

Sécurité de nouvelle génération Cyberoam pour les entreprises



Face aux nouvelles tendances (Internet très haut débit, virtualisation, explosion des applications, utilisation croissante des applications Web et de la politique BYOD (PAP en français, Prenez vos appareils), les entreprises doivent se préparer aux risques de sécurité qui planent sur leurs réseaux, ainsi qu'aux préoccupations croissantes liées aux menaces internes, à la disparition des « barrières de sécurité », à la gestion de la conformité, et bien d'autres encore. La croissance des entreprises et la rapidité de développement des réseaux ont conduit à une demande accrue de sécurité de nouvelle génération, de performances plus élevées, de gestion de la sécurité simplifiée et de mise en conformité dans les entreprises. La sécurité de nouvelle génération de Cyberoam répond aux préoccupations des entreprises actuelles et à leur demande en matière de sécurité réseau avancée.



La solution de Cyberoam pour la sécurité des réseaux

Présente dans plus de 125 pays, Cyberoam est une entreprise de sécurité informatique mondialement reconnue. Avec une multitude de produits certifiés et réputés dans le monde entier, Cyberoam offre des solutions fiables pour couvrir les différents besoins des TPE (SOHO), des sites et bureaux distants (ROBO), des PME et des grandes entreprises, notamment les besoins en matière de sécurité réseau, de gestion centralisée de la sécurité et de visibilité centralisée. Dans le monde entier, des milliers de clients font confiance aux technologies et aux produits innovants de Cyberoam. La société jouit d'une expérience éprouvée au service de nombreux clients renommés dans les secteurs les plus divers.

Portefeuille de produits de sécurité Cyberoam :



Sécurité du réseau

Offre la possibilité de mettre en place des appliances de sécurité matérielles et virtuelles pour sécuriser aussi bien les réseaux physiques et que les réseaux virtuels



Gestion centralisée de la sécurité

Permet aux entreprises/MSSP de gérer plusieurs installations de sécurité Cyberoam réparties sur différents sites distants ou filiales



Visibilité centralisée

Offre une visibilité en temps réel sur l'activité des utilisateurs sur le réseau d'entreprise



Formation et assistance

L'assistance client permet de résoudre plus rapidement les problèmes et des formations sont dispensées afin de gérer et de déployer efficacement les solutions Cyberoam



CYBEROAM : LA SÉCURITÉ BASÉE SUR L'IDENTITÉ DE COUCHE 8

La technologie de couche 8 de Cyberoam considère l'identité de l'utilisateur comme la 8e couche (couche utilisateur) de la pile de protocoles. Elle permet aux entreprises d'identifier précisément les utilisateurs, de contrôler l'activité de ces derniers sur le réseau, et de créer des politiques et des rapports par nom d'utilisateur, même dans des connexions IP dynamiques telles que DHCP et Wi-Fi. La technologie de couche 8 de Cyberoam accélère les contrôles de sécurité d'un réseau en offrant une visibilité immédiate sur l'origine des attaques par l'identification des victimes/attaquants selon leur nom d'utilisateur, ce qui permet de prendre les mesures proactives et correctives qui s'imposent. Grâce aux contrôles et à l'identification de couche 8, Cyberoam aide les entreprises dans les domaines suivants : gestion de la sécurité, protection des données, analyse légale et gestion de la conformité.

L8 UTILISATEUR

L7 Application



L6 Présentation

ASCII, EBCDIC, ICA

L5 Session

L2TP, PPTP

L4 Transport

TCP, UDP

L3 Réseau

192.168.1.1

L2 Liaison de donnée

00-17-BB-8C-E3-E7

L1 Physique

La technologie de couche 8 de Cyberoam considère l'identité de l'utilisateur comme la 8e couche de la pile de protocoles.

Les pare-feux de nouvelle génération (NGFW) de Cyberoam offrent la sécurité, de la couche 2 à la couche 8, à l'aide de règles basées sur l'identité



SÉCURITÉ DU RÉSEAU

Cyberoam intègre une multitude de fonctionnalités de sécurité sur une seule appliance afin d'apporter une sécurité réseau complète. Les appliances de sécurité Cyberoam fonctionnent au niveau de la passerelle de réseau et protègent les réseaux des menaces liées aux applications, des vulnérabilités des applications Web, des défis que pose la politique BYOD, des fuites de données par le biais des sites et des applications Web, des attaques mixtes et sophistiquées, des logiciels malveillants, des spams, des spywares et de toutes les autres menaces externes en constante évolution. Grâce à la flexibilité des appliances de sécurité matérielles et virtuelles, Cyberoam protège aussi bien les réseaux physiques que les réseaux virtuels des entreprises.

