Protection des charges de travail dans le Cloud

Comment protéger les charges de travail dans les Clouds hybrides

vmware®

Table des matières

Synthèse

Le Cloud hybride se trouve au cœur de la transformation digitale. Aujourd'hui, plus de 90 % des entreprises déclarent suivre une stratégie multicloud. La plupart d'entre elles associent un Cloud public à un Cloud privé.[1] La bonne nouvelle, c'est que cette approche offre la flexibilité et la scalabilité nécessaires pour favoriser des innovations rapides. La mauvaise nouvelle, c'est que cette stratégie est synonyme de complexité et de risques accrus : la sécurité constitue donc un composant essentiel des Clouds privés et publics.

Quand les équipes d'une entreprise déploient et gèrent des charges de travail stratégiques dans des environnements multiclouds, avoir une visibilité sur la stratégie sécuritaire des charges de travail et un contrôle sur la surface d'attaque est crucial pour la protection des données et le maintien des opérations.

Plusieurs équipes de l'entreprise, y compris les équipes responsables des opérations informatiques (IT Ops) et des opérations de sécurité (SecOps), jouent un rôle clé en matière de performances, de disponibilité et de sécurité des charges de travail Cloud. S'assurer que les membres de ces équipes sont alignés, plutôt que fragmentés, constitue également un facteur de réussite essentiel.

Dans ce livre blanc, nous aborderons les principales difficultés auxquelles les équipes sont confrontées dans les entreprises pour sécuriser les charges de travail Cloud, et comment les surmonter en s'appuyant sur l'approche intrinsèque de la sécurité de VMware, avec VMware Carbon Black Cloud™, VMware vSphere® et VMware NSX®. Dans ce livre blanc, nous discuterons également de la nécessité de repenser les risques dans le Cloud : une nouvelle façon d'aborder les choses qui permettra de rassembler les parties prenantes de toutes les équipes, et ainsi de réduire la fracture numérique. Une liste de contrôle d'évaluation de la plate-forme de protection des charges de travail dans le Cloud est également fournie pour aider les entreprises à examiner les éléments à prendre en compte dans le choix d'une solution.

Problématiques de sécurité dans les Clouds privés, publics et hybrides

Le déploiement et la gestion des charges de travail et des applications dans les Clouds privés, publics et hybrides sont un travail d'équipe. Ce que nous avions l'habitude de considérer comme des opérations informatiques traditionnelles a été remplacé par des opérations collectives. Les équipes IT Ops, DevOps et SecOps unissent désormais leurs forces pour distribuer et protéger les applications et services Cloud.

[1] Rapport 2020 sur l'état du Cloud par Flexera, avril 2020.

Comme le montre le Tableau 1, l'absence de coordination entre les équipes et de prise en compte des aspects spécifiques des charges de travail Cloud peut accroître les risques.

	OPÉRATIONS DE CLOUD HYBRIDE	DÉFIS LIÉS À LA SÉCURITÉ	OPÉRATIONS INFORMATIQUES TRADITIONNELLES	LACUNES DANS LA SÉCURITÉ INFORMATIQUE TRADITIONNELLE
Architecture de conception	Services interconnectés	• Aucune visibilité sur la communication et la connexion des charges de travail • Des réseaux sans hiérarchie et non segmentés augmentent les risques	Monolithiques et isolées	• Antivirus (AV) traditionnel non adapté à un contexte de charges de travail Cloud • Une surveillance centrée sur les Data Centers ne permet pas d'identifier le comportement habituel du réseau
Modèle opérationnel	Propriété et gestion distribuées	• L'équipe IT Ops est chargée de la stratégie, de la gestion et de la disponibilité des charges de travail, mais elle ne voit pas les vulnérabilités qui s'y trouvent • Le cloisonnement en silos des technologies et des processus contribue à des configurations incorrectes, à des configurations non sécurisées et à d'autres erreurs humaines	Centralisées	• L'addition de produits de sécurité ponctuels requiert l'installation d'agents supplémentaires, ce qui ralentit les performances du système et complique les opérations • L'absence de visibilité unifiée au sein des charges de travail, entre elles et dans les Clouds, complique la coordination entre les équipes
Scalabilité	Hautement dynamiques, automatiques	• L'absence de contrôle des modifications entraîne des configurations incorrectes, comme un stockage des données non sécurisé, des autorisations excessives, des informations d'authentification et des paramètres de configuration par défaut, et la désactivation des contrôles de sécurité • L'impossibilité de normaliser les règles de sécurité des charges de travail sur les Clouds privés et publics accroît les risques	Statiques, manuelles	• Les analyses traditionnelles ne sont pas conçues pour détecter la plupart des configurations incorrectes du Cloud (il s'agit de la principale cause de violations de données dans le Cloud)[2] • Le déploiement de solutions de sécurité ponctuelles pour chaque environnement de Cloud complique la gestion de la gouvernance et des règles à grande échelle

