorme parc de dispositifs IoT compromis, chacun exécutant un ou plusieurs bots**. Ce réseau de bots (botnet) facilite une attaque de grand volume qui surcharge la bande passante de la victime et met ses opérations hors service. Les botnets englobent souvent des milliers d'adresses IP sources, ce qui rend certaines attaques presque impossibles à bloquer par des approches traditionnelles.

4. LA CYBERCRIMINALITÉ CHAPEAUTÉE PAR L'ÉTAT

Tentatives d'influence des élections nationales, cyber-espionnage industriel et attaques personnelles contre des individus riches et influents... les cyber-crimes chapeautés par l'Etat prennent différentes formes. Perçues comme une alternative facile aux cibles militaires ou gouvernementales bien défendues, les entreprises se retrouvent souvent dans la ligne de mire, surtout si elles conservent des données sensibles, si elles sont très rentables, si elles sont liées à des organismes gouvernementaux, si elles fournissent des services publics essentiels ou si elles sont vulnérables aux pannes informatiques.

La cybercriminalité soutenue par les gouvernements augmente d'année en année. La cyberguerre est un moyen permettant aux nations de faire de l'espionnage peu coûteux, peu risqué et très gratifiant. Aujourd'hui, si la Russie, la Chine et la Corée du Nord sont généralement considérées comme les suspects habituels, les faibles barrières à l'entrée incitent des pays plus pauvres à tenter de passer au niveau supérieur et à faire la guerre en utilisant la technologie pour étendre leur influence dans le monde.

5. UN TRAFIC LATÉRAL EST-OUEST

En général, les mesures de cyber-sécurité sont axées sur la sécurisation du périmètre (une protection dite « nord-sud »). Mais aujourd'hui, **de nombreux pirates choisissent de franchir les défenses du périmètre sans être vus et, une fois à l'intérieur, ils restent inactifs et non détectés pendant des mois.** Au moment opportun, le logiciel malveillant est alors activé et se diffuse latéralement dans le réseau, trouvant un passage d'un hôte ou d'un segment interne à un autre.

Cette stratégie de diffusion est-ouest tire parti de la récente tendance à interconnecter les appareils IT, OT et IoT sur la même infrastructure. Avec un délai moyen de détection des brèches de 207 jours, les attaquants à l'intérieur du périmètre ont tout le loisir d'explorer les réseaux sans être inquiétés, de rechercher les points faibles et de sélectionner les actifs les plus précieux à voler, exploiter ou endommager.

L'ATTAQUE ULTIME SE PRÉPARE

Convergence informatique/technologie de l'information, déploiement de la 5G, attaques DDoS, diffusion est-ouest, piratage habilité par les États : toutes ces menaces pour la sécurité sont en hausse. Prises individuellement, chacune a le potentiel de causer des dommages importants. Mais **collectivement, ces facteurs de risque pourraient se combiner pour déclencher des attaques d'une ampleur sans précédent dans l'histoire de la cybercriminalité.** Cette attaque ultime pourrait avoir des conséquences dévastatrices et dangereuses pour les individus, les entreprises et les économies à l'échelle mondiale.

207*
JOURS :

Délai moyen pour identifier une violation*

73*
JOURS :

Délai moyen pour contenir une violation*

*IBM, Cost of a Data Breach Report, 2020

VISIBILITÉ OT ET IOT POUR UNE PRODUCTIVITÉ ET UNE SÉCURITÉ ACCRUES, ET DES TEMPS D'ARRÊT RÉDUITS

COMPRENDRE ET SÉCURISER VOTRE RÉSEAU OT/IOT

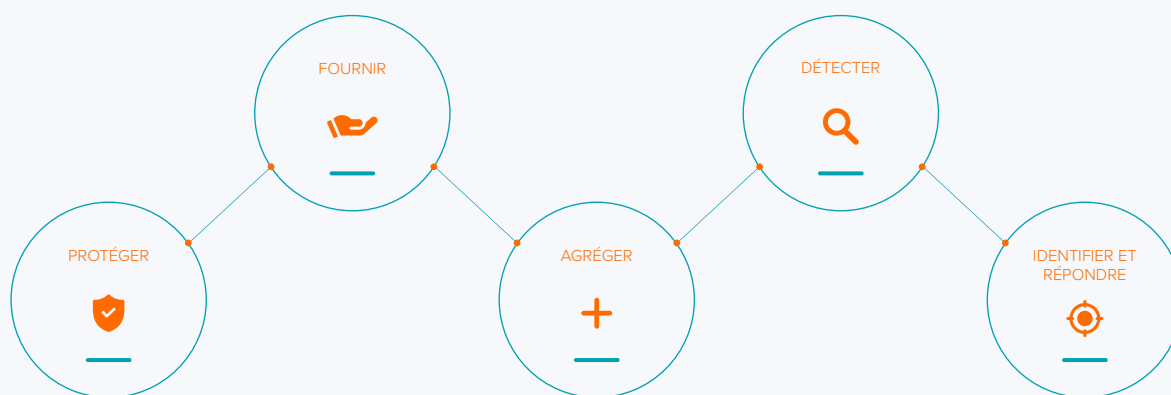
Pour mieux gérer le risque lié à l'intégration de l'IT et de l'OT, **les organisations ont besoin d'une visibilité complète de leur réseau en suivant et en surveillant les actifs, les vulnérabilités et les contrôles opérationnels**, et en identifiant rapidement tout changement inhabituel.

