WatchGuard®

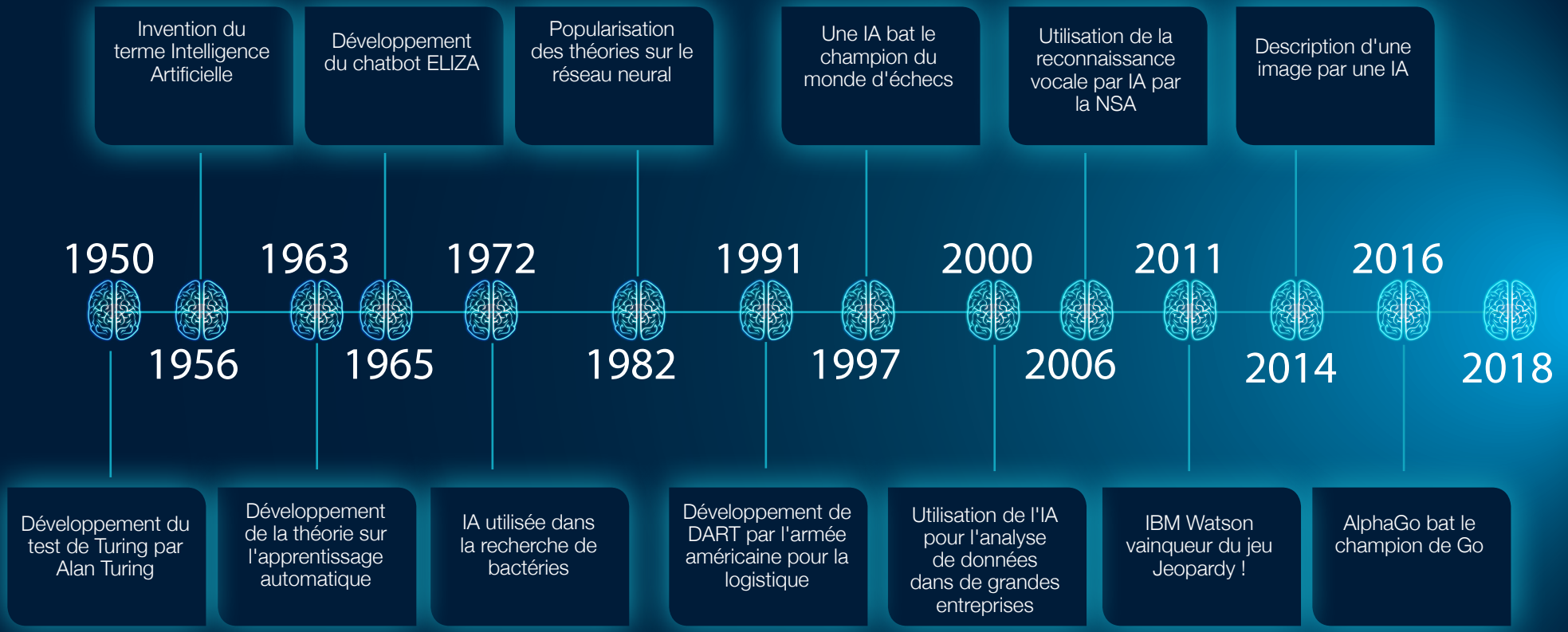
L'INTELLIGENCE ARTIFICIELLE

Une couche de sécurité indispensable

Qu'est-ce que l'Intelligence Artificielle ?

De manière générale, on définit l'Intelligence Artificielle (IA) comme le processus de développement de systèmes informatiques qui s'adaptent à l'évolution des circonstances et effectuent des tâches nécessitant normalement l'intervention de l'intelligence humaine. Si pour beaucoup, l'IA est une vraie nouveauté, ce concept remonte au moins aux années 1950. Des pionniers des sciences de l'informatique comme Alan Turing avaient déjà avancé que dans un avenir certain, les ordinateurs seraient en mesure d'imiter le travail des humains et d'effectuer des tâches « intelligentes », comme jouer aux échecs. Au cours des soixante dernières années, les effets de mode et les espoirs entourant l'IA sont apparus à mesure que les progrès informatiques ont rendu possible l'analyse d'ensembles de données conséquents et ouvert la porte à de nouvelles applications.