TABLEAU 1 : Les défis liés à la sécurité des charges de travail dans le Cloud hybride naissent de l'incapacité à reconnaître les différences clés entre le Cloud Computing et l'informatique traditionnelle

2. Cloud Security Alliance. « Top Threats to Cloud Computing: Egregious Eleven Deep Dive. » Septembre 2020.

Les équipes IT Ops, DevOps et SecOps sont toutes chargées de maintenir la sécurité et la disponibilité des charges de travail stratégiques dans le Cloud.

Trois étapes de redéfinition des risques

Pour tirer le meilleur parti de la transformation digitale, il faut accepter le changement de paradigme qu'elle représente. Les anciens modèles de gestion des risques ne s'appliquent plus lorsque le changement est une constante et que les intervenants sont si nombreux.

Pour sécuriser les charges de travail Cloud, voici ce que les équipes des entreprises devraient faire :

1. Augmenter la visibilité : identifier les risques inconnus ou non détectés dans les charges de travail.
2. Accélérer la récupération : accélérer la reprise en développant une résilience dans les charges de travail Cloud.
3. Simplifier la sécurité : unifier la réduction des risques sur les charges de travail, les terminaux et les conteneurs.

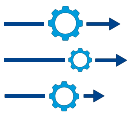
Étape nº 1 : Augmenter la visibilité : identifier les risques inconnus ou non détectés dans les charges de travail

- **Pourquoi c'est problématique** : vous ne pouvez pas gérer des risques si vous ne savez pas qu'ils existent. Malheureusement, la plupart des administrateurs de machines virtuelles (VM) manquent de visibilité sur les vulnérabilités potentielles des applications et charges de travail s'exécutant sur leurs VM. Un cybercriminel n'a besoin d'identifier et d'exploiter qu'une seule vulnérabilité pour obtenir un accès non autorisé, alors que les personnes chargées de leur protection doivent connaître toutes les failles exploitables pour pouvoir les combler. En outre, une fois les vulnérabilités identifiées, il n'est pas toujours simple pour les équipes IT Ops et SecOps de se mettre d'accord sur la priorité des corrections, leur motif et le moment où elles devraient être appliquées.
- **Exemple** : Joe est un ingénieur de la fiabilité du site (SRE) d'une grande entreprise de services de santé. Il est chargé de gérer son infrastructure de Cloud privé, qui comprend des serveurs, des charges de travail et des applications qui traitent des données médicales sensibles. Joe sait qu'il doit identifier et éliminer toutes les vulnérabilités pouvant avoir un impact sur la conformité ou exposer les données des patients. En outre, les performances et la disponibilité des services sont des priorités pour Joe et les autres SRE de son équipe. En effet, les soins dispensés aux patients sont essentiels.

