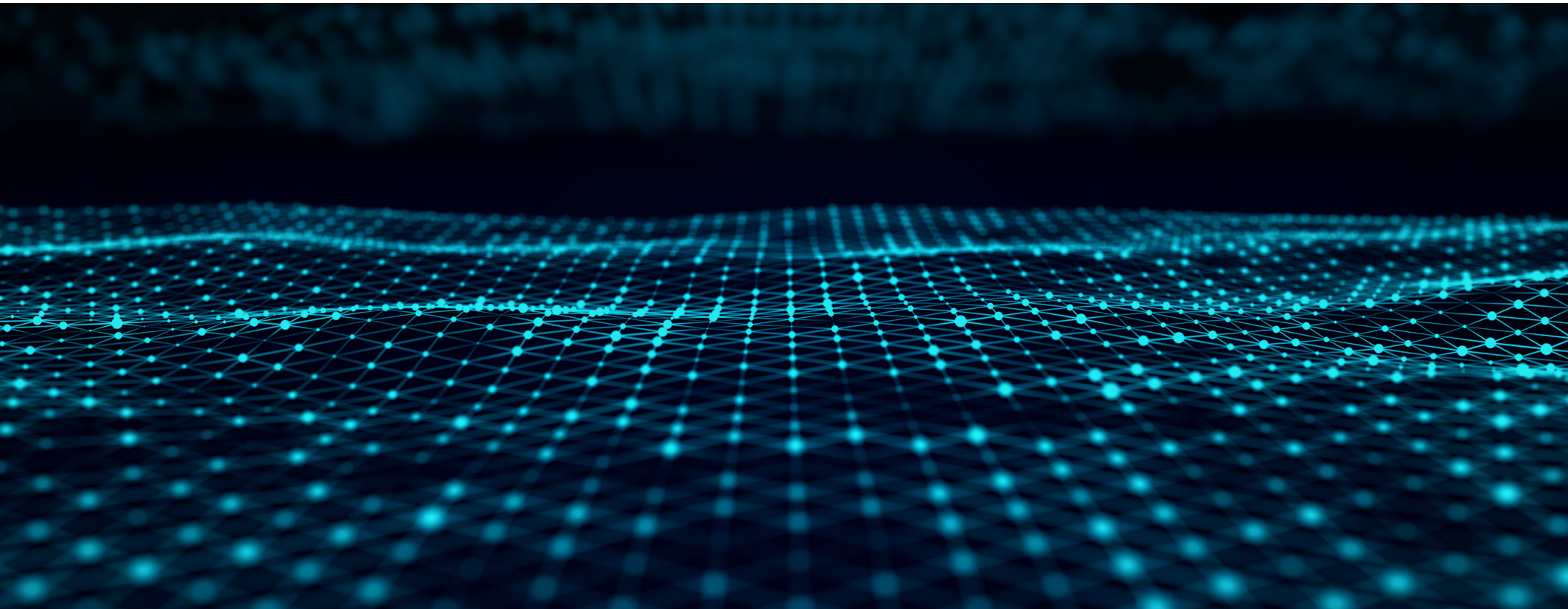
Cisco Hybrid Mesh Firewall – Présentation

La sécurité de demain, accessible aujourd'hui



Les environnements IT d'entreprise modernes sont distribués et complexes.

La multiplication des applications, l'essor des technologies d'intelligence artificielle (IA) et la mobilité des équipes ne cessent d'élargir la surface d'exposition aux attaques. Les entreprises doivent être en mesure de sécuriser les principales limites du trafic réseau, de protéger les applications métiers et celles reposant sur l'IA, et de s'assurer que les utilisateurs et les équipements n'ont accès qu'aux ressources spécifiquement autorisées.

Un changement radical implique une réflexion radicale. C'est pourquoi nous avons réinventé la sécurité pour qu'elle s'adapte à tous les environnements, à très grande échelle. Les pare-feu, qui sont à la base de la sécurité des entreprises, sont plus importants que jamais. C'est pourquoi Cisco porte leur puissance à un niveau inédit.