Fonctions de sécurité de nouvelle génération sur les appliances de sécurité réseau de Cyberoam :

- Pare-feu dynamique
- Gestion de la bande passante
- Visibilité et contrôle d'application
- Connectivité 3G / 4G / WiMAX*
- Pare-feu d'application Web
- Archivage et contrôle des messageries instantanées
- VPN (VPN SSL et IPSec)
- Gestion des liens multiples
- Système de prévention des intrusions (IPS)
- Reporting intégré
- Antivirus et antispyware
- IPv6 Ready
- Antispam
- Appliances Wi-Fi*
- Protection contre les spams sortants
- Flexi Ports*
- Filtrage Web

**Fonctions non disponibles sur les appliances de sécurité réseau virtuelles*

LES APPLIANCES DE SÉCURITÉ DE CYBEROAM ASSURENT



Sécurité



Connectivité



Productivité

Les appliances de sécurité réseau de Cyberoam garantissent la sécurité sans pour autant compromettre la connectivité et la productivité qui sont des aspects tout autant essentiels. Les entreprises peuvent atteindre une croissance équilibrée grâce à une appliance de sécurité réseau qui offre des contrôles de politiques afin de garantir à la fois sécurité, connectivité et productivité. Grâce à une combinaison idéale des meilleures fonctionnalités sur une seule et même interface, les entreprises bénéficient d'une solution réseau complète.

POINTS FORTS:

- Points de vente, canaux de distribution et clients présents dans plus de 125 pays
- Soutenue par le plus grand investisseur privé au monde (156 milliards de dollars) : le groupe Carlyle
- Plus de 450 employés dans le monde entier ; Centre R&D de premier plan
- Technologie de couche 8 basée sur l'identité (brevet en instance)
- Sécurité certifiée Critères communs EAL4+
- Qualifiée de « Innovateur de la sécurité réseau » par le SC Magazine
- Qualifiée de « Visionnaire » dans le Magic Quadrant de Gartner dédié aux UTM
- Numéro 1 mondial de la sécurité réseau et premier fournisseur d'UTM grâce à son service d'assistance client certifié ISO 20000:2011



Série NG de Cyberoam – Sécurité évolutive

Aujourd'hui, les travailleurs sont de plus en plus mobiles, et ont besoin de pouvoir accéder aux ressources réseau à tout moment, où qu'ils se trouvent. Si on ajoute à cela l'augmentation du nombre d'utilisateurs (clients et partenaires) qui se connectent au réseau d'entreprise depuis l'extérieur, on assiste à une déperimétrisation des réseaux. En outre, avec l'augmentation des utilisateurs et des dispositifs sur le réseau, l'explosion des applications, la virtualisation, l'augmentation de l'utilisation des applications Web application, etc., les entreprises perdent peu à peu le contrôle de la sécurité sur leurs réseaux.

Grâce à ses appliances de sécurité réseau (série NG), disponibles sous la forme de pare-feux de nouvelle génération et d'UTM, Cyberoam offre une sécurité évolutive aux TPE, sites et bureaux distants, PME et grandes entreprises. Les appliances de sécurité de Cyberoam proposent des fonctionnalités de sécurité de nouvelle génération pour aider les entreprises à sécuriser leurs réseaux contre les risques inhérents à ces nouvelles tendances.



Pare-feux de nouvelle génération (NGFW)

Dotés de la technologie de couche 8 basée sur l'identité, les NGFW de Cyberoam offrent aux entreprises une veille décisionnelle et des contrôles afin qu'elles bénéficient d'un contrôle total de la sécurité sur les couches 2 à 8 de leurs réseaux. La protection des NGFW de Cyberoam offre une sécurité basée sur l'identité (couche 8), la visibilité et le contrôle des applications, l'IPS, le VPN (IPSec et SSL), le filtrage des sites Web et la QoS. Selon leurs besoins en matière de sécurité, les entreprises peuvent souscrire à des fonctionnalités de sécurité supplémentaires telles que le pare-feu d'application Web, l'antivirus au niveau de la passerelle, l'antispam, etc.