  Actuellement, Joe compte sur Sarah, analyste en sécurité, pour le prévenir lorsqu'une analyse planifiée détecte une vulnérabilité de haute gravité devant être éliminée. Ils sont souvent en désaccord sur la marche à suivre, car chacun utilise son propre jeu d'outils. Sans système d'enregistrement en commun, il est bien compliqué de se mettre d'accord sur la résolution de ces problèmes critiques : quelles vulnérabilités sont les plus urgentes, les contrôles compensatoires sont-ils suffisants, quelle est la cible des cybercriminels et comment comptent-ils l'atteindre ?
- **Ce qu'il faut : Détection des risques entre plusieurs domaines** : détecter tous les risques associés aux charges de travail Cloud, en prenant en compte tous les angles et vecteurs d'attaque, et utiliser un système d'enregistrement commun pour les gérer. Si aucun correctif ne peut être appliqué en raison d'un risque d'interruption de service, se mettre d'accord sur un contrôle compensatoire, ou définir une liste de surveillance qui permettra de détecter le moment où une vulnérabilité sera ciblée.

Étape nº 2 : Accélérer la récupération : accélérer la reprise en développant une résilience dans les charges de travail Cloud

- **Pourquoi c'est problématique** : Pour la plupart des entreprises, il ne s'agit plus de savoir si des violations de données sont à prévoir, mais quand elles surviendront. En cas de violation, il est essentiel de connaître l'étendue de l'exposition pour prévenir des épidémies similaires dans le futur. De plus, ces informations sont fondamentales pour une récupération rapide et complète. La difficulté provient de la hiérarchisation des priorités. La priorité des équipes DevOps et IT Ops est de restaurer les services aussi rapidement que possible, même si cela implique la destruction des preuves et objets dont l'équipe SecOps a besoin pour identifier la source et la portée de l'attaque, et enquêter dessus.
- **Exemple** : Récupérer d'une attaque par rançongiciel dans votre environnement de Cloud peut être coûteux, compliqué et nécessiter beaucoup de main-d'œuvre. Ces épidémies peuvent migrer des charges de travail vers les serveurs qui les hébergent et se retrouver sur les terminaux que les collaborateurs utilisent pour



accéder à ces charges de travail. L'objectif est de réduire la surface d'attaque du rançongiciel en le tuant dans l'œuf, au moment de l'exécution du code dans la charge de travail elle-même, avant que le jeu d'outils ne soit entièrement déployé ou que les connexions de commande et de contrôle (C2) ne soient établies pour exfiltrer ou chiffrer les données qui feront l'objet de la demande de rançon.

- **Ce qu'il faut : Résilience contre les risques** : La restauration rapide des services après une violation ou une attaque de logiciel malveillant, et la rétention des données nécessaires aux enquêtes judiciaires sont possibles dans le Cloud avec la plate-forme de protection des charges de travail adaptée. De fait, combler ce fossé constitue l'un des objectifs principaux du développement d'une résilience contre les risques dans vos charges de travail Cloud. Gérer la sécurité des charges de travail et des terminaux à partir d'une même plate-forme permet aux équipes d'identifier les risques au niveau de tous ces points de contrôle et de suivre une stratégie de récupération plus résiliente.

Étape nº 3 : Simplifier la sécurité : unifier la réduction des risques sur les charges de travail, les terminaux et les conteneurs