La solution Cisco Hybrid Mesh Firewall est une fabric de sécurité hautement distribuée, optimisée pour bloquer les menaces avancées, protéger les vulnérabilités des applications et mettre en œuvre une segmentation Zero Trust dans tous les environnements. Grâce à la gestion unifiée du cloud, qui rationalise les workflows et renforce la sécurité, Cisco vous permet de faire évoluer votre fabric de sécurité sans avoir à remplacer l'infrastructure existante. Pour augmenter la productivité, vous pouvez désormais tirer parti des fonctionnalités natives de l'IA pour simplifier la résolution des problèmes et optimiser les performances de vos outils de mise en œuvre.

La solution Hybrid Mesh Firewall simplifie l'adoption et protège vos investissements grâce aux licences flexibles de la suite Cisco Cloud Protection. Celles-ci vous permettent d'accéder facilement à différentes fonctionnalités ainsi qu'aux innovations à mesure que les besoins de votre entreprise évoluent.

Avantages

Simplifiez la gestion de la sécurité : accédez à toutes les fonctionnalités de sécurité de votre environnement hybride et gérez-les pour obtenir des informations basées sur l'IA à partir d'une interface centralisée.

Protégez-vous contre les menaces modernes : sécurisez les environnements au niveau des limites stratégiques tout en bloquant les attaques zero-day et les menaces chiffrées.

Bloquez les mouvements latéraux non autorisés : réduisez la surface d'exposition aux attaques et minimisez l'impact grâce à une segmentation superficielle et précise pour les workloads classiques et Kubernetes.

Sécurisez l'adoption de l'IA : détectez et bloquez les menaces dynamiques qui apparaissent lors du développement et du déploiement des applications d'IA.

Bloquez les exploits : protégez-vous contre les exploits en quelques minutes grâce à un moteur de règles natif de l'IA qui hiérarchise les vulnérabilités et recommande automatiquement un contrôle ciblé.

Composants de Cisco Hybrid Mesh Firewall

Hypershield :
Architecture de sécurité distribuée native de l'IA, pour une évolutivité à l'échelle de l'IA

Secure Firewall :
Pare-feu de pointe qui analysent le trafic chiffré, à grande échelle

Secure Workload :
Plateforme qui améliore la visibilité et permet d'appliquer des politiques de segmentation aux applications dans les environnements hybrides, avec ou sans agent

Multicloud Defense :
Orchestration et automatisation cloud natives pour simplifier les déploiements, la gestion du réseau et la mise à l'échelle des pare-feu dans le cloud public

AI Defense :
Protections pour le développement et le déploiement d'applications d'IA

Isovalent Enterprise Platform :
Identifiez les interactions entre les microservices et appliquez des politiques dans les environnements Kubernetes

Security Cloud Control :
Portail centralisé pour la gestion de tous les points d'application des politiques dans la fabric de sécurité

Pourquoi choisir Cisco Hybrid Mesh Firewall ?

Fabric de sécurité hautement distribuée, gérée de manière unifiée et proposée par un seul fournisseur

Cisco ne se contente pas d'offrir un pare-feu prêt à l'emploi : la sécurité est intégrée dans le réseau, le cloud, les containers et les workloads pour une fabric hautement distribuée. Sa solution place la sécurité là où vous en avez besoin, intègre vos pare-feu existants, évolue avec votre entreprise et prend en charge la gestion des politiques lorsqu'elle dépasse les capacités humaines. Elle est disponible sous la forme d'une licence flexible qui évolue selon vos besoins et les innovations de Cisco.

Cinq caractéristiques qui distinguent la solution Cisco Hybrid Mesh Firewall :

1. Gestion centralisée intelligente : configuration, déploiement et mise à l'échelle automatique des pare-feu dans les environnements multicloud, sans script. En outre, l'assistant IA réduit les frais de gestion et libère des ressources et les experts.
2. Protection avancée contre les menaces : visibilité sur les menaces chiffrées sans sacrifier les performances, grâce à la première plateforme de visibilité chiffrée basée sur l'apprentissage automatique. Là où le déchiffrement est essentiel, une architecture d'accélération matérielle hautes performances offre un excellent rapport qualité-prix et une visibilité renforcée. Protégez-vous contre les menaces connues et inconnues avec la Threat Intelligence de Cisco Talos, le système de prévention des intrusions Snort 3 et Snort ML.
3. Segmentation : blocage des mouvements latéraux non autorisés et protection des applications dans le data center et dans les différents clouds grâce à une sécurité tenant compte de la topologie, qui comprend les dépendances des applications et applique des politiques de segmentation Zero Trust dans la fabric de sécurité Cisco.
4. Protection des modèles d'IA : intégration de contrôles d'IA dans la fabric du réseau pour bloquer en temps réel les menaces dynamiques qui apparaissent lors du développement et du déploiement des applications d'IA.
5. Protection contre les exploits : maîtrise des vulnérabilités par l'application d'un bouclier ciblé positionné de manière optimale sur le chemin de l'application pour bloquer l'exploit, sans nuire à la disponibilité de l'application.

