Partager la responsabilité de la sécurité des charges de travail

Mise en œuvre et simplification pour les équipes chargées de la sécurité et les administrateurs informatiques

vmware®

Table des matières

Introduction

Les équipes de sécurité ont besoin de l'aide des équipes chargées des opérations informatiques pour sécuriser les charges de travail

Les administrateurs informatiques et les équipes chargées de la sécurité jouent chacun un rôle dans la sécurisation des systèmes, mais de manière relativement indépendante. Mais la transition des applications et des charges de travail vers des environnements de Cloud modifie l'exécution de ces rôles.

Les équipes chargées de la sécurité d'une entreprise comptent généralement des groupes responsables des règles et des audits et des équipes de recherche de menaces et de réponse aux incidents. Les responsabilités quotidiennes en matière de sécurité et de conformité reviennent au personnel des opérations informatiques, et ces ressources ne sont pas toujours centrées sur la sécurité. En fait, selon un rapport Forrester Consulting Spotlight, seulement 33 % des entreprises ont une équipe unifiée chargée à la fois de la sécurité et des opérations informatiques, mais 47 % pensent que cette unification deviendra la norme d'ici trois à cinq ans[1]. C'est le moment idéal pour adopter une approche favorisant la cohésion entre ces équipes.

Dans ce livre blanc, nous allons découvrir les concepts clés permettant aux équipes informatiques et à celles chargées de la sécurité de réduire la surface d'attaque et de renforcer les ressources de manière proactive. L'adoption de ces concepts permettra de combler le fossé entre ces équipes, de simplifier les opérations et de partager la responsabilité de la sécurité des charges de travail.

CONCEPT CLÉ	DESCRIPTION
Réduire la surcharge d'agents	L'élimination de la nécessité d'installer des agents sur les charges de travail réduit la prolifération des agents de sécurité, les installations et les redémarrages, et la surcharge opérationnelle. Cela simplifie l'application d'une sécurité sous forme de service pour les équipes informatiques.
Partager la visibilité sur les vulnérabilités	Une vue unifiée des données de sécurité garantit une communication et une compréhension claires des vulnérabilités détectées.
Automatiser la hiérarchisation des risques	Pour réduire le phénomène de désensibilisation aux alertes et l'épuisement des ressources, les deux équipes doivent connaître les éléments qui auront le plus d'impact sur leurs mécanismes de défense. Il est essentiel de disposer d'un système centré sur le contexte capable de hiérarchiser automatiquement les vulnérabilités par ordre de priorité sans parti pris.
Simplifier les processus des charges de travail	Avec une visibilité et une hiérarchisation des risques partagées, les équipes informatiques et chargées de la sécurité peuvent travailler sans accroc grâce à l'automatisation et à la mise en œuvre systématiques d'une sécurité cohérente pour assurer l'hygiène informatique.

TABLEAU 1 : Quatre concepts clés permettant de réduire la surface d'attaque et de renforcer les ressources.

1. Forrester Consulting, à la demande de VMware. « Security As A Team Sport: A Spotlight On The Growing Role Of IT In Security Tasks. » Mai 2020.

Défi

Les charges de travail : une vulnérabilité pointée du doigt

Nos environnements deviennent plus diversifiés et plus complexes : les charges de travail sont donc de plus en plus distribuées. De nombreuses applications Cloud stratégiques sont vulnérables aux compromissions dès qu'un élément de la charge de travail (application, données ou système d'exploitation) subit un dysfonctionnement. Évidemment, il ne s'agit pas d'arrêter un serveur d'entreprise dès la survenue d'un incident. Les responsables de l'informatique et de la sécurité ne tiennent pas le premier rôle dans la productivité de l'entreprise. En d'autres termes, la sécurisation et la surveillance de chaque élément d'une charge de travail représentent désormais un aspect supplémentaire crucial de la protection de votre activité.