- **Pourquoi c'est problématique** : Gérer les risques dans les charges de travail Cloud à l'aide de solutions ponctuelles traditionnelles implique l'utilisation de processus en couloir qui représentent des surcharges opérationnelles et compliquent les risques. Avec l'utilisation de plusieurs outils de sécurité : en fonction du fournisseur de Cloud public, du système d'exploitation hôte ou du type de Cloud (privé ou public), il est très difficile de suivre une stratégie de réduction des risques cohérente. En effet, en l'absence de source unique et fiable sur la sécurité, les équipes ne peuvent pas se mettre d'accord sur la prévention des épidémies de logiciels malveillants, la recherche et la correction de configurations incorrectes ou le confinement des menaces à évolution rapide.
- **Exemple** : Pour optimiser la résilience opérationnelle, certaines équipes IT Ops choisissent d'avoir recours à plusieurs fournisseurs de Cloud ou d'utiliser des infrastructures de Clouds à la fois publics et privés. Sans règles de sécurité réellement indépendantes de ces environnements, les équipes sont confrontées à une mosaïque de contrôles ou sont obligées de se cantonner à un fournisseur de services Cloud ou à une architecture de Cloud (privé ou public).
- **Ce qu'il faut : Une sécurité unifiée** : L'objectif est de déployer une sécurité unifiée adaptée au Cloud et appliquée uniformément, indépendamment de l'emplacement de la charge de travail (Cloud public ou privé). L'utilisation d'une seule solution de gestion du cycle de vie pour l'ensemble des Clouds, charges de travail et conteneurs permet d'appliquer des règles de sécurité et une stratégie de réduction des risques cohérentes et étendues. Par exemple, l'utilisation d'une plate-forme unique pour la gestion des vulnérabilités, l'audit et la correction, et la détection et réponse des terminaux (EDR) simplifie la sécurité des charges de travail et favorise la collaboration entre les équipes IT Ops, SecOps et DevOps.

Sécurité intrinsèque pour les charges de travail Cloud

Comme indiqué dans ce livre blanc, l'utilisation de technologies hétérogènes pour gérer les charges de travail dans le Cloud complique les risques et cette solution n'est tout simplement pas scalable. Parallèlement, il est essentiel de permettre aux équipes IT Ops, DevOps et SecOps d'utiliser leur console de prédilection. Cela ne signifie pas que la migration vers le Cloud nécessite l'adoption d'un processus entièrement nouveau, d'une nouvelle interface utilisateur ou d'une nouvelle console de gestion. En effet, ces équipes ont déjà suffisamment d'autres choses à gérer.

Avec l'approche intrinsèque de la sécurité VMware, une surveillance et des analyses comportementales approfondies sont implémentées à chaque point de contrôle : Cloud, charge de travail, terminal, réseau et identité, puis elles sont unifiées pour une reconnaissance contextuelle complète. Telle une caméra qui enregistre les mouvements détectés à chaque point de contrôle, la sécurité intrinsèque permet de bénéficier d'une reconnaissance contextuelle exhaustive. Puisqu'il est inutile de rassembler manuellement les données de télémétrie de plusieurs points de contrôle, les équipes peuvent rapidement pister les menaces dès leur point d'entrée, et à chaque étape.

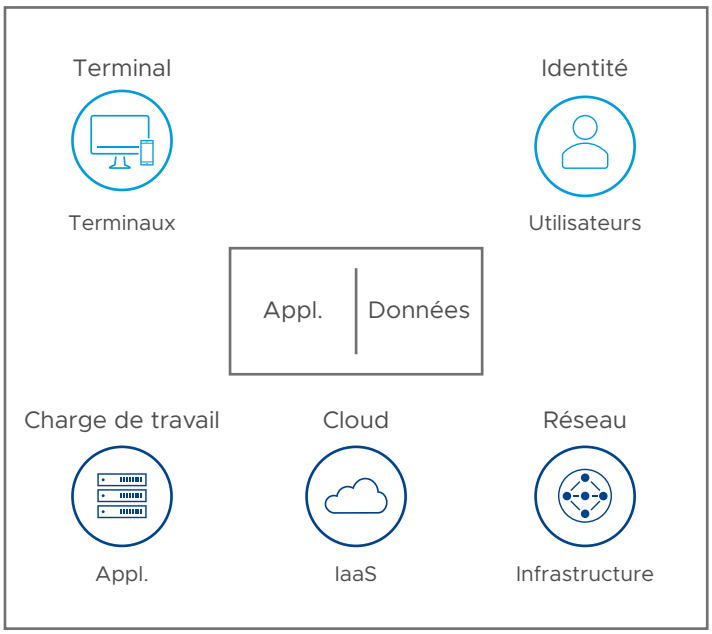


FIGURE 1 : Les cinq points de contrôle d'une sécurité intrinsèque.

