Fiche technique
Document public de Cisco

Cisco Secure Workload pour la protection de la charge de travail

Août 2023

The bridge to possible

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Table des matières

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Cisco Secure Workload (anciennement Tetration) offre une microsegmentation Zero Trust fluide pour toutes les charges de travail, tous les environnements ou emplacements à partir d'une console unique. 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.

Présentation du produit

Traditionnellement, dans le secteur informatique, notre vision était centrée sur l'infrastructure. Nos données les plus précieuses se trouvaient dans le centre de données, et notre tâche consistait donc à laisser entrer le bon trafic et à empêcher les intrusions d'acteurs malveillants. Et notre outil de prédilection était le pare-feu.

Dans les entreprises d'aujourd'hui, le centre de gravité a résolument changé en faveur des applications. Les applications sont essentielles à la façon dont vous communiquez avec vos clients, gérez vos opérations et êtes payés. Mais la prolifération constante et la nature dynamique de ces applications ont créé un défi de sécurité sans précédent pour les professionnels de l'informatique.

Les applications sont distribuées. Elles sont déployées en périphérie, à proximité de l'utilisateur, dans le centre de données sur site ou dans le nuage privé, et dans le nuage, ou sur plusieurs nuages. 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. D'une certaine manière, on pourrait même considérer que le périmètre n'existe plus. Pour prospérer dans ce monde centré sur les applications, vous avez besoin d'une solution de sécurité capable de rapprocher la sécurité des applications à l'aide d'un « nouveau pare-feu ou micropérimètre » qui entoure chaque charge de travail, vous permettant de protéger ce qui compte le plus pour vous : vos applications et vos données.

Avec Cisco Secure Workload, vous pouvez **sécuriser votre environnement applicatif en créant un micropérimètre au niveau de la charge de travail pour l'ensemble de votre infrastructure**, que les applications soient déployées sur des serveurs sans système d'exploitation, des machines virtuelles ou des conteneurs. Cisco Secure Workload **offre une microsegmentation Zero Trust pour protéger les applications, réduire les risques** et **maintenir la conformité** grâce à :

- des politiques de microsegmentation générées automatiquement au moyen d'une analyse complète des schémas et des dépendances de communication des applications à l'aide de modèles d'apprentissage automatique,
- la définition dynamique de politiques en fonction d'attributs avec un modèle de politique hiérarchique pour fournir des contrôles complets dans plusieurs groupes d'utilisateurs avec des contrôles d'accès basés sur le rôle,
- l'application cohérente de politiques à grande échelle grâce au contrôle distribué des pare-feu de l'hôte natif, des mécanismes de sécurité intégrés dans le nuage et à l'infrastructure, y compris des contrôleurs de distribution d'applications (Application Delivery Controllers ou ADC), des pare-feu et des réseaux,
- la supervision en temps quasi réel de la conformité de toutes les communications afin d'identifier une infraction à la politique ou une compromission potentielle, et d'émettre des alertes,
- la définition d'un ensemble de règles comportementales sur la charge de travail et la détection proactive des anomalies,
- la détection des vulnérabilités courantes grâce à l'atténuation dynamique et à la quarantaine basée sur les menaces.

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Figure 1.
Cisco Secure Workload – approche de protection de la charge de travail

Sécuriser les applications grâce à la microsegmentation

Cisco Secure Workload fournit à votre équipe des recommandations automatisées en matière de politiques de microsegmentation, et vous aide à appliquer ces politiques de manière uniforme et à grande échelle dans tous vos environnements. Ce modèle **réduit considérablement votre surface d'attaque, augmente l'efficacité opérationnelle** grâce à l'automatisation et **permet un modèle Zero Trust**.