L'Intelligence Artificielle à travers les âges

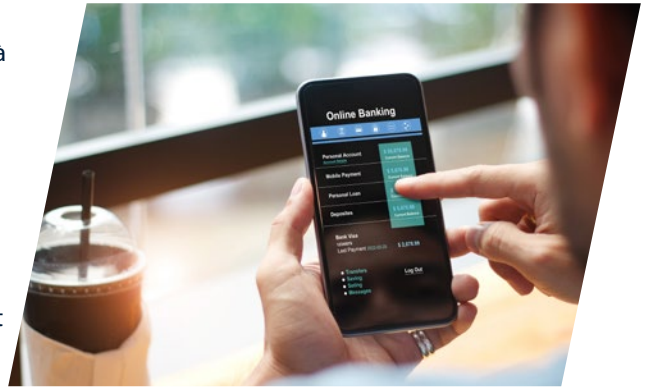


L'ascension vertigineuse de l'IA

Ces vingt dernières années, les capacités de l'IA ont connu des avancées fulgurantes. Souvenons-nous de ce jour de 1997 où Deep Blue d'IBM a failli battre le champion du monde d'échecs Gary Kasparov, ou encore de la victoire, en 2011, de Watson AI sur les champions du Jeopardy, Brad Rutter et Ken Jennings, démontrant ainsi que l'Intelligence Artificielle était désormais entrée dans les mœurs.

Nous utilisons aujourd'hui les éléments de l'Intelligence Artificielle dans bien des aspects de notre quotidien :

- **Les applications de covoiturage** comme Uber et Lyft utilisent l'IA et le Machine Learning pour fixer le prix des courses, anticiper les demandes et estimer l'heure d'arrivée, allant même jusqu'à recommander aux conducteurs de se déplacer pour récupérer leurs clients en fonction des tendances émergeant de millions de situations fructueuses ou complexes.
- **La remise de chèques** par smartphone nécessite un système complexe d'IA et de Machine Learning pour déchiffrer et convertir correctement en texte l'écriture manuscrite des chèques.
- **Les jeux vidéo** utilisent depuis longtemps des éléments d'IA pour proposer de nouveaux défis aux joueurs, avec des ennemis maintenant capables d'interagir avec leur environnement et de tirer des enseignements de rencontres antérieures avec le joueur pour augmenter leurs chances de réussite.
- **Les capacités de recommandation de morceaux de musique et de films** de Spotify, Netflix et Pandora ont recours à un système simple d'IA pour vous proposer de nouveaux supports correspondant à vos centres d'intérêts et à des avis antérieurs.
- **La gestion des investissements** devient plus intelligente, l'IA ayant pris la tête du développement de portefeuilles financiers respectant les objectifs d'investissement et la tolérance au risque du client, et gérant les portefeuilles en temps réel selon l'évolution du marché.
- **Les chatbots et les assistants virtuels** sont désormais en première ligne du service client de nombreuses marques et gèrent tout, du recrutement à l'assistance technique.



L'Intelligence Artificielle fait désormais partie intégrante de nos vies et l'adoption de nouvelles technologies va très probablement connaître une croissance exponentielle dans les années à venir. De fait, d'après un rapport récent de PWC, l'impact économique total de l'IA devrait atteindre les 15,7 billions de dollars d'ici 2030.

Toutefois, l'adoption et l'évolution de l'IA ne sont pas sans susciter de fortes inquiétudes, les sceptiques avançant de nombreux arguments allant du risque de perte d'emploi du fait de l'automatisation aux craintes quant à la capacité des ordinateurs à effectuer les tâches complexes pour lesquelles ils ont été conçus, comme la conduite.

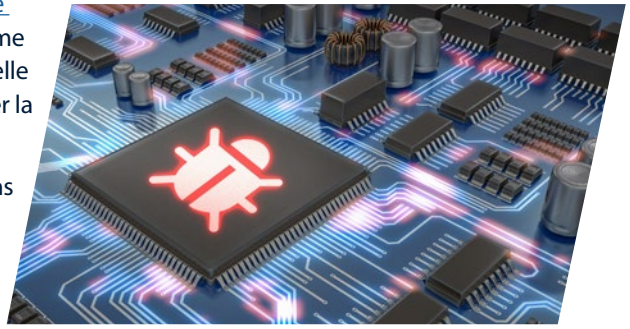
L'IA au service des cybercriminels ?

