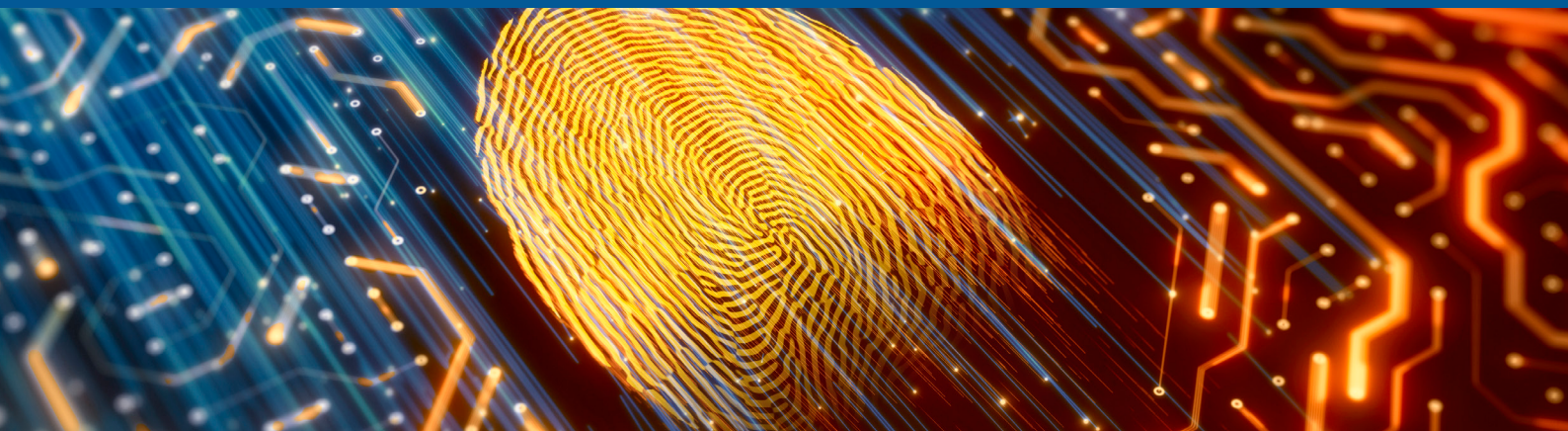




AuthPoint Identity Security

Remarquablement simple. Fortement sécurisé.

Il suffit d'un seul identifiant compromis pour nuire gravement à une entreprise voire stopper son activité. La sécurité des identités doit être la première ligne de défense contre les cyberattaques.

AuthPoint Identity Security offre la sécurité dont vous avez besoin pour protéger les identités, les actifs, les comptes et les informations. Permettez à vos collaborateurs de travailler en toute confiance et sans souci grâce à des solutions d'authentification multifacteur et de gestion des informations d'identification faciles à utiliser, rentables et complètes. De plus, répondez aux exigences en matière de framework de sécurité, de conformité et de cyberassurance liées à l'authentification des utilisateurs et au contrôle d'accès.

- Permet un accès distant sécurisé avec des réseaux privés virtuels (VPN)
- Offre une expérience transparente aux employés grâce à une technologie de sécurité simple à utiliser
- Assure la conformité réglementaire et répond aux exigences en matière de cyberassurance



« AuthPoint respecte sa promesse d'authentification multifacteur en limitant le risque inhérent aux mots de passe vulnérables sans compromettre la facilité d'utilisation pour les employés et le personnel informatique.

*Tout est compris dans le service Cloud – il n'y a aucun matériel à installer ni de logiciels à entretenir...
Le MFA est désormais considérée comme une protection essentielle et la solution proposée par WatchGuard répond à tous les besoins. »*

Tom Ruffolo
CEO, eSecurity Solutions

Principaux défis auxquels les entreprises sont confrontées en ce qui concerne les identifiants des employés



82 %

Des violations de données impliquent un élément humain. Les personnes sont donc le facteur principal

