

FireCloud Total Access



Sécuriser les utilisateurs distants et l'accès hybride

Dans un environnement de travail hybride, la protection via VPN ne suffit plus. Les employés ont besoin d'un accès sécurisé et fiable aux applications Cloud, aux services SaaS, ainsi qu'aux ressources privées telles que les applications internes, les bases de données ou les environnements de développement.

FireCloud Total Access est une solution de sécurité dans le Cloud qui regroupe un Firewall-as-a-Service (FWaaS), Secure Web Gateway (SWG), un réseau privé virtuel (VPN) et Zero Trust Network Access (ZTNA) pour protéger les utilisateurs distants contre les attaques sur Internet tout en appliquant des règles d'accès strictes aux ressources hybrides.

Composante intégrée du cadre Zero Trust de WatchGuard, FireCloud Total Access permet aux organisations d'offrir une protection de pointe à tous leurs utilisateurs, partout dans le monde – qu'ils soient en télétravail, en déplacement ou au bureau.

Sécurité hybride de bout en bout

FireCloud Total Access étend les protections de pointe, auparavant limitées au périmètre du réseau d'entreprise, aux utilisateurs distants et à l'accès aux applications privées. Cela inclut le filtrage des URL, la prévention des intrusions, la sécurité DNS, la détection des malwares avancés et les contrôles ZTNA basés sur l'identité qui garantissent un accès uniquement aux utilisateurs, appareils et applications autorisés.

Services de sécurité Core

Zero Trust Network Access (ZTNA)

- Contrôle au niveau de l'application et accès par session
- Vérification de la confiance basée sur l'identité et l'appareil
- Suppression du risque de déplacement latéral au sein du réseau

Firewall-as-a-Service (FWaaS)

- Prévention des intrusions (IPS)
- Gateway AntiVirus et détection des botnets
- Sandboxing Cloud (APT Blocker)
- Inspection TLS et filtrage DNS

Secure Web Gateway (SWG)

- Filtrage des URL (WebBlocker)
- Contrôle d'application pour bloquer les logiciels à risque

Services VPN

- Tunnel chiffré pour les applications personnalisées ou héritées
- Accès sécurisé pour les télétravailleurs nécessitant un VPN traditionnel

Gestion unifiée de la sécurité

- Console cloud unique pour la protection des utilisateurs distants, la gestion VPN et la visibilité ZTNA
- Stratégies centralisées, génération de rapports et renseignements sur les menaces

Principaux avantages de FireCloud

- **Protection des utilisateurs distants**
Protégez les utilisateurs contre les menaces en ligne telles que le phishing, les ransomwares et les sites malveillants grâce à des services de sécurité dans le Cloud.
- **Accès Zero Trust aux applications privées**
Fournissez un accès par session basé sur l'identité aux ressources internes et SaaS sans dépendre de l'infrastructure VPN traditionnelle.
- **Passerelle Firebox native** Activez un accès Zero Trust aux applications privées via votre appliance Firebox, sans recourir à une passerelle virtuelle, afin de réduire la complexité de l'infrastructure.
- **Gestion unifiée de la sécurité**
Regroupez la protection des utilisateurs distants, les services VPN et la visibilité ZTNA dans une plateforme Cloud unique, pour simplifier vos opérations.
- **Accès Internet sécurisé** Contrôlez l'accès à Internet des employés à distance pour améliorer la conformité et vous protéger contre les attaques basées sur le Web.
- **Sécurisez tous les utilisateurs et tous les appareils**
Protégez les collaborateurs en mode hybride utilisant des appareils Windows, macOS, iOS et Android, sans compromettre la sécurité ni l'expérience utilisateur.
- **Expérience mondiale homogène**
Assurez un accès sécurisé, performant et sans interruption, où que se trouvent vos utilisateurs, grâce aux points de présence (PoP) gérés par le Cloud de WatchGuard.

Cas d'utilisation



Sécurité des télétravailleurs

Protégez les utilisateurs contre les attaques provenant d'Internet, où qu'ils se connectent.



Accès hybride

Offrez une connexion sécurisée aux applications SaaS et aux ressources internes.



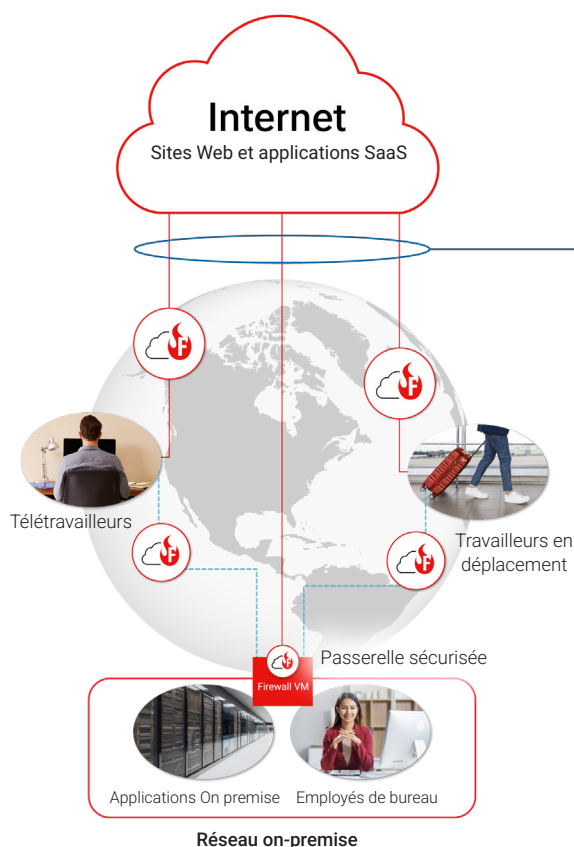
Mise en conformité

Appliquez les principes du moindre privilège et des contrôles traçables et auditable.



Prestation de services pour les MSP

Fournissez un accès géré multi-tenant et une protection centralisée via la plateforme WatchGuard Cloud.



FireCloud Total Access

- Points de présence (PoP) mondiaux pour l'application des politiques de sécurité
- Firewall-as-a-Service (FWaaS)
- Secure Web Gateway (SWG)
- VPN intégré
- Tunnel de transport sécurisé
- Zero Trust Network Access (ZTNA)
- Passerelle FireCloud pour Firebox
- Vérification renforcée de l'identité/ de l'appareil
- VPN intégré
- Contrôle d'identité et authentification multifacteur (MFA) intégrés
- Passerelle sécurisée (accès réseau)
- Compatible avec Windows, Mac, iOS et Android

WatchGuard Cloud

- **Authentification des utilisateurs**
 - Gestionnaire de connexion
 - Fournisseur d'identité (IdP)
- **Services de gestion**
 - Stratégies et configuration communes
 - Assistant de configuration
 - Intégration SAML pour les fournisseurs d'identité (IdP) ou gestion des comptes locaux
 - Passerelle Firebox intégrée
 - Une plateforme unique : Sécurité réseau, identités et endpoints

Trafic utilisateur vers les sites Web et les applications Cloud surveillé et contrôlé

Trafic Zero Trust vers les ressources on-premise surveillé, contrôlé et protégé vers les sites Web et les applications Cloud

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 rapidité tout en améliorant l'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. Leur association fournit 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.com/fr](https://www.watchguard.com/fr)

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

Aucune garantie expresse ou implicite n'est prévue aux présentes. Toutes les spécifications peuvent faire l'objet de modifications et les futurs produits, caractéristiques ou fonctionnalités prévus seront fournis dès qu'ils seront disponibles. ©2026 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, le logo WatchGuard et FireCloud 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 WGCE67866_070926