L'un des principaux avantages de l'Intelligence Artificielle est sa capacité à agir comme caisson de résonance, car elle est en mesure d'exploiter de grandes quantités de données complexes et d'effectuer des tâches très répétitives nécessitant habituellement l'intervention humaine. L'automatisation de tâches traditionnellement manuelles permet aux criminels, et en particulier aux cybercriminels, d'améliorer leur ciblage, d'élargir l'impact de leurs attaques et d'accélérer considérablement la vitesse à laquelle ils peuvent créer de nouveaux malwares. Se basant sur quelques exemples d'attaques ayant eu recours à l'IA, les chercheurs en sécurité travaillent d'arrache-pied pour étudier le vaste champ des possibles.

Voici quelques exemples de recherches sur la façon dont les pirates informatiques pourraient utiliser l'IA :

- **Contournement des systèmes CAPTCHA.** Le système CAPTCHA est devenu un outil essentiel sur Internet, car il nous permet de déterminer si les visiteurs de notre site sont des humains ou des robots. Il montre au visiteur une image, une case à cocher ou un morceau de texte déformé en lui demandant d'effectuer une action nécessitant normalement l'intervention humaine, comme l'identification d'images qui se ressemblent. Grâce à des techniques d'IA, les chercheurs de l'université Columbia ont pu contourner Google reCAPTCHA 98% du temps.

- **Amélioration de la précision et de la portée du phishing.** 76% des entreprises auraient été victimes d'attaques de phishing en 2017. Bon nombre d'entre elles ont donc mis en œuvre des programmes stricts de formation de leurs employés à l'identification des tentatives de phishing en vue de prévenir ces attaques. Grâce à l'IA, les cybercriminels peuvent désormais parcourir des volumes énormes de données sur leurs cibles et produire des messages leur garantissant un plus grand pourcentage de réussite. Des recherches en matière de sécurité effectuées par ZeroFox ont démontré cette approche de ciblage d'utilisateurs de Twitter avec SNAP_R (Phishing automatisé sur les réseaux sociaux avec reconnaissance). SNAP_R a recours à l'IA pour identifier les cibles intéressantes et générer rapidement un profil de cette cible d'après ses anciens tweets. Cette approche permet d'inciter les cibles à cliquer sur des liens malveillants 30% du temps (contre 5 à 15% du temps pour d'autres approches automatisées).



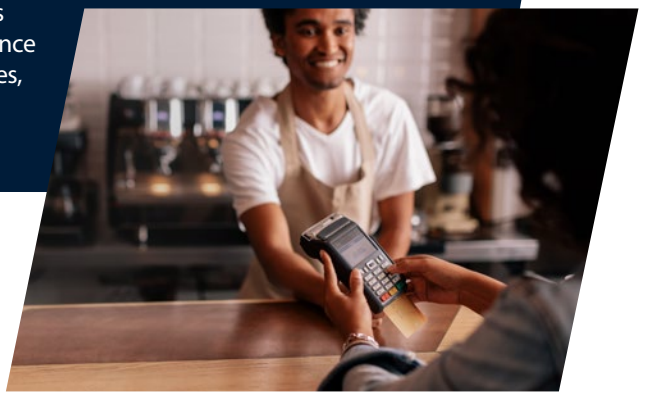
- **Développement de malwares très évasifs.** Les pirates informatiques ont pendant longtemps eu besoin de scripts et de boîtes à outils pour développer et diffuser des malwares. Mais à mesure que la cyberdéfense gagne en intelligence et en sophistication, nos adversaires ont adopté des techniques d'Intelligence Artificielle basiques pour améliorer le caractère évasif de leurs malwares. Les auteurs de malwares ont commencé à utiliser l'IA pour effectuer des contrôles en vue d'identifier la configuration et l'environnement informatiques en présence (par exemple, une sandbox ou une machine physique), et de déterminer si la machine est utilisée par un humain à un moment donné. DeepLocker, développé par des chercheurs d'IBM Research, montre les dangers que présente l'utilisation de l'Intelligence Artificielle comme une arme dans les malwares. En effet, l'IA de DeepLocker a été formée pour n'exécuter sa charge utile que lorsqu'elle atteint un objectif spécifique, et utilise 3 couches de dissimulation pour empêcher les outils de sécurité d'identifier la menace.