Gamme d'appliances matérielles NGFW de Cyberoam :

Série CR NG :

500iNG-XP, 750iNG-XP, 1000iNG-XP, 1500iNG-XP, 2500iNG, 2500iNG-XP

Série CR ia :

500ia, 500ia-1F/10F/RP, 750ia, 750ia-1F/10F, 1000ia, 1000ia-10F, 1500ia, 1500ia-10F



Appliances de gestion unifiée des menaces (UTM)

Cyberoam propose les appliances UTM les plus rapides pour les TPE/PME et les bureaux distants avec une sécurité réseau complète. La série NG de Cyberoam offre aux entreprises une sécurité évolutive en proposant des fonctionnalités de sécurité professionnelles, des ports gigabit et les meilleurs logiciels et matériels du secteur. La plateforme basée sur l'identité de couche 8 comprend une multitude de fonctionnalités de sécurité assurant protection, simplicité et haute efficacité.

Gamme d'appliances matérielles UTM de Cyberoam :

Série CR NG :

10wiNG, 10iNG, 15wiNG, 15iNG, 25wiNG, 25iNG, 35wiNG, 35iNG, 50iNG, 100iNG, 200iNG, 200iNG-XP, 300iNG, 300iNG-XP

Série CR ia :

15i, 25ia, 35ia, 15wi, 25wi, 35wi, 50ia, 100ia, 200i, 300i

Caractéristiques principales

Technologie de couche 8 pour une sécurité basée sur l'identité

- La technologie de couche 8 (brevet en instance) s'applique à chacun des modules de sécurité des appliances de sécurité réseau de Cyberoam, et offre des contrôles sur l'authentification de l'utilisateur, l'autorisation de service et le reporting (AAA)

Visibilité et contrôle d'application

- Couvre plus de 2 000 applications clés
- Privilégie les applications en se basant sur une combinaison utilisateur, heure, applications et bande passante
- Contrôle granulaire des applications avec une classification reposant sur le niveau de risque, les caractéristiques et la technologie
- Le modèle de protection proactive permet d'éviter l'intervention manuelle des administrateurs pour mettre à jour les politiques lorsque de nouvelles applications sont ajoutées

Protection avancée contre les menaces [IPS, AV, AS]

- Protège des nouvelles menaces grâce à un système de prévention des intrusions, un antivirus et un antispyware au niveau de la passerelle, un antispam, et offre une sécurité en plus des meilleures solutions du marché

Reporting intégré

- Reporting intégré avec journaux et rapports en temps réel, ce qui permet d'économiser le coût d'une solution de reporting distincte
- Offre plus de 1 200 rapports et une visibilité en temps réel sur l'activité des utilisateurs et du réseau
- Aide les entreprises dans les domaines suivants : gestion de la sécurité, gestion de la conformité et analyse légale
- Des rapports de conformité en un clic sur PCI DSS, HIPAA, SOX, etc.



Sécurité évolutive.

Appliances de sécurité haute performance

Cyberoam offre une sécurité très performante aux entreprises grâce à ses puissantes appliances matérielles et à Cyberoam OS, qui a la capacité d'exploiter les meilleures performances d'une plateforme multicœur et s'intègre étroitement au matériel pour une accélération du réseau et cryptographique.

Cyberoam propose les appliances UTM les plus rapides des segments TPE/PME. L'appliance d'entrée de gamme de la série NG étant équipée d'un pare-feu dont le débit peut atteindre un gigabit, les entreprises sont assurées de bénéficier d'une sécurité haute performance, y compris pour les petits bureaux et filiales.

Veille décisionnelle et contrôles

La couche 8 (utilisateur) de Cyberoam agit comme une couche abstraite classique, qui s'associe aux couches existantes (2 à 7), ce qui permet aux entreprises de reprendre le contrôle de la sécurité et de mettre en place des contrôles de sécurité où elles le souhaitent dans les couches 2 à 8, avec une visibilité complète sur l'activité des utilisateurs et du réseau.

Firmware intelligent – Cyberoam OS

Intégré de façon transparente au matériel, pour l'accélération réseau et cryptographique, Cyberoam OS exploite les meilleures performances d'une plateforme multicœur, tout en offrant une latence minimale. Il dispose de fonctions de sécurité de nouvelle génération pour offrir une protection contre les nouvelles menaces.