Les réseaux OT sont souvent peuplés de nombreux appareils « fantômes », inconnus des gestionnaires et représentant une menace importante pour la sécurité. Avec une telle incertitude, **il est important que les outils IT, OT et IoT travaillent conjointement pour verrouiller votre réseau**. Les fonctions intelligentes de filtrage et de mise en forme du réseau protègent vos précieux actifs OT en garantissant que les paquets réseau sont toujours acheminés au bon endroit et au bon moment.

COMMENT LES ORGANISATIONS PROTÈGENT LEUR OT AVEC GIGAMON ET NOZOMI NETWORKS

Conjointement, Gigamon et Nozomi Networks fournissent aux grandes entreprises et aux organisations du monde entier une visualisation en temps réel de leur réseau et une détection des menaces à la minute près pour leurs actifs OT :

- + **Protection des réseaux de contrôle industriels** contre les cyber-attaques et les perturbations opérationnelles par l'analyse passive du trafic réseau
- + **Fourniture d'un inventaire complet des actifs OT** et d'une évaluation de la vulnérabilité
- + **Agrégation de données pour des centaines d'installations industrielles distribuées**, fournissant un accès consolidé et à distance à vos données ICS à partir de dispositifs Guardian déployés sur le terrain
- + **Détection des menaces connues et inconnues**, renforcée par l'IA et la technologie d'apprentissage automatique de Nozomi Network pour détecter les anomalies
- + **Identification et réponse** plus rapide aux alertes de sécurité les plus **importantes**.



VISIBILITÉ COMPLÈTE SUR L'IT ET L'OT

Vous ne pouvez pas protéger et sécuriser ce que vous ne voyez pas. **La visibilité est fondamentale pour la cyber-résilience, la détection, la protection et l'atténuation.**

Gigamon se positionne entre le réseau d'entreprise OT, la fabrication, le réseau de process et les outils, tels que Nozomi Networks, pour fournir une visibilité quel que soit le support (physique, virtuel, cloud) et en incluant le trafic est-ouest.

En résumé, **la solution conjointe permet une visibilité complète et intégrée des actifs IT et OT.** La solution Visibility and Analytics Fabric de Gigamon garantit que le trafic pertinent est transmis à Nozomi Networks Guardian et aux autres outils de manière efficace et dans le format requis.

Elle agrège les liens à faible volume avant de les transmettre, supprime les doublons de paquets pour éviter les surcharges inutiles et offre un contrôle plus facile du routage asymétrique pour rassembler les informations de session à des fins d'analyse par les outils de sécurité de Nozomi Networks.

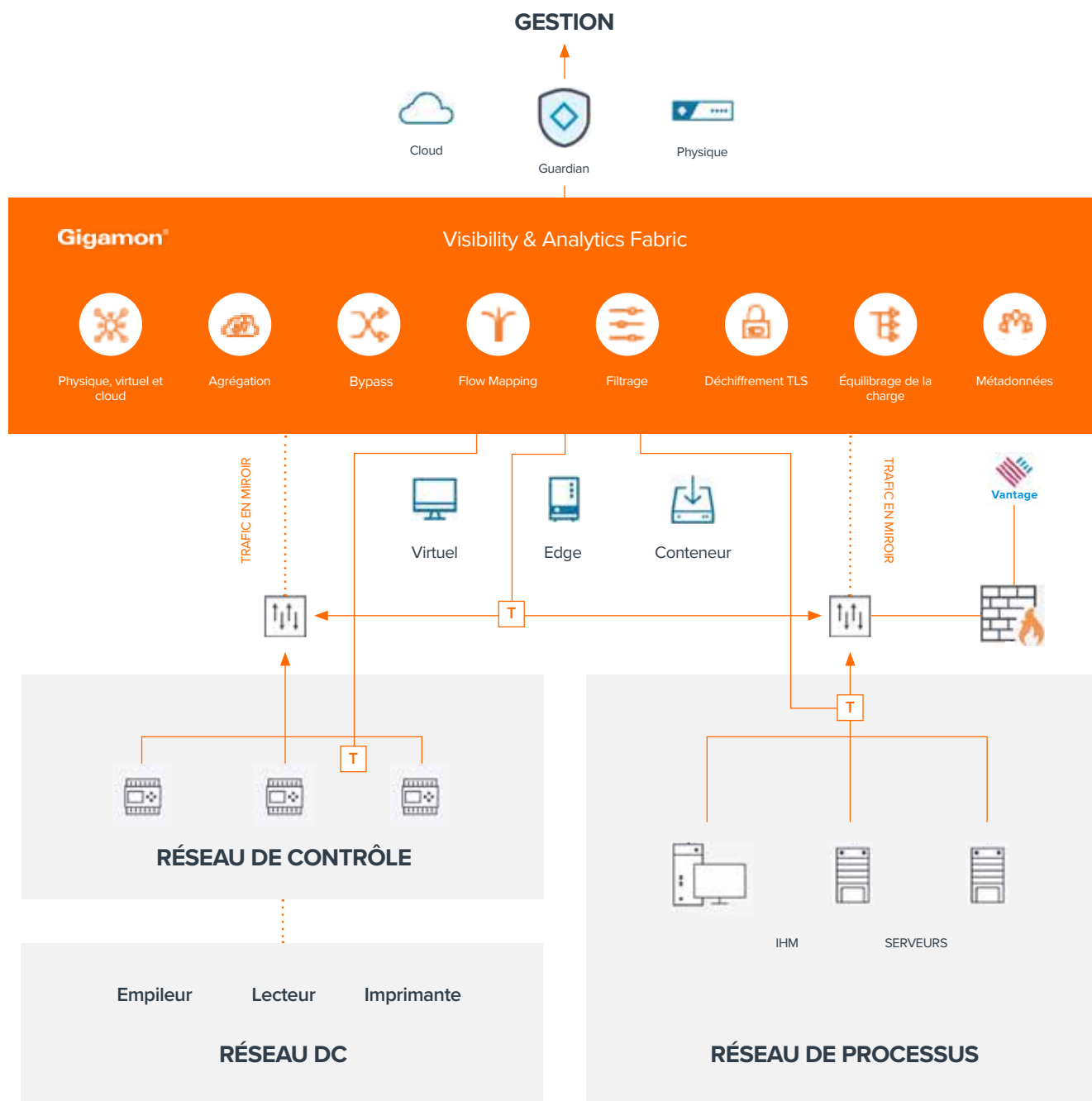
PROTÉGEZ VOTRE OT AVEC GIGAMON ET NOZOMI NETWORKS

