Solutions Sécurité

Optimisez vos investissements IT et réduisez les risques de cyberattaque avec Cisco

Cisco Partner
Distribution Partner

Cybersecurity first !

Grâce à un portefeuille intégré et à des informations de pointes sur les menaces, Cisco vous donne la portée, l'échelle et les capacités nécéssaires pour faire face à la complexité et au volume des menaces. Anticiper les menaces évolutives de demain en toute sérénité.

01 Advanced Malware Protection

02 Sécurité du Cloud

03 Sécurité de messagerie

04 Visibilité sur le réseau et protection

05 Pare-feu nouvelle génération

06 Système de prévention des intrusions

07 Sécurité des routeurs

08 Clients VPN, sécurité des terminaux

09 Sécurité du Web

01. Cisco Advance Malware Protection

La visibilité et le contrôle dont vous avez besoin pour contrer les attaques avancées

Profitez d'une Threat Intelligence à l'échelle mondiale, de fonctions de sandboxing avancées et d'un blocage des malwares en temps réel pour prévenir les failles grâce à Cisco AMP (Advanced Malware Protection). Mais comme la prévention ne fait pas tout, Cisco AMP analyse également en permanence l'activité des fichiers sur tout votre réseau afin de détecter, de contenir et de supprimer rapidement les malwares avancés.

o Une Threat Intelligence à l'échelle mondiale

Les experts Cisco Talos analysent des millions d'échantillons de malwares et des téraoctets de données chaque jour, puis transmettent ces informations à Cisco AMP. Cisco AMP compare les fichiers, leur comportement et les données de télémétrie à cette base de connaissances contextuelle pour assurer une défense proactive contre les menaces connues et les nouveaux types d'attaques.

o Un sandboxing avancé

Les fonctionnalités de sandboxing avancées permettent de comparer automatiquement, et de manière dynamique et statique, les fichiers avec plus de 700 indicateurs comportementaux. Ces analyses permettent de détecter les menaces furtives et d'aider votre équipe chargée de la sécurité à identifier, à hiérarchiser et à bloquer les attaques les plus sophistiquées.

o La détection et le blocage ponctuels des malwares

Bloquez en temps réel les malwares qui tentent d'infiltrer votre réseau. Grâce à des moteurs de détection antivirus, à la mise en correspondance biunivoque des signatures, à l'apprentissage automatique et à la recherche d'empreintes partielles, Cisco AMP analyse les fichiers au niveau de leur point d'entrée afin de détecter les malwares connus et inconnus. Le résultat ? Des délais de détection plus courts et une protection automatisée.

o Des fonctions d'analyse continue et de sécurité rétrospective

Lorsqu'un fichier, quel qu'il soit, entre sur votre réseau, Cisco AMP continue d'observer, d'analyser et d'enregistrer son activité. Si un comportement suspect est détecté ultérieurement, Cisco AMP envoie une alerte rétrospective à votre équipe chargée de la sécurité pour lui indiquer la provenance du malware, ses déplacements et ses activités. En quelques clics, vous pouvez le contenir et l'éradiquer.

Besoin d'infos ou d'un devis ?

CONTACT

Protégez vos terminaux

Grâce à la solution Cisco de protection des terminaux, vous pouvez bloquer les malwares au point d'entrée, avoir une visibilité sur l'activité au niveau des fichiers et des exécutables, et éliminer les malwares de vos PC, Mac, systèmes Linux et terminaux mobiles.

Cisco AMP pour terminaux >

Protégez votre réseau

Bénéficiez d'une visibilité avancée sur l'activité des menaces, au coeur ou à la périphérie du réseau et bloquez les malwares les plus avancés.

AMP for Networks >
Pare-Feu >
Plate-Forme de gestion unifiée des risques Meraki MX >
Le routeur d'une succursale (ISR) >

Protégez votre messagerie et le trafic web

Ajoutez des fonctionnalités Cisco AMP à vos appliances de sécurisation du web et de la messagerie ou lors de vos déploiements de solutions cloud de sécurisation du web et de la messagerie.