Architecture de sécurité extensible (ESA)

L'architecture de sécurité extensible de Cyberoam aide les entreprises à se prémunir contre les futures menaces en offrant la possibilité de prolonger la durée de vie et les performances de ses appliances de sécurité afin qu'elles puissent prendre en charge les toutes dernières fonctionnalités et améliorations de sécurité.

Extensibilité

Outre l'architecture de sécurité extensible (qui offre la prise en charge des futures exigences de sécurité sans avoir à changer d'appliance), les entreprises peuvent ajouter une autre appliance en grappe pour supporter davantage d'utilisateurs.

Flexibilité

Disponibles sur les appliances de sécurité Flexi Port (XP), les Flexi Ports offrent une connectivité réseau flexible avec des ports E/S qui permettent d'ajouter des ports supplémentaires 1G/10G (cuivre/fibre) sur la même appliance de sécurité. Ainsi, les entreprises peuvent adopter les nouvelles technologies en toute simplicité et à moindre coût et bénéficier d'une sécurité évolutive.

VPN

- Garantit un accès à distance sécurisé grâce aux protocoles IPSec VPN, LT2P, PPTP et VPN SSL sur ses appliances de sécurité réseau
- La technologie TFT (Threat Free Tunneling) analyse le trafic à la recherche de logiciels malveillants et de tentatives d'intrusion
- Propose des clients VPN mobiles pour les appareils Android et iOS, afin de simplifier les communications

Filtrage Web

- Base de données d'URL exhaustive avec 100 millions d'URL réparties dans plus de 89 catégories
- Possibilité de créer une politique avec plusieurs critères (utilisateur, catégorie de sites web, heure et bande passante)
- Bloque les sites web nuisibles, empêche les logiciels malveillants, le phishing, le pharming et améliore la productivité en limitant l'accès à des contenus contre-productifs

Pare-feu d'application Web (WAF)

- Disponible sous la forme d'un module d'abonnement intégré
- Protège les sites Web et les applications basées sur le Web contre les
- 10 principales attaques publiées par l'OWASP dirigées contre les applications Web telles que les injections SQL, les attaques sur les éléments dynamiques (XSS), le piratage des paramètres des URL, et bien d'autres encore
- Suit un modèle de sécurité positive par le biais de la détection intuitive du trafic réseau (Intuitive Website Flow Detector) qui identifie et bloque automatiquement toutes les attaques de la couche application sans avoir recours aux tableaux de signatures ou aux techniques de reconnaissance matricielle

QoS ou gestion de la bande passante

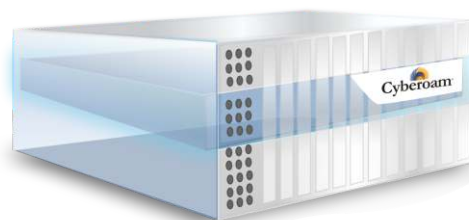
- Allocation de QoS/bande passante aux utilisateurs, groupes d'utilisateurs, applications, catégories de sites Web et règles de pare-feu
- Privilégie les applications vitales et les utilisateurs clés, en assurant la QoS pour les applications vitales comme la téléphonie sur IP ou la CRM
- Possibilité de réserver la bande passante à tout moment ou d'attribuer automatiquement la bande passante inutilisée à d'autres applications/utilisateurs/catégories de sites web

Sécurité virtuelle

Les appliances de sécurité réseau virtuelles de Cyberoam sont conçues pour répondre aux exigences de sécurité des environnements virtualisés, comme les centres de données virtuels, les solutions de sécurité intégrée ou de gestion intégrée pour les MSSP/Entreprises. Les appliances de sécurité réseau virtuelles de Cyberoam peuvent être déployées comme pare-feux de nouvelle génération ou comme UTM.

Les appliances de sécurité réseau virtuelles de Cyberoam offrent :

1. La sécurité pour les réseaux virtualisés en analysant le trafic dans les réseaux virtuels, en protégeant la console de gestion de l'hyperviseur, l'hyperviseur et l'OS invité, et en sécurisant les réseaux zero trust.
2. Une sécurité réseau complète grâce à une multitude de fonctionnalités de sécurité intégrées sur une seule et même appliance de sécurité virtuelle afin que les environnements virtuels soient aussi sécurisés que les infrastructures physiques.
3. Déploiement et mise à niveau faciles.
4. Des rapports de conformité et fonction de journalisation/reporting en un clic qui aident à gérer la conformité.
5. Gestion centralisée de la sécurité des filiales par le biais d'une seule interface de Cyberoam Central Console (CCC), disponible en version matérielle et virtuelle, qui rassemble toutes les appliances de sécurité réseau physiques/virtuelles.
6. Visibilité centralisée sur les activités du réseau et des utilisateurs avec le logiciel Cyberoam iView qui offre une fonction de journalisation et de reporting.
7. Solution de sécurité virtuelle complète grâce aux appliances de sécurité réseau virtuelles de Cyberoam, à la CCC virtuelle et au logiciel Cyberoam iView pour une journalisation et un reporting centralisés.