La course à l'armement en matière de cybersécurité n'en est qu'à ses débuts et nous pouvons affirmer que nous entrons dans une nouvelle ère, au cours de laquelle l'IA et le Machine Learning joueront un rôle toujours croissant tant au niveau des attaques que des lignes de défense.

Une couche de sécurité indispensable pour les entreprises de toutes tailles

Les cyberattaques sont fulgurantes. Le moindre point d'infection peut se répandre comme une traînée de poudre, de postes de travail en poste de travail, de site en site et d'entreprise en entreprise. Les approches traditionnelles de protection se basent principalement sur des processus manuels et les stratégies préétablies de blocage des attaques ne parviennent pas à suivre le rythme des menaces, par nature en constante évolution.

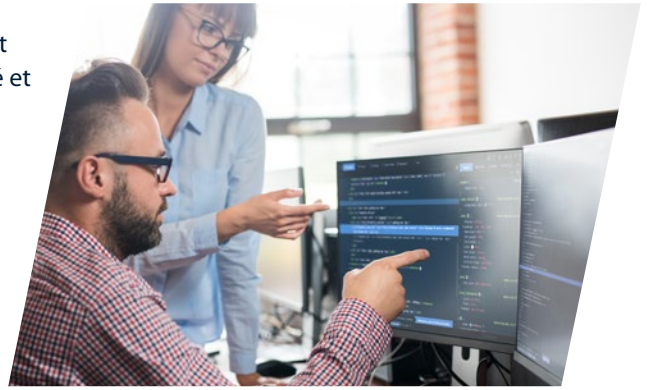
Le traitement de volume considérable d'indicateurs sur les menaces est un processus intensif et chronophage, même pour les équipes les plus qualifiées. Vos équipes informatiques sont probablement déjà dépassées par le volume des alertes et des faux positifs, et des attaques peuvent passer inaperçues pendant des mois. C'est là que l'IA peut apporter une valeur ajoutée considérable. En vous basant sur l'Intelligence Artificielle, vous pourrez gagner du temps, mettre en corrélation davantage de données, prendre des décisions plus rapides et plus éclairées, réduire le risque d'erreurs humaines et prédire les tendances futures des menaces tout en améliorant considérablement votre système de sécurité.



Quels sont les problèmes que l'IA peut vous aider à résoudre ?

Le manque d'expertise en matière de sécurité

- De nombreuses entreprises, en particulier les petites, ne disposent pas des effectifs et de l'expertise nécessaires en matière de sécurité. Les fonctions des équipes informatiques sont souvent floues et celles-ci doivent porter plusieurs casquettes. L'IA permet d'automatiser les processus de sécurité et ainsi de gagner du temps qui peut être consacré à des tâches stratégiques par les équipes informatiques. En effet, l'IA est capable de remplir des fonctions nécessitant normalement l'intervention d'un analyste qualifié de la sécurité, de comprendre des quantités conséquentes de données de sécurité et d'agir automatiquement pour améliorer votre niveau de sécurité global.

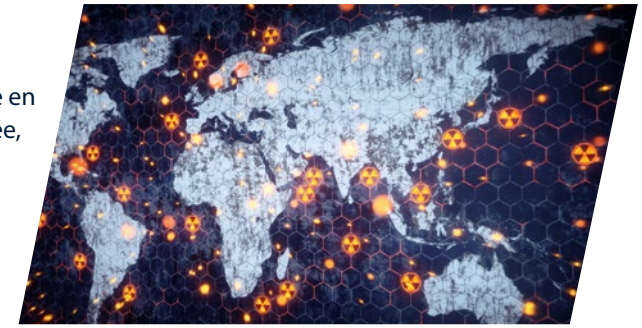


Les restrictions au niveau des ressources

- Les petites entreprises au budget serré ne peuvent se permettre de se doter de SIEM et d'outils de gestion de la sécurité. Et même si elles possèdent les données, les contraintes de temps les empêchent de les analyser et de les exploiter dans des délais efficaces. Bien mise en œuvre, l'IA peut effectuer pour vous des tâches de mise en corrélation, d'analyse et de notation tout en apprenant auprès de différentes sources d'intelligence sur les menaces pour garantir sa cybervigilance. De plus, l'IA vous permet d'automatiser la résolution en réduisant au minimum la perturbation de vos activités.