- + Les taps unidirectionnels optionnels de Gigamon garantissent que le trafic des produits OT ne subit pas d'impact négatif.
- + Quelle que soit la provenance du trafic de vos appareils, y compris les sources sans fil pour les appareils à distance, Gigamon garantit qu'aucun angle mort ne subsiste sur votre réseau. Ce qui inclut même la visibilité de l'activité de gestion des identités et des accès afin de garantir une sécurité fondamentale.
- + La disponibilité est obligatoire pour les réseaux de production d'OT. Les taps actifs/passifs et le bypass inline de Gigamon offrent une capacité d'ouverture en cas de défaillance pour garantir une disponibilité constante, y compris lorsque des opérations de maintenance doivent être effectuées sur les outils de sécurité.
- + Si nécessaire, Gigamon peut fournir un décryptage TLS/SSL centralisé du trafic crypté, où les logiciels malveillants aiment se cacher.
- + Nozomi Networks répertorie les actifs technologiques opérationnels de votre réseau, analyse ses vulnérabilités et établit une base de référence de l'état normal afin de minimiser les temps d'arrêt.
- + Nozomi Networks assure la détection des anomalies dans les événements opérationnels et de sécurité grâce à sa technologie unique d'intelligence artificielle et d'apprentissage automatique.

En outre, la solution VAF de Gigamon :

- + un équilibrage de la charge pour répartir le volume du trafic sur plusieurs instances des outils Nozomi Networks.
- + la suppression des labels pour améliorer l'efficacité des outils de Nozomi Networks
- + le masquage pour le respect de la confidentialité des données
- + une gestion à guichet unique pour simplifier et réduire la charge des opérateurs et des professionnels de la sécurité.

DÉPLOIEMENT DE NOZOMI NETWORKS AVEC GIGAMON



À PROPOS DE GIGAMON ET DE NOZOMI NETWORKS



Gigamon permet à votre organisation d'opérer avec rapidité, de rester protégée et d'innover. Nous sommes la première société à offrir une visibilité réseau unifiée et des analyses sur toutes les données en temps réel.

Nous agrégeons, transformons et analysons le trafic réseau sur vos infrastructures physiques, virtuelles et de cloud pour répondre aux besoins critiques de performance, y compris la détection et la réponse rapide aux menaces, libérant ainsi votre entreprise pour qu'elle puisse se consacrer à l'innovation numérique. Plus de 4000 clients, dont 83 des entreprises du Fortune 100, nous font confiance.



Nozomi Networks accélère la transformation numérique en protégeant les infrastructures critiques du monde, ainsi que les organisations industrielles et gouvernementales contre les cyber-menaces.

Notre solution offre une visibilité exceptionnelle sur le réseau et les équipements, la détection des menaces et des informations opérationnelles précises pour les environnements OT et IoT. Les clients comptent sur nous pour minimiser les risques tout en maximisant la résilience.

©2021 Gigamon. Tous droits réservés. Gigamon et le logo Gigamon sont des marques déposées de Gigamon aux États-Unis et/ou dans d'autres pays. Les marques déposées de Gigamon sont disponibles sur www.gigamon.com/legal-trademarks. L'ensemble des autres marques déposées sont la propriété de leurs propriétaires respectifs. Gigamon se réserve le droit de changer, modifier, transférer ou autrement réviser cette publication sans préavis.



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