The bridge to possible

Cisco Secure Workload

Table des matières

Réduisez votre surface d’attaque et protégez les applications qui propulsent votre entreprise

Les applications constituent le moteur des affaires. Elles permettent de mettre en relation les entreprises avec leurs clients, leurs employés, leurs chaînes logistiques, leurs partenaires et même de générer des revenus. Mais la prolifération et la nature dynamique des applications modernes ont créé des défis de sécurité sans précédent.

Aujourd’hui, les applications sont distribuées. Elles sont déployées à la fois sur site et dans le nuage, ou sur plusieurs nuages, et les charges de travail critiques ne sont plus conservées dans le centre de données où elles peuvent être protégées par un pare-feu de périmètre. À certains égards, le concept traditionnel de périmètre appartient en grande partie au passé. Pour évoluer dans ce monde multinuage hybride et centré sur les applications, vous avez besoin d’une solution de sécurité qui est plus proche de l’application et compatible avec toutes les infrastructures sous-jacentes, ce qui vous permet de protéger ce qui compte le plus : vos applications et vos données.

Cisco[MD] Secure Workload protège les applications en offrant une microsegmentation Zero Trust fluide pour toutes les charges de travail, tous les environnements ou emplacements à partir d’une console unique. La microsegmentation Zero Trust empêche le déplacement latéral en appliquant une politique de pare-feu distribué ou « micropérimètre » ainsi qu’un accès de type « moindre privilège » à chaque charge de travail. Cisco Secure Workload est une solution pour l’ensemble de votre environnement applicatif, que les applications soient déployées sur des serveurs sans système d’exploitation, des machines virtuelles ou des conteneurs. Ce produit est flexible et compatible avec toutes les infrastructures, offre des capacités avec et sans agent, protège les charges de travail dans le centre de données et chez les principaux fournisseurs de nuage public, comme AWS, Azure et GCP.

Avantages

- Limitez les violations et empêchez les menaces de se propager en mettant en œuvre la microsegmentation Zero Trust de manière fluide pour tous les environnements, toutes les charges de travail ou tous les emplacements à partir d’une seule solution.
- Améliorez immédiatement votre posture de sécurité grâce à une visibilité approfondie de la charge de travail de chaque application et de l’interaction comportementale avec les utilisateurs et les appareils.
- Tirez parti d’une puissante automatisation basée sur l’intelligence artificielle et l’apprentissage automatique pour formuler des recommandations de politiques exemplaires, adaptées à votre environnement et à vos applications uniques.
- Assurez la conformité avec un modèle de politique hiérarchique qui offre des protections complètes pour plusieurs groupes d’utilisateurs grâce au contrôle d’accès basé sur les rôles.
- Obtenez des renseignements exploitables grâce à des rapports basés sur le profil, une supervision de la conformité en temps quasi réel et des alertes d’investigation basées sur le cadre MITRE ATT&ACK.

Protégez les applications de manière uniforme et précise

Grâce à des fonctionnalités avancées d’intelligence artificielle et d’apprentissage automatique, Cisco Secure Workload rend la microsegmentation Zero Trust pratique et réalisable. Les processus intelligents à la base de Cisco Secure Workload cartographient chaque interaction et dépendance de l’application et conseillent des politiques adaptées à votre environnement et à vos applications uniques.

Cisco Secure Workload vous permet de réaliser les actions suivantes :

- Tester et valider les politiques Zero Trust sans avoir d’incidence sur l’application
- Automatiser les politiques pour les scénarios souhaités
- Appliquer les politiques de manière uniforme et précise, même lorsque les charges de travail se déplacent ou évoluent
- Utiliser l’analyse historique à long terme pour affiner et tester les modifications de politiques afin d’améliorer constamment votre posture de sécurité
- Maintenir la conformité interne grâce à un modèle de politique hiérarchique qui fournit des protections complètes pour plusieurs groupes d’utilisateurs avec un contrôle d’accès basé sur les rôles
- Assurer une intégration à la chaîne d’outils de CI/CD pour écrire la politique en tant que code, assurant une sécurité renforcée et un déploiement plus rapide des applications

Améliorez immédiatement votre posture de sécurité

Avec Cisco Secure Workload, vous obtenez une visibilité complète sur chaque communication relative à la charge de travail des applications, afin de déterminer ce que font vos applications et leurs interactions comportementales avec les utilisateurs et les appareils. Cisco Secure Workload offre des avantages immédiats dès le début.