Qui est responsable de la sécurisation des charges de travail ?
Lorsque les charges de travail résidaient dans les serveurs rack statiques d'un Data Center on premise, il était plus simple d'en confier la sécurisation. Aujourd'hui, les charges de travail peuvent résider sur des serveurs physiques, des serveurs virtuels, dans le Cloud public ou même dans un environnement sans serveur. En outre, elles peuvent se déplacer entre tous ces environnements, ce qui complique leur suivi et leur gestion. Tout le monde a son rôle à jouer dans le cycle de vie des charges de travail : équipes responsables de la sécurité, administrateurs informatiques, administrateurs Cloud, administrateurs VMware vCenter®, ingénieurs de la fiabilité des sites, équipes DevOps et développeurs. Autant d'acteurs qui peuvent avoir un impact sur les charges de travail : parfois pour un objectif commun, parfois contradictoire.

Les administrateurs informatiques peuvent sécuriser les charges de travail efficacement. Mais ils n'ont pas de visibilité sur la plupart des vulnérabilités des charges de travail, et ils ne disposent certainement pas du contexte nécessaire pour donner la priorité à un objectif plutôt qu'un autre. Et parce que souvent, ils n'ont pas le contrôle de l'environnement de Cloud, les rôles et les responsabilités de chacun s'emmêlent. Les équipes responsables de la sécurité disposent d'une partie des informations nécessaires pour identifier les vulnérabilités, mais pas des informations requises pour hiérarchiser précisément les risques ou connaître le contexte, qui leur permettraient d'appliquer une correction efficace.

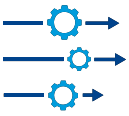
En d'autres termes, la gestion de la sécurité des charges de travail est insuffisante dans toutes les équipes.

La responsabilité de la sécurité peut-elle être partagée ?
Ce qu'il faut retenir, c'est qu'il incombe aussi bien aux équipes chargées de la sécurité et aux administrateurs informatiques de s'occuper de la sécurité des charges de travail. Mais pour éviter de rejeter la faute sur l'autre, ces équipes doivent être unifiées avec les processus, les informations et les outils propres à ces charges de travail.

Avec une vision et une méthodologie partagées pour automatiser la détection et la hiérarchisation des corrections, il devient bien plus facile pour les administrateurs informatiques de collaborer pour renforcer la sécurité et réduire les surfaces d'attaque. En effet, des dispositifs de sécurité peuvent être mis en œuvre sur les charges de travail pour éliminer toute tension et toute accusation entre ces deux équipes essentielles. Vous pouvez faire de cette idée une réalité en seulement quatre étapes clés.

DONNÉES CLÉS À PARTAGER ENTRE LES ÉQUIPES CHARGÉES DE LA SÉCURITÉ ET LES ADMINISTRATEURS INFORMATIQUES

- Indicateurs de compromission
- Tactiques, techniques et procédures
- Visibilité sur les attaques bloquées et détectées
- Événements ordinaires qui se produisent sur le système
- Évaluation de plus de 2 000 configurations de charges de travail
- Inventaire des charges de travail avec leur état de protection
- Contexte des vulnérabilités sans analyse avec scores de risque et liens vers la National Vulnerability Database
- Suivi et tendances de l'hygiène informatique dans le temps



Quatre étapes pour mettre en œuvre et simplifier la sécurité des charges de travail

Étape 1 : Réduire la surcharge d'agents

La prolifération d'agents de sécurité greffés entraîne nombre de problèmes à la fois pour les administrateurs informatiques et les équipes de sécurité. Voici les plus courants :

- Sources d'informations disparates entraînant une mauvaise communication
- Efforts de maintenance accrus et plus grande probabilité d'erreur
- Coûts supplémentaires en matière de stockage pour les données collectées

Pour résoudre ces problèmes, consolidez les piles informatiques et de sécurité en remplaçant les solutions ponctuelles par une approche globale de la sécurité : une approche permettant de recueillir les données sur l'ensemble des environnements on premise et Cloud.

Choisir un agent intégré unique

La solution idéale consiste à utiliser un seul agent dans la couche de virtualisation intégrée à votre infrastructure existante. Tous les événements nécessaires pour bénéficier d'une visibilité totale sur l'ensemble des environnements pourront alors être enregistrés. En ayant recours à un agent unique, l'empreinte de la surveillance des dispositifs de sécurité est quasi nulle.