Protection scalable des charges de travail dans le Cloud

VMware Carbon Black Cloud fournit toutes les fonctionnalités nécessaires à une protection scalable des charges de travail dans le Cloud, et s'intègre avec vSphere et NSX de manière native. De par cette intégration étroite, les administrateurs vSphere et NSX peuvent accéder à toutes les données pertinentes sur les menaces dans le contexte de leurs domaines respectifs et à partir de la même console, optimisée pour leur rôle.

En plus de la reconnaissance contextuelle complète dans les Clouds, les charges de travail, les terminaux, les réseaux et l'identité et entre ces derniers, VMware Carbon Black Cloud fournit le système d'enregistrement commun nécessaire aux équipes IT Ops, DevOps et SecOps pour prévenir, détecter et corriger les menaces ayant un impact sur leurs applications et charges de travail stratégiques.

Voici les principaux composants de la sécurité intrinsèque :

- VMware Carbon Black Cloud
- VMware vSphere
- VMware NSX

VMware Carbon Black Cloud

VMware Carbon Black Cloud est une plate-forme native Cloud de protection des charges de travail dans le Cloud qui allie l'intelligence avancée du système à la prévention comportementale nécessaires pour écarter les nouvelles menaces grâce à une seule solution de gestion du cycle de vie et à une console simple d'utilisation.

VMware vSphere

vSphere est la première plate-forme de virtualisation informatique. Elle a été restructurée pour exécuter *Kubernetes* en natif afin que les clients puissent moderniser leurs charges de travail s'exécutant sur vSphere.

VMware NSX Advanced Threat Prevention™

Reposant sur l'autoapprentissage, VMware NSX Service-defined Firewall™ assure l'analyse du trafic réseau, la détection et la prévention des intrusions, ainsi que l'analyse avancée des logiciels malveillants grâce à des fonctionnalités complètes de détection et de réponse réseau.

Protection des charges de travail dans VMware Cloud : Fonctionnement

Avec l'approche intrinsèque de la sécurité VMware, les entreprises peuvent protéger leurs charges de travail Cloud en utilisant une infrastructure existante pour identifier les risques de manière proactive, empêcher l'exploitation des vulnérabilités et les expositions, détecter les menaces nouvelles et émergentes, et y répondre rapidement.

Ce processus en trois étapes fonctionne de la manière suivante, et s'appuie sur des contrôles de sécurité essentiels.

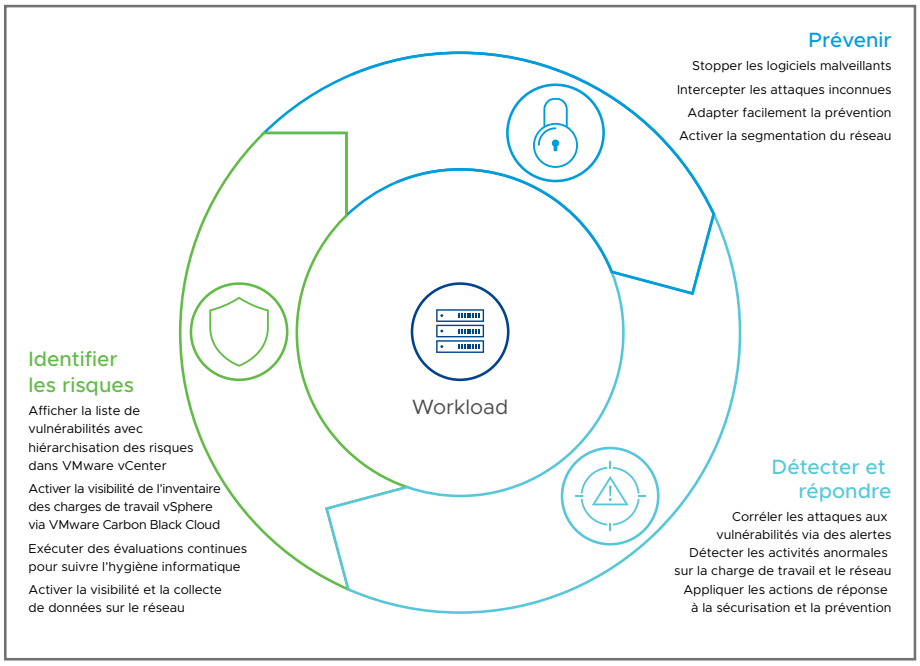


FIGURE 2 : Une approche intrinsèque de la sécurité des charges de travail Cloud offre une protection complète aux charges de travail vSphere.