Les menaces de type Zero Day et les malwares évasifs

- Les stratégies et les bases de signatures peuvent rapidement devenir obsolètes et dépassées et si elles sont le seul rempart, cela engendre des failles de sécurité importantes. L'IA offre des couches intelligentes de défense en mesure de détecter et de contrer les malwares bien plus rapidement que les anciennes approches. Bien formée, l'IA offre des protections prédictives anticipant les menaces futures sans nécessiter de bases de signatures, de connectivité au Cloud, etc. L'IA peut examiner les centaines de milliers de caractéristiques d'un fichier donné pour déterminer rapidement son niveau de menace.



L'IA oeuvre comme un analyste automatisé de la Sécurité au service de vos équipes

Tous les analystes de la sécurité ont pour objectif de prévenir les attaques le plus efficacement possible tout en étant en mesure de détecter les menaces et d'y réagir le plus tôt possible. L'automatisation de l'IA revient à pouvoir compter sur un analyste qualifié de la sécurité travaillant 24 h/24, 7 j/7 pour vous protéger. L'IA permet d'automatiser :

PRÉVENTION	DÉTECTION	RÉPONSE
Sans signature ou connectivité sur le cloud	Par des outils d'apprentissage automatique pour les analyses statiques et dynamiques	Par une notation corrélée des menaces

L'IA au coeur du portefeuille de WatchGuard

L'Intelligence Artificielle intégrée au sein du portefeuille de services de sécurité WatchGuard agit comme un multiplicateur permettant d'automatiser les processus et d'améliorer considérablement notre couverture des menaces émergentes. À mesure que les mises en œuvre de l'IA à des fins de sécurité continuent de progresser, nous relierons l'ensemble de nos plateformes les unes aux autres pour proposer le set d'informations le plus complet et le plus pointu possible, de la manière la plus simple et la plus pratique qui soit, afin de dresser un rempart des plus hermétiques, à même de contrer la totalité des attaques à venir.

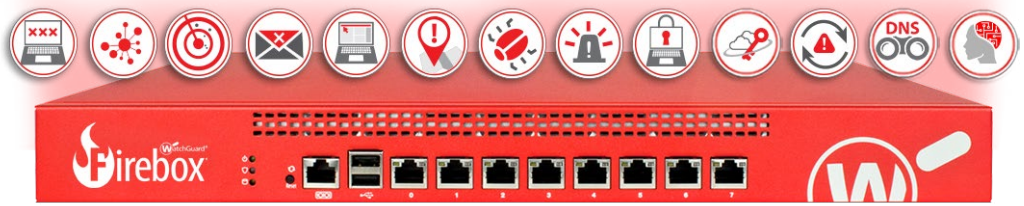
Que pouvez-vous attendre de l'IA intégrée au sein du portefeuille de WatchGuard ?

Une protection prédictive. Le délai qui sépare la découverte d'un malware et l'application des signatures, des analyses heuristiques et des modèles de comportement constitue un défi considérable. IntelligentAV offre une couverture prédictive contre les menaces de malware avec une moyenne de 25 mois avant leur apparition.

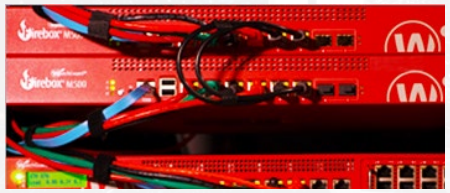
Un délai de détection raccourci. La détection et la destruction dans les temps des malwares invasifs supposent de savoir comment examiner des milliers d'indicateurs malveillants. ThreatSync, en conjonction avec notre service de sécurité APT Blocker, détecte les fichiers suspects et les envoie automatiquement dans une sandbox nouvelle génération dans le Cloud en vue d'une analyse plus approfondie. APT Blocker utilise l'IA au cours du processus d'inspection approfondie afin de procéder à une analyse complète des fichiers.