Avantages d'un agent unique

La consolidation des solutions de sécurité dans un seul agent, une source de données complète unique, offre des avantages considérables pour l'amélioration de la sécurité des charges de travail :

- Simplifie la mise en œuvre de la gestion de l'agent pour le département informatique
- Permet l'intégration des workflows et le partage des données entre les équipes
- Fournit des informations contextuelles, pour des résultats exploitables plus facilement
- Élimine les analyses de vulnérabilités ponctuelles, ce qui améliore les performances et accélère le temps de réponse aux attaques
- Réduit les coûts de stockage et les efforts de maintenance

Étape 2 : Partager la visibilité sur les vulnérabilités

Le groupe chargé de l'application de correctifs est rarement le même que celui qui analyse l'impact des vulnérabilités sur la sécurité. Les données d'analyse classiques sont rapidement obsolètes, et les systèmes d'ouverture de tickets sont souvent lents, ce qui entraîne des disparités dans l'identification des correctifs nécessaires.

Les administrateurs informatiques s'appuient sur des sources de données distinctes de celles qu'utilisent les équipes chargées de la sécurité, mais qui doivent tout de même contribuer à la définition de processus de sécurité plus vastes. Les attentes ne sont pas alignées, et cela entraîne une mauvaise hygiène informatique.

Une vue unifiée des données de sécurité garantit une communication et une compréhension claires des vulnérabilités détectées et du niveau de risque associé.

Une vue unifiée réduit efficacement les risques

La consolidation des dispositifs dans un agent unique décrite à l'Étape 1 génère des données de sécurité pouvant être facilement partagées entre les administrateurs informatiques et les équipes chargées de la sécurité. Dans l'idéal, ces informations devraient être présentées dans les outils que ces équipes utilisent au quotidien, tels que des outils de virtualisation (VMware vSphere® et vCenter par exemple).

Disposer des mêmes données et des mêmes résultats d'évaluation améliore la communication et la collaboration entre les équipes. Ce qui importe, c'est de toujours avoir les données sur les vulnérabilités à portée plutôt que de s'appuyer sur des analyses ponctuelles. Ainsi, les équipes sont toujours sur la même longueur d'onde. Un inventaire commun des vulnérabilités des charges de travail classées par niveau de risque permet de garantir la mobilisation des ressources sur les problèmes les plus urgents.

Étape 3 : Automatiser la hiérarchisation des risques

Utiliser un agent unique et profiter d'une visibilité partagée sur les données liées à la sécurité constituent des étapes essentielles pour une gestion efficace de la sécurité des charges de travail. Toutefois, avoir accès aux vulnérabilités connues ne suffit pas à garantir un consensus sur la mobilisation des ressources.

Logiquement, l'étape suivante consiste à normaliser l'évaluation des risques. Envisagez d'adopter une solution de sécurité gérant automatiquement l'évaluation et la hiérarchisation des risques.

Données classées par niveau de risque dans les outils courants pour des résultats exploitables

Un système d'évaluation des risques basé uniquement sur le système commun de notation des vulnérabilités n'est pas suffisant. Avec des données contextuelles sélectionnées à partir d'ensembles d'informations sur les menaces personnalisés (flux d'informations sur les attaques et les menaces, et plus de 7 milliards de vulnérabilités gérées), les entreprises pourront appliquer une modélisation prédictive qui permettra de prévoir l'arrivée de nouvelles vulnérabilités et de hiérarchiser les activités de correction en fonction de leur gravité.

Dans l'idéal, les administrateurs informatiques devraient avoir une vue d'ensemble des attaques et vulnérabilités à haut risque les plus courantes dans leur console vCenter. Cela permettra d'intégrer facilement le renforcement des charges de travail dans les activités quotidiennes d'hygiène informatique.

De plus, les administrateurs informatiques ont besoin des informations d'audit relatives à l'état actuel du système pour pouvoir collaborer avec les équipes chargées de la sécurité sur la correction des menaces. Une visibilité partagée sur ces informations permettra naturellement à ces équipes de collaborer sur l'application de correctifs par ordre de priorité ou de se mettre d'accord sur des mesures alternatives, comme l'arrêt des systèmes vulnérables.