Étape nº 1 : Identifier les risques

- **Vérification de l'intégrité initiale** : VMware Carbon Black Cloud exécute une vérification initiale de l'intégrité pour vérifier que le système sur lequel la charge de travail s'apprête à être installée est propre, conforme et adapté à ce type de charge de travail. Il collecte et analyse également les niveaux de correctifs du système d'exploitation, évalue les vulnérabilités et les configurations incorrectes, et détermine si une sécurisation supplémentaire est justifiée.
- **Visibilité continue sur l'état du système** : VMware Carbon Black Cloud identifie les dérives de configuration, la présence d'applications inconnues ou non autorisées, les vulnérabilités et d'autres activités dynamiques qui augmentent la surface d'attaque de l'environnement. Par exemple :
  - Il surveille les modifications indiquant une activité malveillante (la mise à zéro des mots de passe ou les modifications dans la configuration de BitLocker par exemple).
  - Il effectue l'audit et la correction pour la requête de 1 500 objets pour chaque charge de travail et terminal dans les Clouds privés et publics.
  - Il permet aux administrateurs d'exécuter des requêtes SQL pour rechercher des activités ou comportements malveillants spécifiques.
- **Visibilité continue sur les vulnérabilités et l'activité du réseau** : VMware Carbon Black Cloud permet aux administrateurs vSphere d'afficher les vulnérabilités des charges de travail avec hiérarchisation des risques dans VMware vCenter® et d'effectuer régulièrement des évaluations de vulnérabilité sans analyse sur les charges de travail. NSX propose un pare-feu distribué intégré, permettant aux équipes IT Ops de surveiller la communication des charges de travail dans les Clouds privés et publics, de détecter les charges de travail faisant partie d'une application et de déterminer comment segmenter les charges de travail non connexes.

Étape nº 2 : Empêcher l'aggravation des risques

- **Empêcher l'exploitation des vulnérabilités sur la charge de travail** : VMware Carbon Black Cloud fournit un antivirus nouvelle génération (NGAV) offrant une protection allant au-delà des indicateurs ponctuels de logiciels malveillants, rançongiciels, menaces zero-day, variantes à évolution rapide, fichiers suspects et processus potentiellement indésirables propres aux charges de travail dans les Clouds privés et publics. La plate-forme VMware allie des leurres contre les rançongiciels, l'analyse dynamique et l'autoapprentissage pour une analyse en continu qui empêche l'exécution des fichiers suspects.
- **Empêcher les attaques non-malveillantes** : en plus de bloquer les attaques de logiciels malveillants, VMware Carbon Black Cloud protège l'environnement contre les attaques persistantes les plus récentes de logiciels malveillants sans fichier, basées sur la mémoire et LotL (living-off-the-land). Ces attaques pernicieuses s'appuient sur des logiciels existants et des applications figurant dans la liste autorisée (comme PowerShell), ainsi que des protocoles autorisés, pour mener des activités malveillantes. Contrairement aux approches legacy qui reposent uniquement sur les menaces connues, la plate-forme VMware est capable d'identifier les nouvelles variantes et les exploitations zero-day en recoupant les comportements liés.
- **Empêcher les attaques réseau** : NSX Service-defined Firewall protège les charges de travail en limitant le mouvement latéral et en bloquant les exploitations entrantes d'applications et de services vulnérables. Avec ce niveau de visibilité, vous pouvez comprendre comment les attaques LotL se déplacent sur le réseau, identifier les indicateurs de compromission (IOC) et verrouiller ces connexions réseau pour isoler les charges de travail pour les tenir hors de portée des cybercriminels.
- **Personnaliser la prévention** : à chaque environnement sont associées différentes contraintes opérationnelles, souvent concurrentes. VMware permet à nos clients d'équilibrer les risques de sécurité et opérationnels avec une granularité très précise. Avec le moteur de règles VMware, vous pouvez choisir comment réduire les menaces en fonction du type de charge de travail spécifique, de sa fonction, de son degré stratégique et de son adjacence avec d'autres charges de travail. Par exemple, pour isoler une charge de travail stratégique, un administrateur système peut empêcher PowerShell de fouiller la mémoire d'un autre processus ou d'invoquer une application non sécurisée.