Quelques jours après le déploiement, vous pouvez renforcer votre sécurité en :

- bloquant des communications non sécurisées ;
- définissant le périmètre des postes de travail virtuels ;
- bloquant les communications indésirables d’application à application ;
- identifiant les vulnérabilités logicielles et en appliquant des correctifs virtuels ;
- arrêtant tous les ports de gestion vulnérables.

Des renseignements exploitables à portée de main

Pensé pour les environnements applicatifs complexes d’aujourd’hui, Cisco Secure Workload est conçu pour évoluer et fonctionner à grande vitesse. En quelques secondes, il peut traiter des millions de flux et vous alerter d’une infraction à la politique ou d’une menace potentielle. Et, en quelques minutes, vous pouvez adopter des politiques pour éviter que cela ne se reproduise ou pour automatiser le processus.

Cisco Secure Workload fournit les fonctionnalités suivantes :

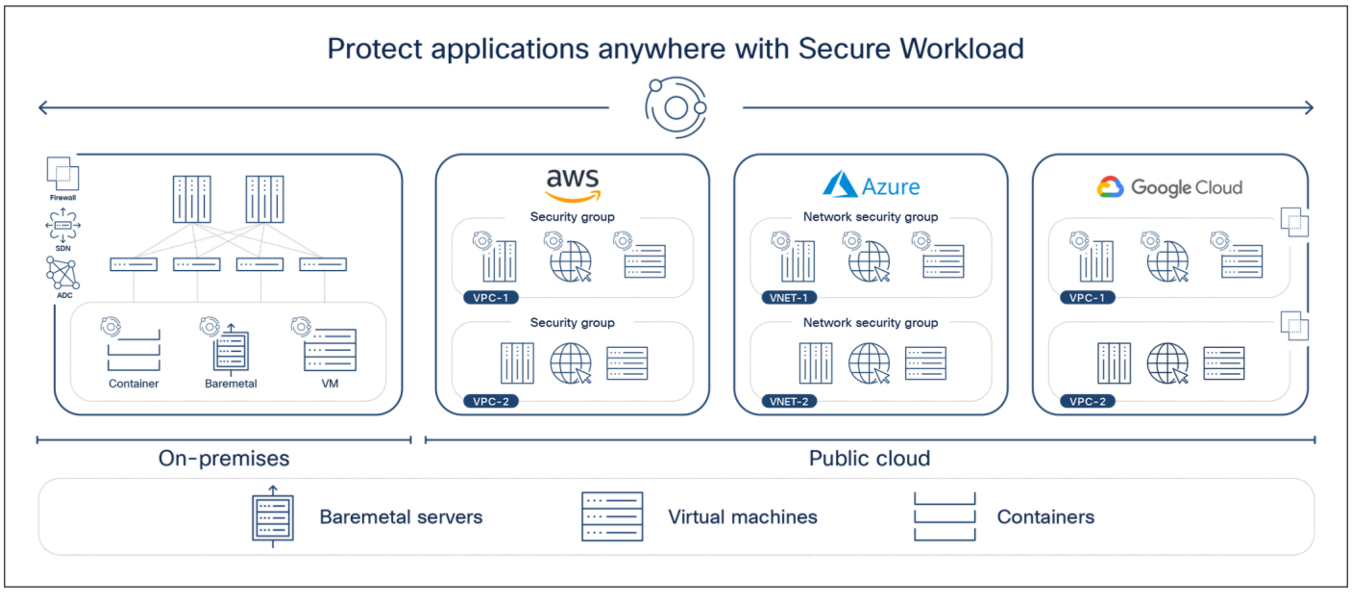
- Supervision en temps réel qui identifie les comportements non autorisés, les infractions à la politique et les menaces potentielles, et envoie des alertes
- Rapports personnels qui décrivent l’intégrité globale de la sécurité des applications et illustrent les tendances émergentes en fonction des données historiques
- Alertes criminalistiques basées sur le cadre MITRE ATT&ACK
- DVR des comportements anormaux et enregistrement vérifiable