Une vue partagée des menaces et vulnérabilités actuelles indiquant le niveau de risque qui y est associé permet de définir des priorités claires et de concentrer ses efforts au même endroit, pour une résolution plus rapide des menaces existantes et une meilleure protection contre les futures attaques.

Étape 4 : Simplifier les processus des charges de travail

Traditionnellement, une analyse des vulnérabilités est réalisée tous les mois ou tous les trimestres. Mais ces analyses ponctuelles ne suffisent pas. Les charges de travail se développent de plus en plus sur des environnements multiclouds, et ces analyses ne fournissent pas les informations nécessaires au moment opportun pour limiter les menaces de sécurité critiques.

Avec une visibilité et une hiérarchisation des risques partagées, l'étape suivante pour les équipes chargées de l'informatique et de la sécurité est d'intégrer la sécurité des charges de travail dans les tâches d'hygiène informatique quotidiennes.

Mise en œuvre de la sécurité des charges de travail

La mise en œuvre de la sécurité des charges de travail exige des administrateurs informatiques qu'ils réduisent les surfaces d'attaques en continu dans le cadre de leurs pratiques en matière d'hygiène informatique. Ils doivent pouvoir accéder à l'évaluation de milliers de configurations sur leurs charges de travail, et aux informations qui leur permettront de savoir quelle direction prendre pour corriger les vulnérabilités détectées.

Les responsables informatiques devraient avoir accès à une vue partagée de l'évolution des tendances en matière d'hygiène informatique dans le temps. Cela encouragera les discussions concernant la gestion des vulnérabilités et la performance des mesures. Les responsables informatiques devraient utiliser ces informations pour s'assurer que les priorités sont respectées et que les ressources sont allouées où il faut pour un renforcement continu des charges de travail.

Quelle est la prochaine étape ?

Aligner les équipes informatiques sur la sécurité des charges de travail réduit les attaques

Les équipes chargées de la sécurité et les administrateurs informatiques peuvent collaborer pour améliorer la sécurité des charges de travail. Et avec les bons mécanismes de sécurité en place, cette collaboration peut se faire sans heurt et être facilement mise en œuvre au quotidien. Pour tirer pleinement parti de cette opportunité, ces équipes doivent :

- Utiliser une solution intégrée avec un seul agent
- Bénéficier d'une visibilité unifiée sur les données de sécurité intégrée dans leurs outils de travail actuels
- Disposer du contexte et de la surveillance continue nécessaires sur les vulnérabilités avec hiérarchisation des risques automatique
- Avoir le soutien de la direction pour garantir la bonne mise en œuvre du renforcement des charges de travail

Trois étapes clés pour améliorer la sécurité des charges de travail

1. Réunissez les responsables des équipes chargées de l'administration informatique et de la sécurité afin qu'ils discutent de la possibilité de collaborer pour réduire les attaques.
2. Identifiez les lacunes actuelles en matière de collecte et de visibilité des données pour être mieux à même de hiérarchiser les vulnérabilités et de renforcer les charges de travail.
3. Explorez les solutions qui permettront aux administrateurs informatiques et aux équipes chargées de la sécurité de profiter d'une visibilité partagée et du contexte nécessaire à des opérations réussies.

Gérer la sécurité des charges de travail s'avère payant

- Couverture totale et visibilité sur toutes les charges de travail
- Simplification de la pile de sécurité informatique
- Possibilité de répondre plus rapidement aux problèmes grâce à une détection précoce
- Meilleur renforcement des ressources
- Meilleure prévention contre les logiciels malveillants et les processus et logiciels indésirables
- Élimination totale des attaques non-malveillantes
- Mise en place d'une sécurité tournée vers l'avenir : environnements et charges de travail modernes

En savoir plus

Consultez cette fiche technique pour découvrir comment VMware Carbon Black Cloud™ permet aux équipes chargées de l'informatique et de la sécurité de collaborer sur l'amélioration de la sécurité des charges de travail.

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