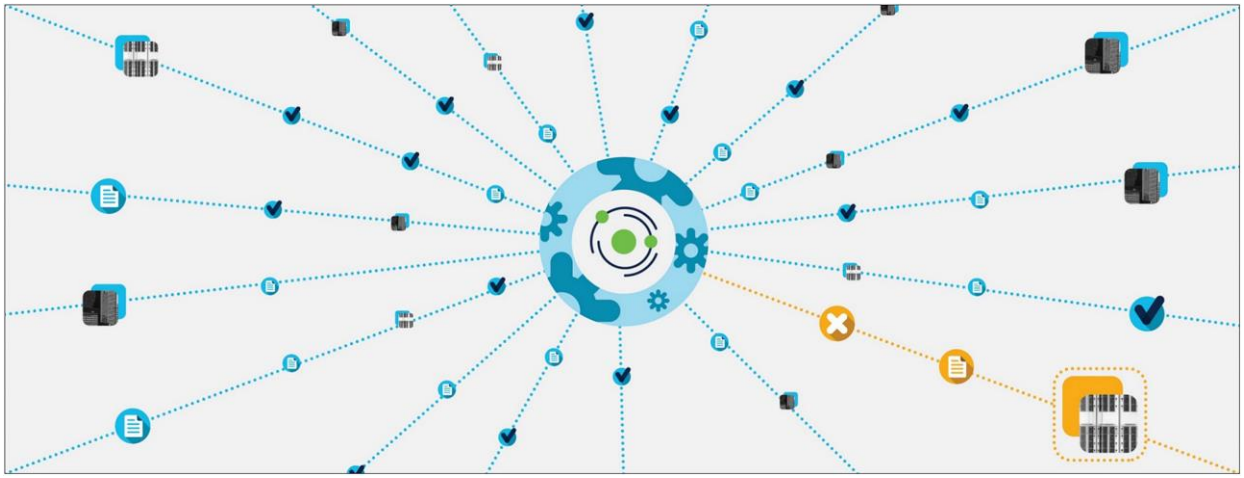

Figure 2.
Sécuriser les applications grâce à la microsegmentation dans n'importe quel nuage

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Définition de politiques flexibles enrichies en métadonnées

Compte tenu de la nature changeante des applications et des infrastructures dans lesquelles elles sont déployées, un modèle de politiques flexible et dynamique est essentiel. Qu'elles soient distribuées sur plusieurs nuages ou qu'elles soient exploitées sur le même segment de réseau, les charges de travail individuelles ont des exigences de politique distinctes basées sur un riche ensemble d'attributs qui définissent l'application et l'environnement, l'emplacement, le contexte réglementaire et bien plus encore.

Pour ce faire, Cisco Secure Workload gère un inventaire riche en contexte de chaque charge de travail et de chaque terminal, ainsi que des métadonnées associées, grâce à l'intégration avec les systèmes d'enregistrement existants, notamment la base de données de gestion des configurations (CMDB), la gestion des adresses IP (IPAM), les principaux fournisseurs de services infonuagiques, les plateformes d'orchestration, les systèmes de contrôle d'accès et d'authentification.

Le langage naturel de définition de politiques de Cisco Secure Workload permet aux utilisateurs de créer et d'appliquer des intentions dynamiques de politiques pour répondre à toute demande, que ce soit pour garantir un accès restreint des utilisateurs ou des terminaux à une application essentielle, ou pour respecter la conformité réglementaire ou les mandats de l'InfoSec.

La politique est continuellement mise à jour en fonction de l'évolution de l'environnement, ce qui garantit une mise en œuvre actuelle des politiques à chaque point d'application.

	Action	Consumer	Provider	Services
Regulatory Policy	Deny	Untrusted	Highly Sensitive	Any
Security Policy	Deny	Prod Workloads	Non-Prod Workloads	Any
Network Policy	Allow	Trusted Management	Mission Critical Retail	SSH
	Allow	Prod Workloads	Approved DNS	DNS

Figure 3.
Définition de politiques flexibles basées sur les métadonnées

Recommandation automatisée de politiques de microsegmentation

En utilisant la plateforme Cisco Secure Workload, vous pouvez **générer automatiquement des politiques de microsegmentation très spécifiques** basées sur une visibilité complète des communications de l'application, des processus en cours et de leurs dépendances. L'outil fusionne de manière déterministe la stratégie générée automatiquement avec la stratégie enrichie en métadonnées définie par l'utilisateur pour une visualisation détaillée de la politique. Cisco Secure Workload permet à l'utilisateur d'examiner, de tester et d'affiner la politique pour fournir un ensemble de politiques précis et détaillé qui peut être déployé et appliqué en toute confiance.