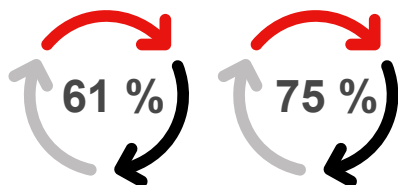
65 %

Des identifiants volés sont mis en vente en moins d'une journée. Les informations personnelles identifiables (PII) représentent un chiffre d'affaires de 40 milliards de dollars sur le marché du dark web



55 %

Des entreprises continueront de travailler sous des formes hybrides ou à distance



Grande entreprise vs PME

Violations de données impliquant l'utilisation d'identifiants volés



Vie professionnelle vs vie privée

Taux de réutilisation des mots de passe dans les applications et les services



Des entreprises prévoient d'externaliser la sécurité et d'augmenter les contrôles d'authentification et d'accès

Solutions AuthPoint Identity Security

Atténuer les risques associés aux attaques généralisées contre les identités des employés

Il DNA del dispositivo mobile: ottimizza la protezione MFA per smartphone

Le MFA d'AuthPoint est conçu pour être résistant au spam (fatigue attack), permettant des mesures d'authentification plus efficaces avec des fonctionnalités telles qu'un bouton contre le phishing qui permet d'éviter à l'utilisateur d'autoriser une attaque par mégarde. Notre VPN facile à déployer et rapide ainsi que notre accès à distance offrent des chemins d'accès sécurisés avec un minimum d'effort. Avec les méthodes d'authentification hors ligne et en ligne disponibles, vous pouvez facilement vous assurer que votre système dispose toujours d'une sécurité forte. De plus, le vaste écosystème d'intégrations et la norme SAML offrent un accès complet, donnant aux entreprises la possibilité de contrôler les permissions d'accès des utilisateurs rapidement et efficacement.



MFA AuthPoint

Authentification multifacteur seulement

Surveillance du Dark Web : Agissez lorsque des identifiants atterrissent sur le Dark Web

La surveillance du Dark Web est un service proactif qui informe les clients si des identifiants compromis appartenant à des domaines surveillés sont trouvés dans une nouvelle base de données publiée sur notre service. Ces notifications peuvent être envoyées aux administrateurs ainsi qu'aux utilisateurs concernés par la fuite, afin que ces derniers puissent changer leur mot de passe de manière proactive. Une licence permet de surveiller jusqu'à trois domaines.



AuthPoint Total Identity Security

Authentification multifacteur ET gestion des identifiants

ADN mobile : améliorer la protection MFA avec les smartphones

La protection MFA AuthPoint protège contre les menaces d'échange de cartes SIM en vérifiant le téléphone de l'utilisateur à l'aide des fonctionnalités uniques et des données cryptées d'un appareil mobile. Cela permet un accès sécurisé et empêche les tentatives de clonage.

Sécurité de connexion : protection de l'accès aux appareils Windows et Mac

Les agents logiciels AuthPoint peuvent être installés sur n'importe quelle machine, quel que soit le système d'exploitation. Que vous utilisiez un système d'exploitation macOS, Windows ou Linux, le logiciel s'intègre parfaitement aux systèmes existants. Grâce aux méthodes de vérification en ligne et hors-ligne disponibles, ce logiciel garantit des processus de connexion sécurisés sans sacrifier le confort des utilisateurs.

Les pirates ne forcent plus l'entrée – ils ne font que se connecter

AuthPoint permet un environnement d'accès adaptatif pour plus de productivité et moins de dépenses



Framework Zero Trust

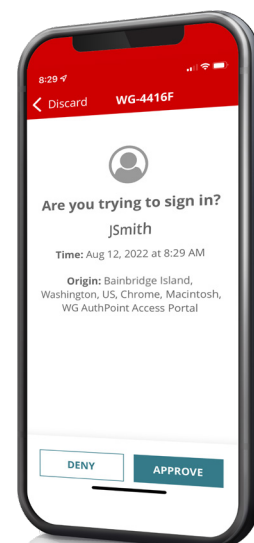
L'adoption du Zero Trust ne peut pas fonctionner sans protection des identités. Nos stratégies d'accès basées sur les risques permettent d'autoriser l'accès au bon utilisateur au bon moment. AuthPoint fournit des stratégies d'authentification et de risque personnalisables sans frais supplémentaires, y compris des capacités de réseau, de temps, et de géofencing.