Étape nº 3 : Détecter les risques en cours et y répondre

- **Savoir où et quand commencer une enquête (zoom avant)** - Utilisez la fonction de détection automatique des menaces prête à l'emploi de VMware via l'analyse intelligente des menaces mise à jour de VMware Threat Analysis Unit™ pour détecter les systèmes affectés et les isoler pour correction. Les API VMware vous permettent d'intégrer vos propres listes de surveillance et flux tiers, et de consulter et partager des informations collaboratives sur les menaces dans le système robuste d'échange entre les utilisateurs de VMware.
- **Connaître la portée et le laps de temps de l'attaque (zoom arrière)** - La plate-forme VMware permet aux enquêteurs de revenir sur les événements pour comprendre le déroulement d'une attaque, déterminer les systèmes affectés et connaître la progression de l'attaque dans le temps. VMware capture toutes les données (par exemple l'activité des processus, les interactions entre processus, les relations entre les processus parent-enfant, etc.), et crée une chronologie détaillée sans aucun angle mort, après coup. Ainsi, cela permet aux équipes chargées de la réponse aux incidents et des enquêtes de connaître tous les faits.
- **Workflow rapide de détection préventive** - En trois étapes simples, VMware Carbon Black Cloud vous permet de transformer la détection des menaces en règles de prévention standard sur toutes vos charges de travail. Commencez par appliquer des règles automatisées, personnalisées pour vos charges de travail en fonction des détections précédentes. Affichez ensuite un aperçu des effets qu'auront les règles de prévention avant leur implémentation. Puis d'un simple clic, déployez les règles mises à jour sur les charges de travail de tous les environnements.

La protection des charges de travail Cloud contre une multitude de menaces demande une approche à plusieurs volets : avec une visibilité à la fois granulaire et unifiée sur tous les aspects de l'environnement informatique. Les équipes IT Ops, DevOps et SecOps doivent collaborer et se charger ensemble de sécuriser les charges de travail stratégiques dans le Cloud. Les entreprises qui tentent d'adopter des approches traditionnelles pour sécuriser les Clouds hybrides rencontrent de nombreux défis, notamment un manque de visibilité sur les relations entre les charges de travail, les processus fragmentés et les configurations incorrectes. Comme indiqué dans ce livre blanc, augmenter la visibilité, accélérer la récupération et simplifier la sécurité sont trois stratégies essentielles que les équipes des entreprises doivent mettre en œuvre pour réduire les risques.

VMware occupe une place unique sur le marché pour la protection des charges de travail dans les Clouds hybrides. Pour être plus précis, les solutions VMware permettent aux équipes d'identifier exactement les risques émergents au niveau des charges de travail, d'empêcher ces risques de s'aggraver, et de contenir rapidement les épidémies sans interrompre les opérations. Alors que d'autres produits de sécurité des terminaux et des charges de travail se contentent de collecter un ensemble de données sur les acteurs malveillants connus, VMware Carbon Black Cloud collecte en continu des données exhaustives sur les charges de travail, les terminaux et le réseau, et analyse les schémas comportementaux des cybercriminels pour bloquer les attaques de manière proactivce, avant qu'elles n'aient un impact. Ce niveau de visibilité accrue sur les opérations simplifie la sécurité et accélère la récupération du système.