La messagerie >
Le web >
Les passerelles Internet sécurisées (Cisco Umbrella) >

Pourquoi travailler avec DistriWan ?

- **Offre de services >** Un catalogue de prestations sur-mesure et adaptées à vos besoins
- **Expertise >** Une équipe avant-vente spécialisée par architecture
- **Accompagnement >** Une équipe commerciale à votre écoute pour répondre à toutes vos demandes de projets
- **Réactivité et flexibilité >** Une forte adaptabilité pour répondre à toutes vos exigences

02. Sécurité du Cloud

Les solutions de sécurité cloud de Cisco vous aident à adopter les technologies Cloud en étant protégé. Elles vous permettent de mieux gérer la sécurité et protègent les utilisateurs contre les menaces, quel que soit le lieu depuis lequel ils accèdent à internet. Elles protègent vos données et vos applications dans le cloud.

- Sécurité de l'infrastructure dans le cloud public
- Sécurité de la messagerie pour Office 365°
- Sécurité pour les applications SaaS
- Evaluation de la sécurité du cloud

Blocage rapide des menaces

Stoppez les malwares avant qu'ils atteignent votre réseau ou vos terminaux. Réduisez le temps passé à éliminer les infections.

Protection ultra étendue

Eliminez les angles morts. Protégez les utilisateurs où qu'ils se trouvent et accèdent à internet

Sécurisation des users, datas et applications

Protégez les utilisateurs, les données et les applications dans le cloud contre le piratage de leur compte, les malwares et les violations de données.

Utilisation sécurisée du cloud

Améliorez la sécurité sans affecter la productivité des utilisateurs.

CONTACT

Pourquoi travailler avec DistriWan ?

- **Offre de services >** Un catalogue de prestations sur-mesure et adaptées à vos besoins
- **Expertise >** Une équipe avant-vente spécialisée par architecture
- **Accompagnement >** Une équipe commerciale à votre écoute pour répondre à toutes vos demandes de projets
- **Réactivité et flexibilité >** Une forte adaptabilité pour répondre à toutes vos exigences

03. Sécurité de messagerie

Une protection avancée pour la sécurité de la messagerie

Les pirates utilisent principalement des e-mails pour répandre des spams, des malwares et d'autres menaces. Pour éviter les failles, il vous faut une solution puissante de sécurité de la messagerie.

La solution Cisco de sécurité de la messagerie vous protège contre les tentatives de phishing, les e-mails professionnels corrompus et le ransomware. Avec Cisco Talos, bénéficiez gratuitement d'une mise à jour toutes les 3 à 5 minutes de votre Threat Intelligence pour une protection optimale. Cisco Advanced Malware Protection vous protège des malwares furtifs dans les pièces jointes et la Threat Intelligence, leader du secteur, basée sur les URL combat les liens malveillants. La solution Cisco de sécurité de la messagerie renforce également la sécurité de la messagerie Office 365.

Enfin, il est tout aussi important de protéger les e-mails sortants. La solution Cisco de sécurité de la messagerie comporte des fonctions robustes de prévention des pertes de données (DLP) et de chiffrement du contenu pour protéger les informations sensibles. Vous êtes ainsi conforme aux réglementations du secteur et aux lois en vigueur.

o Protégez vos utilisateurs contre les menaces visant la messagerie
Découvrez une approche multi niveau de la sécurité pour protéger la messagerie de vos utilisateurs d'un large nombre d'attaques.

o Renforcez la sécurité de la messagerie Office 365°
Mettez en place une couche de protection efficace contre les ransomwares, le phishing, les attaques de type BEC ... et découvrez l'efficacité conjointe d'Office 365° et de la solution Cisco de sécurité messagerie.

o Dépassez la détection ponctuelle
Protégez-vous des fichiers dangereux chaque fois qu'ils deviennent malveillants, grâce à Cisco Advanced Malware Protection pour la messagerie.

o Profitez d'une Threat Intelligence exeptionnelle
Seul Cisco assure une protection exceptionnelle contre les menaces, grâce à Talos, l'une des plus grandes équipes de Threat Intelligence au monde. Les mises à jour arrivent automatiquement toutes les 3 à 5 minutes.

o Découvrez la DLP
Protégez vos données sensibles. Protégez le contenu envoyé par e-mail grâce aux fonctions de prévention des pertes de données.