Garantie étendue avec authentification unique (SSO)

La technologie d'authentification unique (SSO) sécurisée d'AuthPoint permet aux utilisateurs d'accéder en toute simplicité à plusieurs applications Cloud, VPN ou réseaux, avec un seul jeu d'identifiants. Cela réduit les problèmes de fatigue de mot de passe et les risques de vulnérabilités liés aux mots de passe faibles, ainsi que les coûts associés aux réinitialisations de mots de passe.

Faible coût total de possession

Les entreprises disposant d'un service informatique réduit et de connaissances limitées en matière de sécurité bénéficieront de la protection apportée par le MFA, qui est facile à déployer et à gérer depuis le Cloud. Que vous déployiez uniquement une solution MFA ou la Total Identity Security, AuthPoint offre une structure de prix tout compris par utilisateur et par mois, pour permettre aux entreprises d'adopter pleinement des mesures de sécurité des identités sans coût supplémentaire.

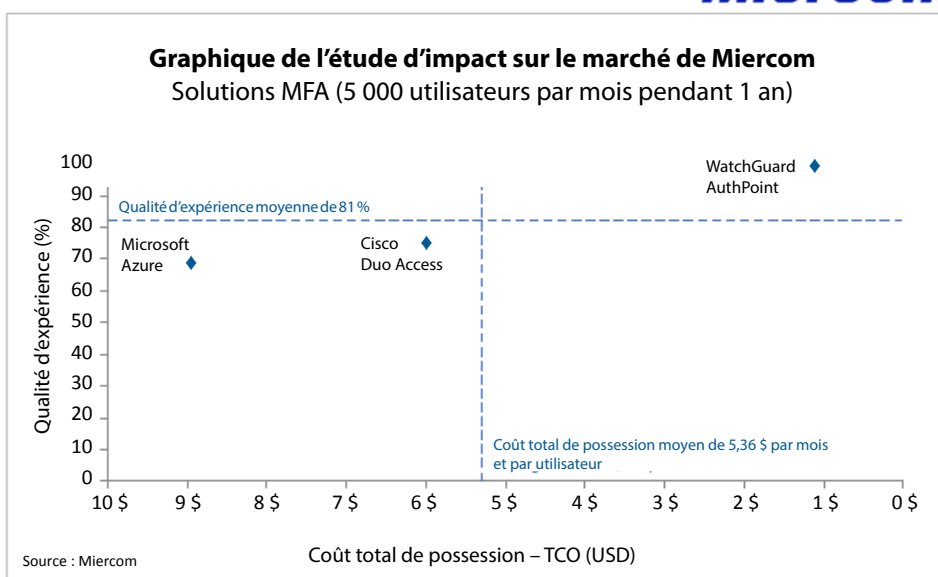


Validation technique tierce partie par Miercom

Miercom, un laboratoire informatique qui fournit des validations tierces, a accordé à la solution AuthPoint MFA de WatchGuard la certification Performance Verified. Cette évaluation a testé AuthPoint et validé son ergonomie et ses performances par rapport à Cisco Duo et Azure MFA.

Haute valeur ajoutée et RSI compétitif

WatchGuard a montré la plus grande valeur ajoutée par sa qualité d'expérience. Par rapport à d'autres solutions, WatchGuard a fourni un riche ensemble de fonctionnalités natives avec un achat unique, tandis que les autres solutions ont ajouté de la complexité et des coûts, nécessitant l'achat d'abonnements supplémentaires.



Les quadrants sont formés à partir de valeurs moyennes. WatchGuard se situe dans le quadrant supérieur droit, ce qui signifie qu'il offre la qualité d'expérience la plus élevée parmi les fournisseurs concurrents, au prix le plus bas. Par rapport à WatchGuard, Cisco et Microsoft offrent beaucoup moins de fonctionnalités et une interface moins intuitive et moins conviviale.