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

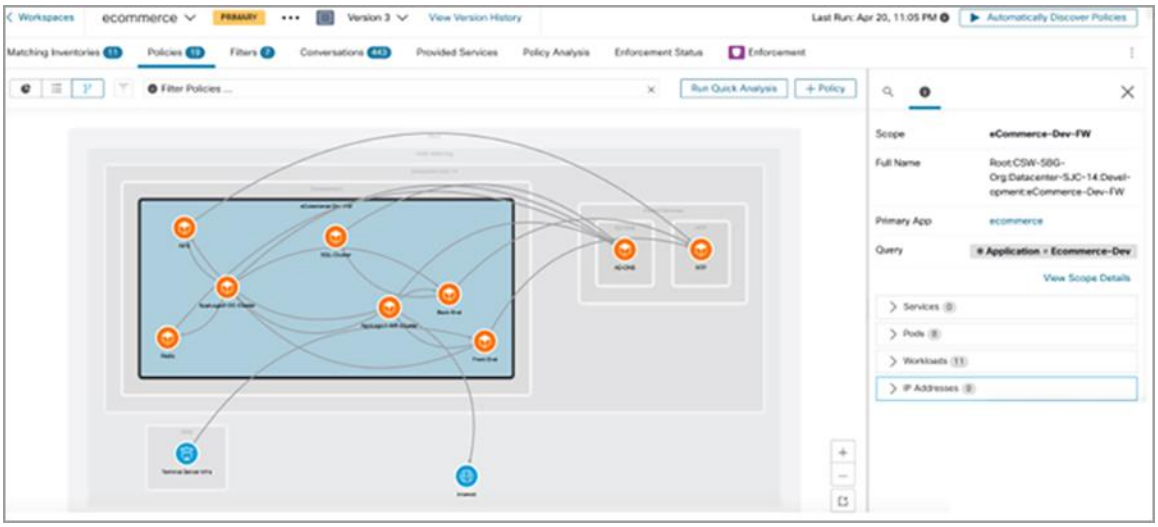

Figure 4.
Recommandation automatisée de politiques de microsegmentation basée sur le comportement de l'application

Les propriétaires d'applications peuvent prendre le contrôle

Avec Cisco Secure Workload, la sécurité devient un vecteur d'innovation rapide, car les propriétaires d'applications peuvent s'approprier les politiques pour leurs applications. En tirant parti d'un modèle de politique hiérarchique et d'un contrôle d'accès basé sur les rôles (Role-Based Access Control ou RBAC), les équipes applicatives peuvent mettre en œuvre des politiques dynamiques tout en respectant les limites des exigences des politiques de l'entreprise.

Figure 5.
Les propriétaires d'applications sont habilités grâce au contrôle des politiques

Les politiques peuvent être flexibles en utilisant l'affectation d'étiquettes de charge de travail au moyen de l'intégration avec les plateformes d'orchestration couvrant les charges de travail basées sur des machines virtuelles et des conteneurs. Les flux de travail d'intégration et de déploiement continus (CI/CD) sont automatisés au moyen d'ensembles de politiques basés sur les API, tout en maintenant la cohérence de bout en bout au-delà des limites de l'entreprise.

Le modèle de politique dynamique de Cisco Secure Workload permet également d'automatiser la réponse à la politique, par exemple une mise en quarantaine ou un renforcement qui peut être déclenché(e) directement ou par une intégration tierce via une API.

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Application automatisée des politiques à grande échelle

Que votre environnement se compose de centaines ou de milliers de charges de travail, Cisco Secure Workload est conçu pour être évolutif, permettant l'application entièrement automatisée d'une politique dynamique de liste d'autorisation pour chaque charge de travail. Un ensemble de politiques distinct est calculé de manière personnalisée pour chaque charge de travail, distribué par l'agent logiciel Cisco Secure Workload et programmé pour être appliqué par le pare-feu du système d'exploitation natif (iptables ou Pare-feu Windows).