Besoin d'infos ou d'un devis ?

CONTACT

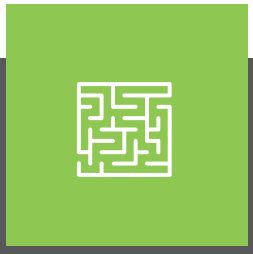
04. Visibilité sur le réseau et protection

Détectez, contrôlez et appliquez

Les réseaux sont de plus en plus complexes et le nombre des périphériques s'accroît de manière exponentielle. Il est plus difficile de voir ce qui se passe sur le réseau et de détecter une menace. La solution Cisco Network Visibility and Enforcement comprend Cisco Stealthwatch, Cisco Identity Services Engine et la technologie Cisco TrustSec. Bénéficiez d'une détection rapide des menaces, d'un accès sécurisé et d'une segmentation logicielle.

Réduire les risques

Transformez votre réseau en un système de sécurité grâce à des solutions conçues pour offrir une protection multicouche de manière coordonnée.



Réduire la complexité

Choisissez parmi des fonctionnalités intégrées, dédiées ou gérées dans le cloud pour assurer la sécurité de l'intégralité du réseau.

Améliorer la visibilité

Utilisez les données en temps réel pour sécuriser les accès, récolter des informations et détecter les activités suspectes, même pour le trafic chiffré.

Protégez des menaces

Appliquez des politiques et réagissez en temps réel pour protéger tout le réseau de votre entreprise contre les menaces connues et inconnues.

Cisco SteathWatch

Stealthwatch collecte des données télémétriques à l'échelle de votre réseau et détecte les activités malveillantes à l'aide du machine learning.

Cisco Identity Engine (ISE)

Isolez rapidement les menaces. ISE partage des informations sur les utilisateurs et les périphériques, contrôle l'accès sur les réseaux filaires, sans fil et VPN.

Cisco TrustSec

La segmentation logicielle réduit la surface d'exposition aux attaques, facilite le contrôle d'accès et simplifie la conformité.

CONTACT

Pourquoi travailler avec DistriWan ?

- **Offre de services >** Un catalogue de prestations sur-mesure et adaptées à vos besoins
- **Expertise >** Une équipe avant-vente spécialisée par architecture
- **Accompagnement >** Une équipe commerciale à votre écoute pour répondre à toutes vos demandes de projets
- **Réactivité et flexibilité >** Une forte adaptabilité pour répondre à toutes vos exigences

05. Pare-Feu nouvelle génération

Un système de défense perfectionné face à des attaques avancées

Bloquez plus de menaces et contrez rapidement celles qui passent à travers vos défenses grâce au premier pare-feu de nouvelle génération axé sur les menaces. Les pare-feu Cisco conjuguent les performances des pare-feu réseau avec celles des meilleurs systèmes de prévention des intrusions nouvelle génération et de protection contre les malwares avancés. Bénéficiez ainsi d'une meilleure visibilité et de plus de souplesse, et réalisez des économies en étant mieux protégé.

ASA 5500-X + fonctionnalités FirePower

- Pour le PME et les succursales
- Débit entre 256 et 1750 Mbit/s
- Inspection des menaces entre 125 et 1250 Mbit/s

FirePower Série 4100

- Pour la périphérie web, les environnements à haute performance
- Débit entre 12 et 30 Gbit/s
- Inspection des menaces entre 10 et 24 Gbit/s

Appliance de sécurité adaptative virtuelle (ASAv)

- Optimisée pour les environnements cloud et data center
- Prise en charge de VMware, de KVM et de l'hyperviseur Hyper-V
- AWS, Azure et cloud gouvernemental Azure
- Débit pare-feu compris entre 100 Mbit/s et 10Gbit/s, qui consomme 1 à 16 Go de mémoire
- Pare-feu « stateful » ASA, VPN
- Inspection des menaces entre 10 et 24 Gbit/s