Une solution pour protéger les applications, réduire les risques et maintenir la conformité

Grâce à une visibilité complète sur chaque interaction avec la charge de travail et à sa puissante automatisation basée sur l'intelligence artificielle et l'apprentissage automatique, Cisco Secure Workload réduit la surface d'attaque en empêchant le déplacement latéral, identifie les anomalies de comportement de la charge de travail, aide à corriger rapidement les menaces et supervise en permanence la conformité.

Cisco Secure Workload vous permet de réaliser les actions suivantes :

- Maintenir les tâches opérationnelles même en présence de menaces
- Réagir rapidement aux changements dans votre environnement
- Réduire les temps d'arrêt des applications
- Intégrer rapidement les nouvelles applications sans friction



Défense approfondie : Cisco Secure Firewall et service Cisco de vérification des identités

Cisco Secure Workload s'intègre de manière native à Cisco Secure Firewall pour unifier les points de contrôle, fournir une défense en profondeur et permettre une approche sans agent dans les scénarios sur site souhaités. L'intégration offre aux clients le contrôle granulaire pour découvrir, appliquer et automatiser certaines politiques sur un pare-feu ou un ensemble de pare-feu spécifique à l'aide de Cisco Secure Workload. De plus, Cisco Secure Workload et Cisco Secure Firewall peuvent partager de manière fluide les renseignements sur les menaces et veiller à ce que la bonne signature SNORT soit appliquée pour protéger l'application contre une vulnérabilité connue. Cisco Secure Workload s'intègre également de manière native à l'identifiant ISE passif du service Cisco de vérification des identités, en assimilant les attributs d'utilisateur, de groupe et d'autres attributs de l'annuaire Active Directory et/ou Azure du client. Cela fournit des renseignements contextuels enrichis qui permettent une visibilité et la mise en œuvre des politiques en fonction de l'identité des terminaux.

Une sécurité renforcée aujourd’hui et pour l’avenir

Cisco Secure Workload protège les charges de travail des applications critiques sans compromettre l’agilité. Il s’agit d’une solution stratégique qui offre des rendements immédiats grâce à une sécurité renforcée dès le départ et des avantages commerciaux d’une grande valeur pour l’avenir. Avec Cisco Secure Workload, vous pouvez protéger votre entreprise contre les violations et les menaces avancées, ce qui protège également les données de vos clients et augmente leur confiance dans votre marque. En tant que catalyseur clé pour de nombreuses initiatives de conformité réglementaire, il allège le coût et la portée de ces efforts. Et, une fois en place, Cisco Secure Workload prend facilement en charge l’intégration de nouveaux processus et applications opérationnels, accélérant et sécurisant ainsi le développement et le déploiement d’applications.

Cisco Secure Workload est proposé en tant que dispositif SaaS et sur site. À vous de choisir l’option qui vous convient le mieux.

Pour en savoir plus : cisco.com/go/secureworkload.

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose, Californie

Siège social d’Asie-Pacifique
Cisco Systems (USA) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam,
Pays-Bas

Cisco compte plus de 200 bureaux à l’échelle mondiale. Les adresses, numéros de téléphone et de fax sont indiqués sur le site Web de Cisco à l’adresse suivante : **https://www.cosco.com/go/offices**.

Imprimé aux États-Unis C45-3810661-00 08/23