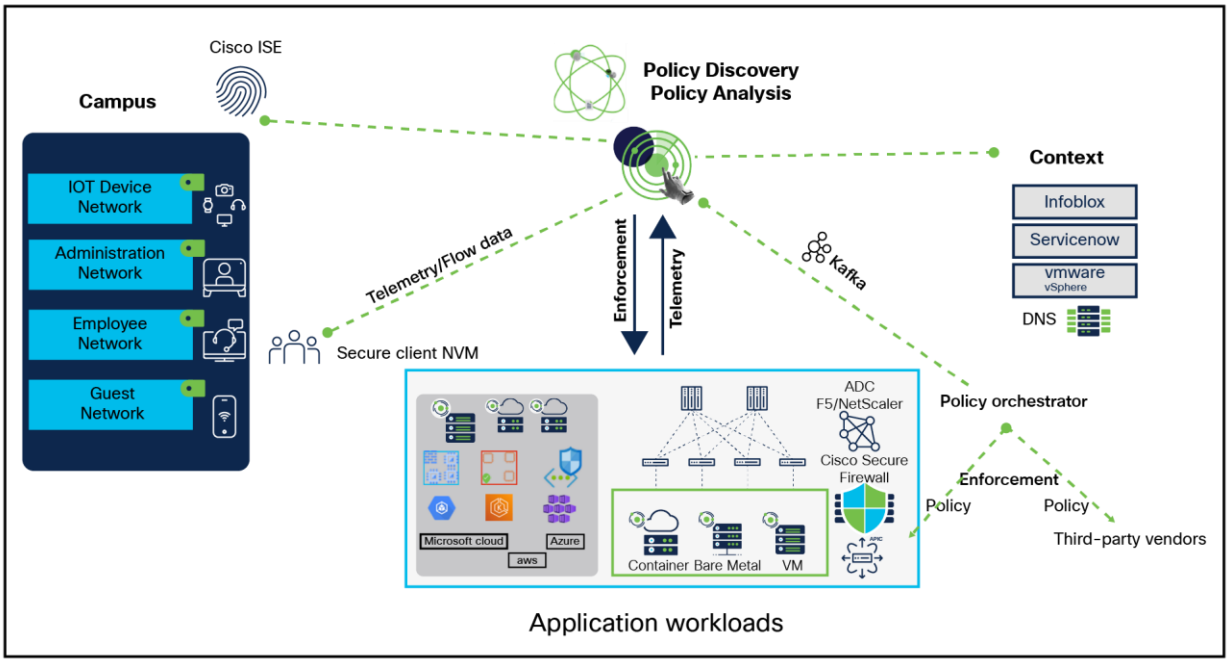

Figure 6.
Application des politiques dans une infrastructure multinuage pour permettre une segmentation cohérente

Cisco Secure Workload peut également utiliser une approche sans agent pour protéger les charges de travail en faisant appel à Cisco Secure Firewall et aux contrôles de politique natifs des principaux fournisseurs de services infonuagiques comme AWS, Azure et Google sous la forme de groupes de sécurité et de règles de pare-feu. L'intention de politique générée est également diffusée en flux continu sur un courtier Kafka sécurisé et sur une API pour une application plus poussée dans l'infrastructure. Elle est transmise aux ADC au moyen d'une intégration directe pour assurer une application cohérente des politiques pour toutes les charges de travail dans le centre de données et dans le nuage.

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

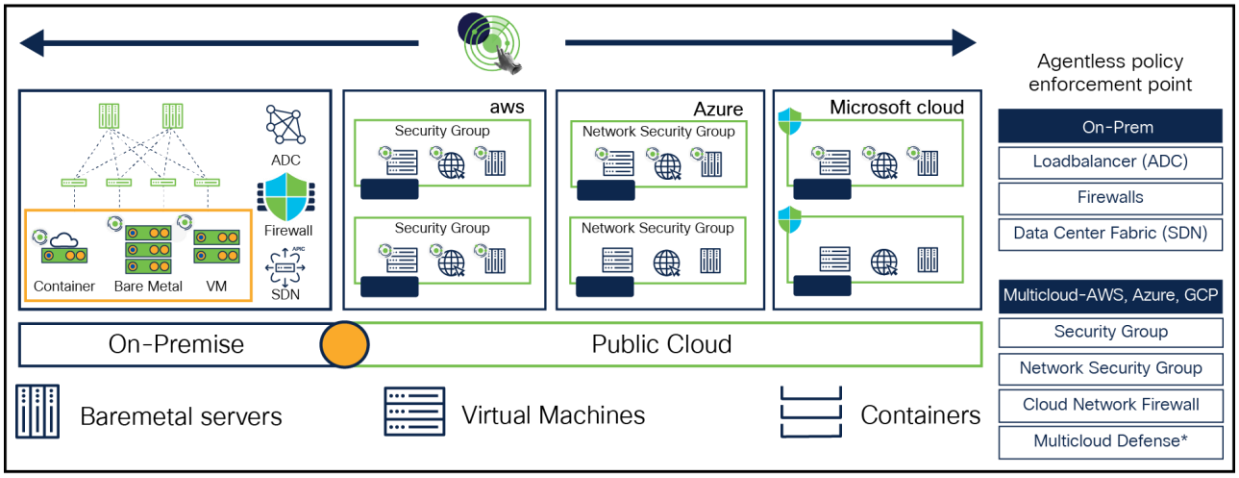

Figure 7.
Application des politiques avec et sans agent dans un environnement multinuage hybride