Meraki MX

- Gestion unifiée des menaces (UTM) dans le cloud pour les environnements distribués
- Débit entre 250 Mbit/s et 6 Gbit/s
- SD-WAN intégré
- Pare-feu « stateful », visibilité et contrôle sur les applications, système de prévention des intrusions nouvelle génération, protection avancée contre les malwares, filtrage des URL

FirePower série 2100

- De la périphérie web jusqu'aux data centers
- Débit entre 2 et 8,5 Gbit/s
- Inspection des menaces entre 2 et 8,5 Gbit/s

FirePower série 9000

- Pour les opérateurs télécoms, les data centers
- Débit jusqu'à 225 Gbit/s
- Inspection des menaces jusqu'à 90 Gbit/s

Pare-Feu virtuel de nouvelle génération

- Optimisé pour les environnements cloud et data center
- Prise en charge de VMware, de KVM et de l'hyperviseur Hyper-V
- AWS, Azure et cloud gouvernemental Azure
- Débit de 1,2 Gbit/s (pare-feu + Cisco AVC), débit 1,1 Gbit/s (Cisco AVC + système IPS)
- Pare-feu « stateful », visibilité et contrôle des applications (AVC), système de prévention des intrusions nouvelle génération (NGIPS), protection contre les menaces avancées (AMP), filtrage des URL, VPN

Besoin d'infos ou d'un devis ?

CONTACT

06. Prévention des intrusions - *NEW*

Une protection complète et intégrée

Face à l'évolution des cyberattaques, vous avez besoin d'une visibilité et d'informations toujours plus précises sur l'ensemble des menaces afin d'assurer une protection complète du réseau. Les différents besoins et priorités au sein de l'entreprise appellent également à une mise en oeuvre cohérente des politiques de sécurité. Pour répondre à ces nouvelles exigences opérationnelles et renforcer la sécurité dans votre entreprise, l'adoption d'un système de prévention des intrusions (NGIPS) dédié est devenue indispensable.

Visibilité

Avec Firepower Management Center, vous avez accès à davantage de données contextuelles sur votre réseau pour pouvoir ajuster vos politiques de sécurité. Vous pouvez voir les apps, signes de compromission, profils d'hôte, trajectoire des fichiers, opérations de sandboxing, informations concernant les vulnérabilités et bien d'autres...

Flexibilité

Le système NGIPS Cisco Firepower offre des options de déploiement flexibles pour répondre à tous les besoins de l'entreprise. Il peut être déployé sur le périmètre du réseau, au niveau de la couche distribution/coeur du data center, ou derrière le pare-feu pour protéger les ressources stratégiques, l'accès invité et les connexions WAN.

Efficacité

Les systèmes NGIPS reçoivent de nouvelles signatures et règles toutes les deux heures, pour garantir une protection optimale. Cisco Talos s'appuie sur le plus grand réseau de détection des menaces au monde pour optimiser l'efficacité de tous les produits de sécurité Cisco.

Intégration

Le déploiement du système NGIPS Firepower sur votre réseau est rapide et ne nécessite aucune modification matérielle majeure. Activez et gérez différentes applications de sécurité depuis une interface unique avec Firepower Management Center.

Coûts opérationnels

Utilisez l'automatisation NGIPS pour augmenter l'efficacité opérationnelle et réduire les coûts en distinguant le simple bruit des événements exploitables. Hiérarchisez les menaces pour simplifier le travail de vos équipes et améliorez votre sécurité en appliquant des politiques recommandées en fonction des vulnérabilités de votre réseau.

Des applicances ultra performantes

Les appliances Cisco Firepower (séries 4100 et 9000) et FirePOWER (séries 7000 et 8000) sont spécialement conçues pour offrir un débit adapté à vos besoins, une conception modulaire et une évolutivité exceptionnelle. Elles intègrent une conception à faible latence et à passage unique et des interfaces fail-to-wire.