Gammes d'appliances de sécurité réseau virtuelles de Cyberoam :

CRiV-1C, CRiV-2C, CRiV-4C, CRiV-8C, CRiV-12C

Les appliances de sécurité réseau virtuelles de Cyberoam prennent en charge différentes plateformes de virtualisation telles que VMware et Hyper-V.





Grâce à la Cyberoam Central Console (CCC), disponible sous la forme d'appliances matérielle et virtuelle, les entreprises peuvent gérer de manière centralisée la sécurité de leurs filiales utilisant des appliances de sécurité Cyberoam.

- Application centralisée des politiques, abonnements de sécurité et mises à niveau des firmwares/signatures avec gestion des changements pour des politiques uniformes et une protection contre les menaces instantanées.
- Offre une gestion rapide avec la possibilité de regrouper les appliances de sécurité de Cyberoam déployées sur l'ensemble des bureaux selon leur localisation géographique, les modèles, les versions de firmware et les abonnements de sécurité
- Contrôles administratifs basés sur les rôles avec journaux répertoriant les actions des administrateurs
- Alertes proactives selon certains paramètres (date d'expiration des abonnements, utilisation excessive du disque, IPS, nombre de menaces virales, navigation internet nuisible, et bien d'autres encore)
- Dispose d'informations de pre-provisioning (détection automatique des appliances) sur les appareils Cyberoam avec des modèles de configuration pour créer rapidement des politiques

Gamme d'appliances CCC :

- **Appliances matérielles CCC NM**
 - CCC15NM, CCC50NM, CCC100NM, CCC200NM, CCC500NM
- **Appliances matérielles CCC**
 - CCC15, CCC50, CCC100, CCC200, CCC500, CCC1000
- **Appliances virtuelles CCC**
 - CCCV15, CCCV50, CCCV100, CCCV200, CCCV500



Les entreprises peuvent bénéficier d'une visibilité en temps réel complète et centralisée sur l'activité du réseau et des utilisateurs grâce au logiciel Cyberoam iView qui offre une fonction de journalisation et de reporting.

- Plus de 1 200 rapports aident à assurer la gestion de la sécurité, la gestion de la conformité et l'analyse légale
- Des journaux, rapports et alertes sur une multitude de périphériques, protocoles et sites fournissent des informations concernant l'activité des utilisateurs et du réseau afin d'identifier les failles de sécurité, réduisant par conséquent le temps de réponse et le temps d'indisponibilité du réseau
- Des rapports de conformité en un clic HIPAA, PCI DSS, GLBA, SOX et des rapports/alertes détaillés sur les failles de sécurité et les fuites de données permettent de répondre aux exigences de conformité
- Facilite l'analyse légale en reconstituant la séquence d'événements qui s'est produite lors de la faille de sécurité grâce aux journaux et aux rapports, ce qui permet de réduire les coûts liés à l'investigation et le temps d'indisponibilité du réseau
- Compatible avec une large gamme d'appareils, y compris les pare-feux proxy, les applications personnalisées et l'ensemble des dispositifs compatibles Syslog, ce qui permet aux entreprises de stocker les journaux et les rapports de tout un éventail d'appareils

Gammes d'appliances iView de Cyberoam :

- **Appliances matérielles**
 - CR-IVU25NR, CR-IVU100NR, CR-IVU200NR
- **Logiciel**



Assistance avant-vente

L'équipe d'assistance avant-vente de Cyberoam propose une planification de la sécurité et une assistance à la migration pour les déploiements et les mises en place de Cyberoam dans les entreprises