Visibilité et conformité en temps quasi réel

Cisco Secure Workload offre une visibilité continue sur toutes les activités de communication grâce à une évaluation de la conformité aux politiques en temps quasi réel pour vous alerter rapidement de toute infraction à la politique. Les enregistrements de flux sont conservés pour un enregistrement criminalistique de toutes les communications avec une analyse de la disposition des flux afin d'identifier la correspondance de politique spécifique. Que ce soit pour répondre à une violation ou pour vous adapter à des changements de comportement d'une application, vous aurez un enregistrement complet et à jour de toutes les communications pour contribuer aux efforts d'intervention et de correction rapides.

Réduire les risques et maintenir la conformité

Cisco Secure Workload vous aide à réduire les risques globaux et à maintenir la conformité en identifiant automatiquement les écarts de comportement des applications et en appelant les flux de travail appropriés pour les mises à jour des politiques. Les observations basées sur l'analyse vous permettent d'acquérir un point de vue unique sur les opérations de votre environnement, et servent de déclencheur pour accroître l'efficacité et la sécurité.

Ensemble de règles comportementales de la charge de travail et détection des anomalies

Cisco Secure Workload **supervise en permanence et établit les références des processus en cours d'exécution sur chaque serveur**, capturant le contexte détaillé pour chaque processus et ses bibliothèques associées. Les processus et les condensés de bibliothèque sont évalués par rapport à un flux de données sur les menaces pour identifier les exécutions de code malveillant et détecter les écarts par rapport aux processus connus comme étant sains.

Les charges de travail sont supervisées afin de détecter les indicateurs comportementaux de compromission au moyen d'un ensemble configurable d'indicateurs d'événements criminalistiques. Ces indicateurs criminalistiques comprennent des détections d'événements du système d'exploitation ainsi qu'un ensemble personnalisé de techniques MITRE ATT&CK, permettant d'identifier les comportements anormaux et de déclencher des alertes.

Les équipes chargées des opérations de sécurité peuvent personnaliser ces événements, leur gravité et les actions associées à l'aide de règles simples à définir. De cette façon, elles peuvent identifier rapidement les indicateurs de compromission et prendre des mesures correctives pour réduire l'impact.

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Les enregistrements d'événements criminalistiques fournissent un instantané du processus pertinent et des métadonnées capturées au sein de l'événement pour faciliter l'analyse des exploits.