Fonctionnalités de Cisco Hybrid Mesh Firewall

Une sécurité aussi rapide et agile que l'entreprise

- Une fabric de sécurité composée de pare-feu (physiques, virtuels et cloud), d'agents (workloads classiques et Kubernetes) et de commutateurs intelligents qui intègrent les fonctions de sécurité à la fabric du réseau
- Extension de la sécurité partout où elle est nécessaire en l'intégrant dans la fabric des environnements physiques, virtuels, cloud, de containers et IoT
- Pare-feu cloud natif qui facilite la gestion du réseau, l'évolution automatique et l'autoréparation des points d'application de la sécurité dans les environnements de cloud public
- Encrypted Visibility Engine pour l'identification et le blocage des menaces dissimulées dans le trafic chiffré
- IPS Snort 3, Snort ML et Threat Intelligence mise à jour en continu de Cisco Talos pour bloquer les menaces connues et les attaques zero-day
- Segmentation des applications dans tous les environnements à l'aide de politiques Zero Trust cohérentes avec une architecture de sécurité conçue pour protéger les data centers modernes à l'échelle de l'IA
- Protection des modèles d'IA en temps réel pour défendre les applications basées sur l'IA contre les utilisations abusives, les violations de données, les dénis de service et les attaques sophistiquées telles que les attaques par injection rapide
- Protection contre les exploits grâce à un moteur de règles natif de l'IA qui hiérarchise les vulnérabilités et recommande automatiquement un contrôle ciblé
- Intégration native avec Cisco ISE (Identity Services Engine) pour simplifier la segmentation des objets connectés grâce à l'utilisation de balises SGT
- Intégration avec l'accès réseau Zero Trust universel Cisco pour fournir une plateforme Zero Trust globale dans l'entreprise hybride

Simplifiez les systèmes à grande échelle grâce à une gestion centralisée intelligente

- Gestion dans le cloud de plusieurs domaines, notamment la gestion de tous les points d'application des politiques à partir d'une interface unique, le partage d'objets dans la fabric, le contrôle d'accès en fonction des rôles des utilisateurs (RBAC), la gestion des licences, l'IA Ops et la gestion du cycle de vie des politiques
- Gestion des politiques cloud sur l'ensemble de l'infrastructure Cisco et des pare-feu tiers, et application des politiques d'accès réseau Zero Trust universel Cisco partout, pour tous les types d'accès utilisateur, on-premise ou distants
- Configuration native, déploiement et mise à l'échelle automatique des pare-feu cloud dans les environnements multicloud
- Cisco AI Assistant fournit des informations unifiées sur le maillage de sécurité pour la configuration des politiques, la résolution des problèmes et l'optimisation
- Cisco AI Assistant est capable d'écrire, de déployer et d'optimiser des règles de pare-feu dans l'environnement et de faire des recommandations pour les tâches courantes

Protection de l'entreprise

Améliorez la résilience et évitez les temps d'arrêt avec des règles de sécurité appropriées et des points d'application optimaux.

Protection des équipes

Améliorez considérablement l'efficacité de votre équipe pour libérer des ressources grâce à la gestion centralisée des outils de sécurité à travers un système autonome pensé pour gagner votre confiance.

Protection des investissements

Cisco Cloud Protection Suite vous ouvre la voie vers la solution Hybrid Mesh Firewall. Cette suite allie simplicité et flexibilité pour vous permettre d'atteindre vos objectifs plus facilement et d'exploiter les solutions innovantes à votre rythme, à mesure que votre entreprise évolue.

En savoir plus

Pour en savoir plus sur les produits et les services Cisco Hybrid Mesh Firewall, rendez-vous sur www.cisco.com/go/hybridmeshfirewall.

Pour consulter les options d'achat et discuter avec un conseiller Cisco, rendez-vous sur www.cisco.com/site/us/en/buy/index.html.