Une défense automatisée contre les menaces. L'Intelligence Artificielle permet de collecter de grandes quantités de données auprès de toutes les sources imaginables ou presque, et d'utiliser ces données pour entraîner automatiquement l'IA en vue d'obtenir d'encore meilleurs résultats en matière de cybersécurité. IntelligentAV, APT Blocker et ThreatSync apprennent en permanence grâce à un flux constant de nouvelles données et de retours d'informations, et mettent à profit cet entraînement pour améliorer votre niveau de sécurité global.

Étant donné la sophistication des menaces émergentes et la vitesse d'évolution de ces menaces, l'Intelligence Artificielle est un outil indispensable dans la course à l'armement cybernétique des entreprises de toutes tailles. Leader en matière de sécurité, WatchGuard continue d'innover pour faire progresser ses produits et ses services grâce aux technologies reposant sur l'IA.



LE PORTEFEUILLE DES SOLUTIONS DE SÉCURITÉ WATCHGUARD



Sécurité Réseau

En plus de garantir une sécurité de pointe à votre entreprise, notre plateforme a été spécialement conçue pour un déploiement, une utilisation et une gestion intuitifs, faisant de WatchGuard la solution idéale pour les TPE, les PME, les ETI, les administrations et les entreprises du monde entier.

Wi-Fi Sécurisé

Conçue pour offrir un environnement Wi-Fi fiable et sécurisé, éliminant les tâches d'administration fastidieuses et réduisant considérablement les coûts, la solution de Wi-Fi sécurisé WatchGuard change littéralement la donne sur le marché actuel. Avec des outils d'engagement exhaustifs et une parfaite visibilité sur vos données d'entreprise, cette solution confère à votre entreprise un avantage concurrentiel indéniable.

Authentification Multifacteur

WatchGuard AuthPoint est la solution idéale pour combler la faille de sécurité qu'implique le recours à des mots de passe qui rendent les entreprises vulnérables à la fuite de données. Il offre une authentification multifacteur sur une plateforme Cloud simple d'utilisation. Notre approche unique se démarque aussi grâce au facteur « ADN de téléphone portable » qui permet de garantir que seules les personnes autorisées ont accès aux réseaux et aux applications Cloud sensibles.

En savoir plus

Pour plus d'informations, contactez votre revendeur agréé WatchGuard ou visitez notre site à l'adresse suivante : **https://www.watchguard.com.**.

À propos de WatchGuard

WatchGuard® Technologies, Inc. est un leader mondial de la sécurité réseau, des connexions Wi-Fi sécurisées, de l'authentification multifacteur et de l'intelligence réseau. Les produits et les services récompensés de WatchGuard sont recommandés par plus de 10 000 revendeurs et prestataires de services spécialisés dans la sécurité et protègent plus de 80 000 clients dans le monde. WatchGuard a pour mission de rendre la sécurité de pointe accessible aux entreprises de tous types et de toutes tailles, ce qui en fait la solution idéale pour les entreprises multisites et pour les PME. L'entreprise a établi son siège social à Seattle, dans l'État de Washington, et possède des bureaux dans toute l'Amérique du Nord, en Europe, en Asie-Pacifique et en Amérique latine. Pour en savoir plus, rendez-vous sur le site WatchGuard. fr.

Service commercial Amérique du Nord : 1.800.734.9905 • Service commercial international : 1.206.613.0895 • Site Web : www.watchguard.com

Le présent document ne contient aucune garantie expresse ou tacite. Toutes les spécifications peuvent faire l'objet de modifications, et les futurs produits, caractéristiques ou fonctionnalités prévus seront fournis dès qu'ils seront disponibles.
© 2019 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, le logo WatchGuard, Firebox et AuthPoint sont des marques commerciales ou des marques déposées de WatchGuard Technologies, Inc. aux États-Unis et/ou dans d'autres pays.
Toutes les autres marques commerciales appartiennent à leurs détenteurs respectifs. Référence WGCE671403_030719