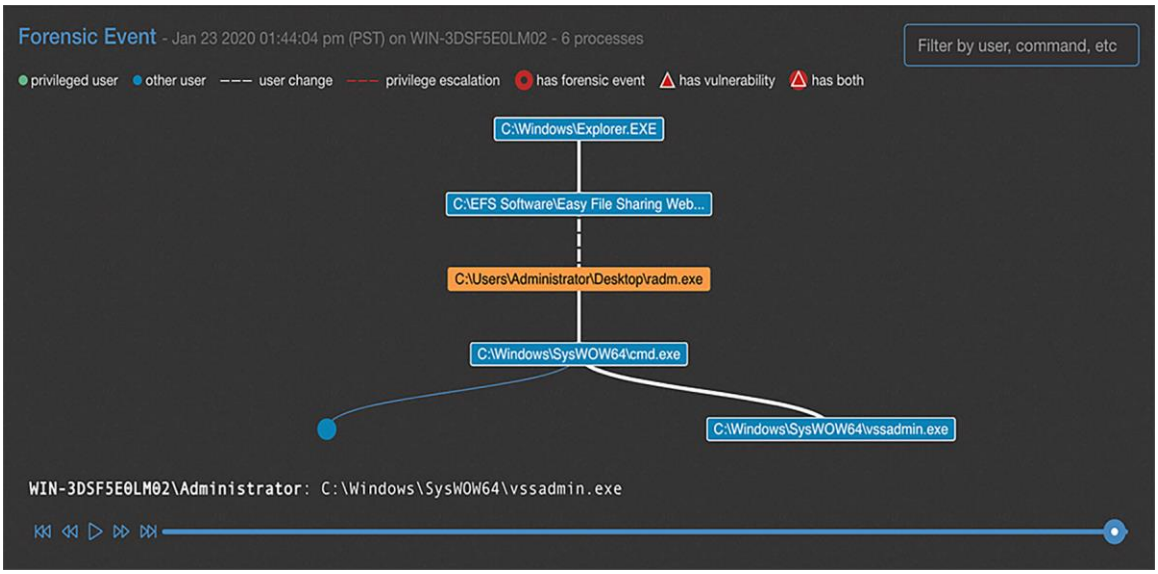

Figure 8.
Événement criminalistique

Détection proactive des vulnérabilités logicielles

Cisco Secure Workload détecte les progiciels et les versions des logiciels installés sur vos serveurs pour produire des rapports sur les vulnérabilités connues en matière de sécurité de l'information en faisant correspondre les versions des logiciels installés avec un flux de données sur les vulnérabilités qui intègre plusieurs sources, notamment la base de données sur les vulnérabilités du National Institute of Standards and Technology (NIST) et des mises à jour propres au fournisseur.

Cisco Secure Workload vous aide à identifier rapidement les charges de travail vulnérables, ce qui permet de provisionner une politique dynamique pour protéger ces machines vulnérables contre les exploits ou d'appliquer une politique de quarantaine efficace jusqu'à ce que les correctifs nécessaires soient appliqués.

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Figure 9.
Renseignements détaillés sur la détection des vulnérabilités logicielles et l'exposition

Tableau de bord de sécurité composite pour des renseignements exploitables

Il est essentiel que les équipes chargées des opérations de sécurité comprennent à la fois leur posture de sécurité dans son ensemble et les éléments individuels qui contribuent à la posture actuelle. Cela fournit des données exploitables pour renforcer et corriger l'environnement contre une violation potentielle.

Le tableau de bord de sécurité de Cisco Secure Workload **vous fournit une note de sécurité composite** basée sur ce qui suit :

- Vulnérabilités associées à vos progiciels.
- Cohérence du hachage des processus et comportement des processus.
- Évaluation de la surface d'attaque de la charge de travail.
- Conformité de la politique de segmentation.

Le tableau de bord vous aide également à identifier les domaines d'amélioration en fournissant la ventilation du score pour chacun de ces éléments.

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Figure 10.
Tableau de bord de sécurité avec une note de sécurité composite

Création de rapports pour le dépannage et la maintenance

Cisco Secure Workload offre également des rapports personnalisés pour différents profils, tels que CxO, NetOps et SecOps. Chaque rapport comprend un survol général des mesures clés suivantes :

- **Présentation :** résumé rapide de l'utilisation des licences et de la posture de sécurité.
- **Opérations :** le dépannage et la maintenance se font en toute transparence grâce à la télémétrie, aux grappes et à la segmentation.
- **Conformité :** le CVE est séparé pour l'espace de travail et le cadre MITRE ATTACK.