Les fournisseurs de solutions de protection des charges de travail dans le Cloud sont légion sur le marché, mais toutes ne se valent pas. Les entreprises doivent prendre en compte quelques exigences clés, comme l'architecture de conception, les modèles opérationnels et la scalabilité, et se poser les bonnes questions pour déterminer si la plate-forme est adaptée à leurs besoins. Utilisez la liste de contrôle du Tableau 2 pour choisir la plate-forme de protection des charges de travail dans le Cloud adaptée. Il y a 100 points à attribuer. Affectez des points à chaque question clé en fonction de sa véracité pour votre entreprise. La valeur totale de la colonne valeur pondérée doit être égale à 100. En renseignant cette liste de contrôle, vous aurez une meilleure idée de vos priorités et des éléments clés à prendre en compte.

Liste de contrôle d'évaluation de la plate-forme de protection des charges de travail dans le Cloud

	EXIGENCE CLÉ	QUESTIONS CLÉS	VALEUR PONDÉRÉE
Architecture de conception	Expliquer comment la plate-forme de protection des charges de travail dans le Cloud permet de visualiser les communications et les connexions entre les charges de travail.	Peut-elle consolider les données de télémétrie de l'ensemble des Clouds, charges de travail, réseaux et terminaux ?	
		Prend-elle en charge toutes les applications indépendamment de la configuration du système d'exploitation et du Cloud, ou dépend-elle de l'un de ces éléments ?	
		Peut-elle reconnaître ce qui constitue un comportement habituel au sein des charges de travail ou entre ces dernières ?	
		Quels modèles comportementaux déploie-t-elle pour détecter les attaques via des logiciels malveillants et des logiciels non malveillants (sans fichier) au sein des charges de travail et entre ces dernières ?	
Modèle opérationnel	Expliquer comment la plate-forme de protection des charges de travail dans le Cloud favorise un alignement et une coordination aisée entre les équipes IT Ops, DevOps et SecOps pour réduire les risques, simplifier la conformité et augmenter la résilience.	Combien d'agents faut-il installer sur chaque charge de travail, conteneur et système d'exploitation ?	
		Les équipes IT Ops, DevOps et SecOps peuvent-elles exploiter le même ensemble de données pour la surveillance et la réponse aux incidents ?	
		Quels cadres de gouvernance votre plate-forme prend-elle en charge (par exemple NIST 800-53) ?	
		Comment se déroule un workflow type dans les équipes IT Ops, DevOps et SecOps une fois qu'une menace, vulnérabilité ou configuration incorrecte a été identifiée ?	
Scalabilité	Expliquer comment la plate-forme de protection des charges de travail dans le Cloud utilise des programmes de contrôle des modifications sécurisés mais rapides pour améliorer la normalisation des règles de sécurité et réduire les risques de configuration incorrecte et d'autres erreurs humaines à grande échelle.	Quelle est la consommation CPU moyenne de l'agent de protection de chaque charge de travail dans le Cloud ?	
		Peut-elle consolider plusieurs fonctions de sécurité comme la détection et réponse des terminaux, l'antivirus nouvelle génération (NGAV) et la gestion des vulnérabilités dans un seul agent et une seule console de gestion ?	
		La plate-forme de protection des charges de travail dans le Cloud peut-elle appliquer des règles de sécurité standard cohérentes dans des environnements de Cloud privés, publics et hybrides et exécuter des rapports dessus ?	
		Comment fait-elle des analyses de vulnérabilités régulières sans affecter la disponibilité et les performances ?	

TABLEAU 2 : Liste de contrôle d'évaluation de la protection des charges de travail dans le Cloud

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Global Inc. Tour Franklin, 100-101 Quartier Boieldieu, 92042 Paris La Défense Cedex, France Tél. +33 1 47 62 79 00 www.vmware.com/fr