Trouvez le système de prévention des intrusions nouvelles génération idéal

FirePower Série 4100

• Conçu pour les environnements ultraperformants à la périphérie d'Internet
• Inspection des menaces entre 10 et 20 Gbit/s
• Cisco Application Visibility and Control intégré avec AMP et URL en option
• Interfaces fail-to-wire disponibles

FirePower Série 7000

• Conçu pour les services commerciaux et les bureaux distants
• Inspection des menaces entre 50 Mbit/s et 1,25 Gbit/s
• 8 à 12 interfaces de surveillance
• Small Form-Factor Pluggable (SFP) : 2 modèles

Réseaux FirePower Série 9000

• Conçu pour les opérateurs télécoms et les déploiements de data centers
• Inspection des menaces jusqu'à 90 Gbit/s
• Cisco Application Visibility and Control intégré avec AMP et URL en option
• Interfaces fail-to-wire disponibles

NGIPSv pour VMware

• Petites succursales et bureaux distants
• Inspection des menaces jusqu'à 800 Mbit/s
• Data center est-ouest/serveurs critiques PCI
• Fonctionnalités complètes du système NGIPS et de ses options

FirePower Série 8000

• Conçu pour les déploiements d'entreprise et de réseaux locaux
• Inspection des menaces jusqu'à 60 Gbit/s
• Évolutivité empilable
• Interfaces fail-to-wire disponibles

Solutions de protection FirePower pour ISR Cisco (NGFWv)

• Conçue pour les succursales et les bureaux distants
• Inspection des menaces jusqu'à 800 Mbit/s
• Déploiement sur des routeurs série 4000 et ISR G2
• Sécurité renforcée et réduction des coûts liés au réseau WAN

Besoin d'infos ou d'un devis ?

CONTACT

07. Sécurité des routeurs

Protégez vos données contre les programmes malveillants, les intrusions, les attaques par déni de service et menaces avancées. Les routeurs Cisco conjuguent leurs efforts pour étendre la sécurité de l'entreprise à vos succursales et protéger l'ensemble de votre réseau. Grâce aux fonctions de sécurité intégrées, vous êtes protégé contre les menaces sophistiquées, tout en gardant un haut niveau de performance et en réduisant les coûts.

Simplifier la gestion des succursales

Gagnez du temps et de l'argent grâce à une plate-forme tout-en-un, physique ou virtuelle.

Riposter rapidement face aux menaces

Gérez les vulnérabilités de votre réseau. Protégez vos succursales et vos clients là où ils en ont le plus besoin.

Gagner en visibilité avec l'analytique

Étendez la visibilité sur le réseau des succursales pour mieux adapter vos services de sécurité.

Réduire les coûts améliorer les performances

Utilisez un chemin d'accès Internet pour réduire la consommation de bande passante et améliorer les performances des applications.

Pourquoi travailler avec DistriWan ?

- **Offre de services >** Un catalogue de prestations sur-mesure et adaptées à vos besoins
- **Expertise >** Une équipe avant-vente spécialisée par architecture
- **Accompagnement >** Une équipe commerciale à votre écoute pour répondre à toutes vos demandes de projets
- **Réactivité et flexibilité >** Une forte adaptabilité pour répondre à toutes vos exigences

Trouvez la solution la plus adaptée à vos besoins en matière de sécurité

Les routeurs à services intégrés Cisco ISR, les routeurs avec services d'agrégation Cisco ASR 1000 et les routeurs de services cloud Cisco 1000v forment une suite complète de technologies de sécurisation du routage.

Protection des succursales

Profitez de fonctions de contrôle du périmètre du réseau, de prévention des intrusions, de sécurisation du web et de protection contre les programmes malveillants.

- Pare-feu IOS par zone
- Système de prévention des intrusions Snort
Umbrella en succursale
- Fonctionnalités cloud de sécurisation du web
- Solution de protection FirePOWER pour ISR

Connectivité sécurisée

Parmi les modes de connectivité ultrasécurisés, on trouve les technologies VPN d'accès à distance et de site à site. Elles protègent les communications sensibles de l'entreprise.

- DMVPN
- VPN GET

Visibilité et analytique

Avec plus de visibilité, vous pouvez suivre le trafic du réseau et établir des points de référence. Les fonctions d'analytique identifient les comportements anormaux pour vous permettre d'agir.