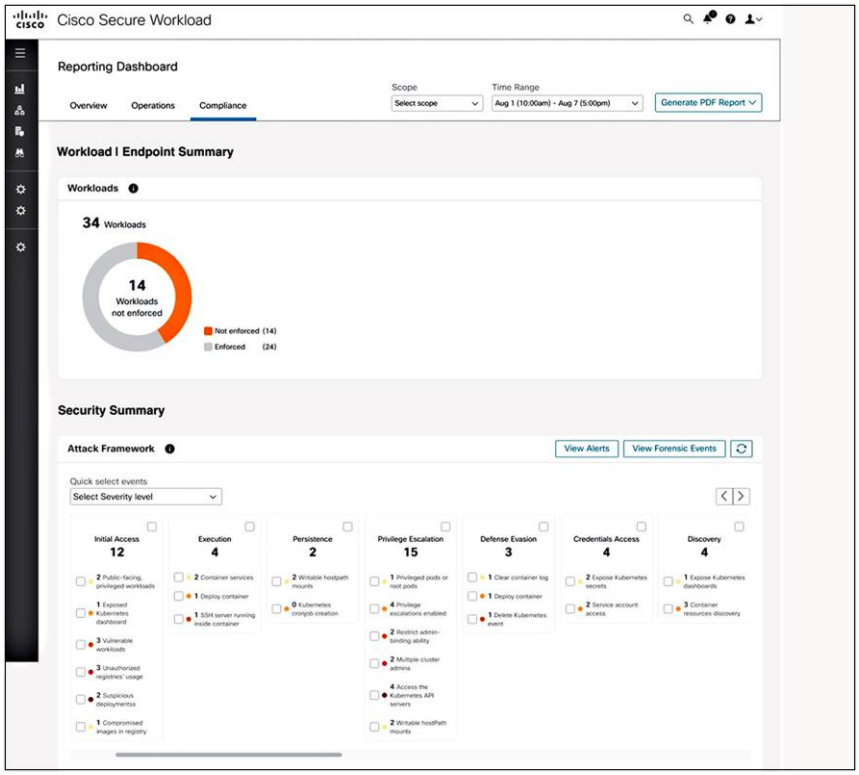

Figure 11.
Tableau de bord de rapport basé sur le cadre MITRE ATT&CK

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Fonctionnalités et avantages

Le tableau 1 présente les principales caractéristiques des fonctionnalités de protection de Cisco Secure Workload et leurs avantages.

Tableau 1. Principales caractéristiques et avantages

Fonctionnalité	Avantage
Modèle Zero Trust utilisant la microsegmentation	• Concrétisez la mise en œuvre de la microsegmentation dans votre environnement. • L'approche automatisée de Cisco Secure Workload contribue à accélérer le déploiement de la microsegmentation. • Sécurisez les charges de travail multinuages hybrides et limitez le mouvement latéral grâce à la microsegmentation.
Élargissement des définitions de politiques en fonction du contexte supplémentaire	• Éliminez les opérations fastidieuses de création manuelle de listes de ressources pour segmenter les applications. • Définissez des politiques par défaut et absolues de microsegmentation à l'aide d'étiquettes de métadonnées (annotations). • Élaborez rapidement des politiques cohérentes pour les applications à l'aide d'annotations en temps réel : ◦ Associez le contexte opérationnel riche aux serveurs. ◦ Définissez des politiques basées sur les utilisateurs et les groupes d'utilisateurs qui ont besoin d'un accès.
Détection des événements de non-conformité des politiques	• Suivez la conformité des politiques des applications en temps réel. • Activez des alertes pour les événements de conformité qui peuvent ensuite être intégrées aux systèmes de gestion des incidents et des événements de sécurité (Security Incident & Event Management ou SIEM) à des fins d'enquête et de correction.
Suivi des vulnérabilités logicielles	• Obtenez un inventaire des logiciels de référence et les renseignements sur la version installée sur les serveurs. • Déterminez rapidement si l'une des versions du progiciel comporte des vulnérabilités ou des expositions connues, ainsi que la gravité. • Obtenez un inventaire précis de tous les serveurs sur lesquels le progiciel est vulnérable. • Associez ces renseignements à une politique qui désigne une action spécifique, telle que la mise en quarantaine d'un serveur spécifique.
Détection des anomalies de charge de travail basée sur le comportement	• Définissez une référence pour le comportement ou les charges de travail en fonction des activités et processus de communication sur les charges de travail. • Détectez de manière proactive les comportements anormaux et identifiez les indicateurs de compromission. • Activez des alertes pour ces événements afin de les intégrer à vos systèmes SIEM pour une gestion supplémentaire des incidents de sécurité.
Contexte riche pour les utilisateurs et les terminaux	• Intégrez Cisco[MD] Identity Services Engine (ISE) et Cisco AnyConnect[MD] pour obtenir le contexte de l'utilisateur, la posture des terminaux et d'autres renseignements sur les terminaux. • Définissez des politiques pour sécuriser vos applications et vos charges de travail contre les terminaux ou les renseignements utilisateur compromis.

Renseignements détaillés sur la plateforme Cisco Secure Workload

Vous trouverez de plus amples renseignements concernant les options de déploiement, l'évolutivité prise en charge, les systèmes d'exploitation pris en charge, les licences et les renseignements sur les commandes dans la fiche technique de la plateforme : https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html.