Assistance après-vente

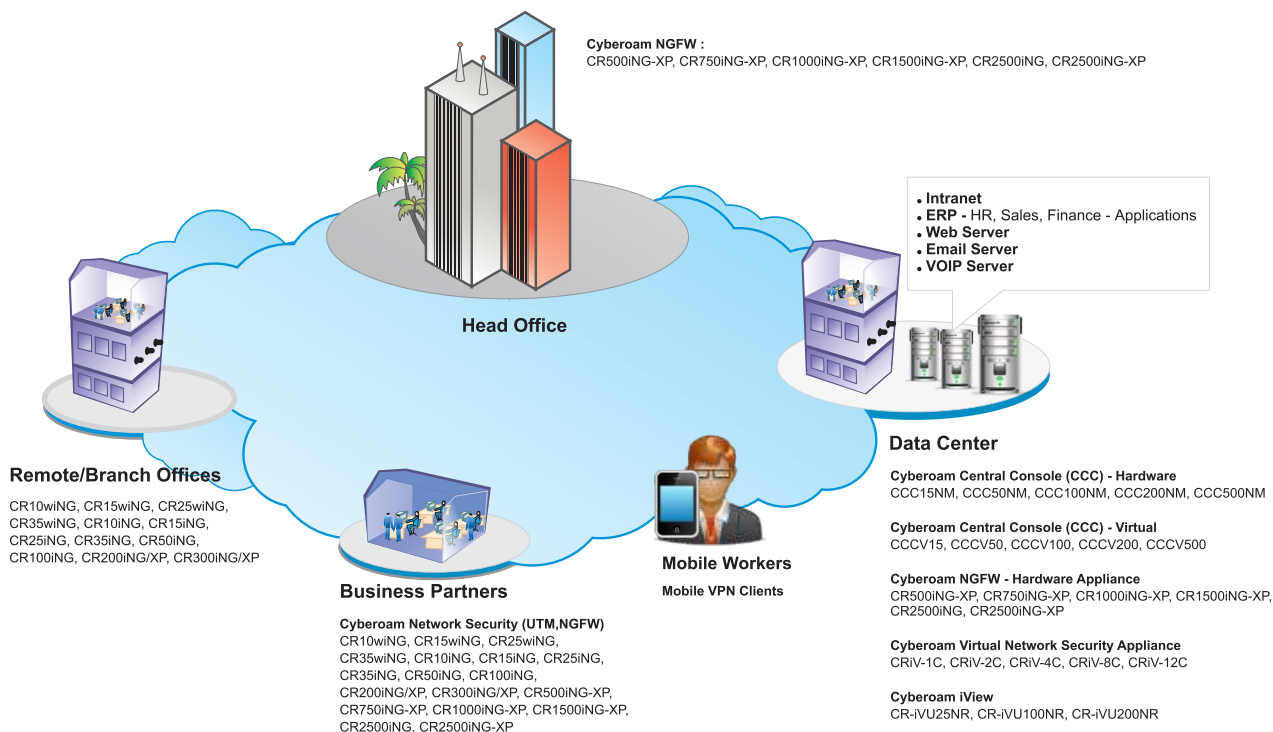
L'équipe d'assistance mondiale certifiée ISO 20000:2011 de Cyberoam est disponible 24h/24 et 7j/7 ou 8h/j et 5j/semaine (selon le contrat souscrit par le client) par téléphone, email et tchat.

Formation

Cyberoam propose à ses clients des formations et des mises à jour sur les produits pour un déploiement, une configuration et une gestion efficaces de ses solutions.

Le Cyberoam Threat Research Labs (laboratoire de recherche des menaces) comprend une équipe de chercheurs qui détectent et identifient les menaces de sécurité dès le début de la propagation, et protègent ainsi les clients de Cyberoam des innombrables vulnérabilités et attaques de logiciels malveillants. Le CTRL assure une protection adéquate de la sécurité en publiant en permanence des signatures, des mises à niveau de sécurité et des rapports de recherche.

Cyberoam Solutions for Enterprise Networks



Note :The above diagram shows multiple models for Cyberoam NGFW and UTM, CCC as appropriate for Head Office, Branch Offices, Data Center, Mobile Users, Business Partners. Enterprise may use any one or multiple models from Cyberoam Product line as appropriate.

Récompenses et certifications



Cyberoam Technologies

505 Thornall Street, Suite # 304 Edison, NJ - 08837, États-Unis,
Tél : +1-847-235-4684 Numéro d'appel gratuit : +1-800-686-2360

sales@cyberoam.com | www.cyberoam.com



® Marques déposées de Cyberoam Technologies Pvt. Ltd.