LE PORTEFEUILLE DE WATCHGUARD



Sécurité réseau

WatchGuard fournit une large gamme de solutions de sécurité réseau, comprenant des appliances tabletop et d'autres montées en rack 1U, ainsi que des firewalls virtuels et dans le Cloud. Nos appliances Firebox® fournissent des services de sécurité essentiels, allant de l'IPS standard, du filtrage d'URL, de la passerelle AV, du contrôle d'application et de l'antispam, à des protections avancées telles que le sandboxing de fichiers, le filtrage DNS et plus encore. L'inspection approfondie des paquets (DPI) haute performance signifie que vous pouvez tirer parti de tous nos services de sécurité contre les attaques qui tentent de se cacher dans des canaux cryptés comme HTTPS. De plus, chaque appliance Firebox fournit des fonctionnalités SD-WAN prêtes à l'emploi pour améliorer la résilience et les performances du réseau.



Sécurité des identités

WatchGuard AuthPoint® permet de combler la faille de sécurité qu'induit le recours à des mots de passe au moyen d'une authentification multifacteur, via une plateforme Cloud facile à utiliser. L'approche unique de WatchGuard se démarque grâce au facteur « ADN de téléphone portable » qui permet de vérifier que seules les personnes autorisées ont accès aux réseaux et aux applications Cloud sensibles. AuthPoint offre également une expérience utilisateur optimisée avec des méthodes d'authentification en ligne et hors ligne, ainsi qu'un portail d'applications Web pour un accès facile à l'authentification unique.



Wi-Fi Cloud sécurisé

Les solutions Wi-Fi sécurisées et gérées dans le Cloud de WatchGuard fournissent un espace en ligne sûr et protégé pour les environnements Wi-Fi tout en éliminant les maux de tête administratifs et en réduisant considérablement les coûts. Des bureaux à domicile aux vastes campus d'entreprise, WatchGuard propose la technologie Wi-Fi 6 avec chiffrement WPA3 sécurisé. Avec WatchGuard Cloud, la configuration du réseau Wi-Fi et l'administration des politiques, le déploiement sans contact, les portails captifs personnalisés, la configuration VPN, les outils d'engagement avancés, la visibilité sur les analyses commerciales et les mises à niveau sont à portée de clic.



Sécurité des postes de travail

Les solutions de sécurité des endpoints de WatchGuard vous aident à protéger vos appareils contre les cybermenaces. Nos solutions endpoints phares fondées sur l'IA, que sont WatchGuard EPDR et Advanced EPDR, renforcent votre posture en matière de sécurité en intégrant de manière transparente la fonctionnalité de protection des endpoints (EPP) aux capacités de détection et de réponse (EDR), aux côtés de nos services Zero-Trust Application et Threat Hunting. Tous sont étroitement intégrés dans WatchGuard Cloud et ThreatSync, offrant une visibilité et une intelligence précieuses tout en renforçant la détection et la réponse multiproduit (XDR).

À propos de WatchGuard

WatchGuard® Technologies, Inc. est un leader mondial de la cybersécurité unifiée. Notre approche Unified Security Platform® est pensée pour les fournisseurs de services managés afin d'assurer une sécurité de pointe augmentant l'évolutivité et la vélocité de leur entreprise tout en améliorant leur efficacité opérationnelle. Recommandés par plus de 17 000 revendeurs et prestataires de services spécialisés dans la sécurité et adoptés par plus de 250 000 clients, les produits et services primés de WatchGuard mettent en lumière des solutions d'intelligence et de sécurité réseau, de protection avancée des endpoints, d'authentification multifacteur et de Wi-Fi sécurisé. Ensemble, ils offrent les cinq éléments essentiels d'une plateforme de sécurité : sécurité complète, intelligence collective, clarté et contrôle, alignement opérationnel et automatisation. La société 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](https://www.watchguard.com).

SERVICE COMMERCIAL FRANCE +33 97 755 4336 **ADRESSE EMAIL** france@watchguard.com **SITE INTERNET** <https://www.watchguard.com/fr> **WatchGuard Technologies, Inc. | 4**

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.
© 2025 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, Unified Security Platform, le logo WatchGuard, AuthPoint et Firebox sont 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 WGCE67458_020525