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Conditions de licence du logiciel Cisco Secure Workload

Déploiement de Cisco Secure Workload SaaS :

L'abonnement à des logiciels-services (SaaS) est régi par la Description de l'offre Cisco Secure Workload SaaS https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco_tetration_saas_offer_description.pdf et le Contrat Cisco Universal Cloud accessible à l'adresse https://www.cisco.com/go/uca (ou des conditions semblables existant entre Cisco et vous) (le « Contrat »), et tout logiciel que vous installez est concédé sous licence en vertu des Conditions générales de Cisco, accessibles à l'adresse https://www.cisco.com/go/eula.

Modèles de déploiement sur site :

En plus d'être assujetti aux Conditions générales de Cisco (voir https://www.cisco.com/go/eula), le logiciel Cisco Secure Workload est assujetti aux Conditions générales de Cisco. Voir : https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/cisco-secure-workload.pdf .

Profitez de l'expertise de Cisco pour accélérer l'adoption

Cisco fournit des services professionnels et de soutien, allant des conseils, de la mise en œuvre et de l'optimisation au soutien continu de solutions, pour aider les entreprises à tirer le meilleur parti de la plateforme Cisco Secure Workload. Les experts des services Cisco vous aident à intégrer la plateforme dans votre environnement de production du centre de données, à définir les cas d'utilisation adaptés à vos objectifs commerciaux, à configurer l'apprentissage automatique et à valider les politiques et la conformité pour améliorer les performances applicatives et les performances de fonctionnement. Le service d'assistance pour la solution Cisco Secure Workload offre une assistance matérielle, logicielle et pour l'ensemble de la solution.

Nous proposons une sélection de services personnalisés à prix fixe et à étendue fixe pour Cisco Secure Workload qui vous garantissent une rentabilisation accélérée des investissements, l'adoption exhaustive dans votre environnement, des politiques et des performances applicatives optimisées, ainsi que l'assistance pour l'ensemble de la solution.

Durabilité de l'environnement Cisco

Des renseignements sur les politiques et les initiatives de Cisco en matière de durabilité environnementale pour nos produits, nos solutions, nos activités et nos activités étendues ou notre chaîne d'approvisionnement sont fournis dans la section « Durabilité de l'environnement » du rapport sur la responsabilité sociale d'entreprise de Cisco (CSR).

Les liens de référence vers des renseignements sur les principaux sujets de durabilité environnementale (mentionnés dans la section « Durabilité de l'environnement » du Rapport RSE) sont fournis dans le tableau suivant :

Sujet concernant la durabilité	Numéro de référence
Renseignements sur les lois et règlements sur le contenu des produits	Matériel
Renseignements sur les règlements concernant les déchets électroniques, notamment les produits, les batteries et les emballages	Conformité

Cisco rend les données relatives à l'emballage accessibles à titre informatif seulement. Il se peut qu'ils ne reflètent pas la situation juridique actuelle. Par conséquent, Cisco n'en garantit pas l'exhaustivité, l'exactitude ou la mise à jour. Les informations sont modifiables sans préavis.

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Cisco Capital

Des solutions de paiement flexibles pour vous aider à atteindre vos objectifs

Cisco Capital facilite l'obtention des bonnes technologies pour atteindre vos objectifs, favorise la transformation de votre entreprise et vous aide à rester compétitif. Nous pouvons vous aider à réduire le coût total des droits de propriété, à économiser sur le capital et à accélérer la croissance. Dans plus de 100 pays, nos solutions de paiement flexibles peuvent vous aider à acquérir du matériel, des logiciels, des services et des équipements tiers complémentaires au moyen de paiements simples et prévisibles. Pour en savoir plus.

Pour en savoir plus

Pour plus de renseignements sur la plateforme Cisco Secure Workload, consultez la page https://www.cisco.com/site/us/en/products/security/secure-workload/index.html ou communiquez avec votre représentant de compte Cisco local.

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**.

Cisco et le logo Cisco sont des marques de commerce ou des marques de commerce déposées de Cisco ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques de commerce Cisco, rendez-vous à l'adresse URL suivante : https://www.cisco.com/go/trademarks. Les autres marques de commerce mentionnées appartiennent à leurs détenteurs respectifs. L'utilisation du terme « partenaire » ne signifie pas nécessairement qu'il existe un partenariat entre Cisco et une autre entreprise. (1110R)

Imprimé aux États-Unis C78-740328-11 08/23

© 2023, Cisco et/ou ses sociétés affiliées. Tous droits réservés.