- Licence Stealthwatch Learning Network

Besoin d'infos ou d'un devis ?

CONTACT

08. Clients VPN, sécurité des terminaux

Une protection continue pour votre entreprise

Les menaces exploitent de nombreux vecteurs d'attaque. Vous devez donc assurer une connectivité sécurisée et la protection permanente de vos terminaux. Déployez des clients Cisco de sécurisation des terminaux sur Mac, PC, Linux ou des terminaux mobiles pour protéger vos collaborateurs sur les réseaux sans fil, filaires ou VPN.

Accès simple et sécurisé

Donnez les moyens à vos collaborateurs de travailler partout et à tout moment, aussi bien sur les ordinateurs portables de l'entreprise que sur leurs terminaux mobiles personnels. Bénéficiez d'une visibilité sur vos terminaux à l'échelle de l'entreprise. Protégez vos collaborateurs sur le réseau et en dehors. Mettez en oeuvre des politiques de gestion de l'état des terminaux connectés.

Gestion centralisée des équipements

Contrôlez les terminaux mobiles et les équipements de bureau depuis le tableau de bord Meraki sécurisé accessible par navigateur. Intégrez en toute fluidité les nouveaux équipements et automatisez l'application des politiques de sécurité.

Visibilité, données contextuelles et contrôle

Prévenez les failles de sécurité. Surveillez en continu le comportement de tous vos fichiers afin de repérer les attaques furtives. Détectez, bloquez et éliminez les malwares avancés sur tous vos terminaux, rapidement et automatiquement.

Besoin d'infos ou d'un devis ?

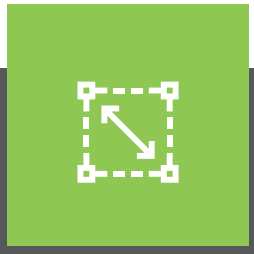
CONTACT

09. Sécurité du Web

Les menaces les plus avancées peuvent se cacher dans les endroits les plus anodins, sur des sites web dignes de confiance ou dans des fenêtres publicitaires attrayantes. Vos collaborateurs ou vos invités peuvent mettre votre entreprise en péril en cliquant là où ils ne devraient pas. L'appliance Cisco pour la sécurité du web (WSA) est optimisée par Talos. Elle vous protège en bloquant automatiquement les sites à risque et en testant les sites inconnus avant d'autoriser les utilisateurs à y accéder, renforçant ainsi la conformité.

Protection avant, pendant et après une attaque

Profitez d'une surveillance et d'une analyse automatisées sur tout le réseau. Lorsqu'un incident se produit, déterminez rapidement l'étendue des dégâts, éliminez le problème et rétablissez un fonctionnement normal.



Des options de déploiement flexibles

Sécurisez le web depuis une appliance, une machine virtuelle, voire le routeur d'un site distant, et ce, sans frais supplémentaires. Cette solution de sécurité ouverte vous permet de faire évoluer votre environnement au même rythme que votre entreprise. Protégez vos sites distants sans acheminer le trafic vers la passerelle de l'entreprise.

Des analyses automatisées du trafic entrant et sortant

Analysez tout le trafic web en temps réel, à la recherche de malwares connus et de nouvelles menaces. Utilisez l'analyse dynamique de la réputation et l'analyse comportementale sur tout le contenu web.

L'identification rapide des attaques de type «zero day»

Recherchez les activités suspectes en permanence afin de détecter tout comportement anormal. Appliquez l'analyse rétrospective avec Advanced Malware (AMP) pour la sécurisation du web en ayant la possibilité de retracer le parcours passé et d'éliminer les malwares dans les périphériques infectés.

CONTACT

Pourquoi travailler avec DistriWan ?

- **Offre de services >** Un catalogue de prestations sur-mesure et adaptées à vos besoins
- **Expertise >** Une équipe avant-vente spécialisée par architecture
- **Accompagnement >** Une équipe commerciale à votre écoute pour répondre à toutes vos demandes de projets
- **Réactivité et flexibilité >** Une forte adaptabilité pour répondre à toutes vos exigences