kaspersky BRING ON THE FUTURE

Kaspersky Hybrid Cloud Security pour DevOps

Rapidité, exactitude ou innovation : DevOps fonctionne sous pression constante. De ce fait, les exigences de sécurité peuvent sembler faire obstacle au travail de DevOps. Néanmoins, tenir la sécurité à distance de vos processus critiques n'est pas judicieux ; vous avez besoin d'une solution qui comble l'écart entre DevOps et la sécurité des informations.

Combler l'écart entre DevOps et la sécurité des informations

L'adoption de DevOps connaît une croissance rapide, axée principalement sur les besoins de l'entreprise, le délai de mise sur le marché, la rapidité, la flexibilité et l'automatisation complète. Mais la sécurité a tendance à affecter négativement un ou plusieurs de ces indicateurs. Pour DevOps, le seul moyen de satisfaire les KPI consiste, semble-t-il, à minimiser ou à faire totalement l'impasse sur la sécurité, tandis que le département informatique s'efforce d'identifier l'informatique de l'ombre, à la fois dynamique et en pleine croissance, pour assurer sa couverture par le système de sécurité de l'entreprise.

De nombreuses problématiques se posent de chaque côté et viennent encore creuser l'écart. Le fait de ne pas parler le même langage et d'avoir des KPI différents (qui constituent à eux seuls des sources de préoccupation) ne simplifie en rien la situation.

En fournissant à DevOps une boîte à outils complète et les interfaces nécessaires pour tirer pleinement parti d'une approche de « sécurité en tant que code », Kaspersky Hybrid Cloud Security comble l'écart entre DevOps et la sécurité informatique et transforme DevOps en DevSecOps

Besoins informatiques	Besoins de DevOps
Gestion des risques liés aux informations	Configurabilité totale
Frais minimums	Une approche « tout en tant que code », intégrant la sécurité
Augmentation raisonnable du nombre d'outils de gestion	Prise en charge étendue des plates-formes
Image positive d'outil commercial	Impact minimal sur les performances
	Dynamique : le cycle de vie d'une entité peut être de quelques minutes, voire quelques secondes

Favoriser une approche DevSecOps avec la « sécurité en tant que code »

La solution Kaspersky Hybrid Cloud Security est un ensemble d'outils de sécurité efficace et hautement configurable permettant d'instaurer une véritable culture DevSecOps dans votre entreprise.

- Elle protège les plateformes Linux et Windows, les infrastructures de serveurs dans les clouds publics et virtualisés ainsi que les conteneurs Docker et Windows pour empêcher les attaquants d'utiliser un composant de conteneur malveillant comme porte d'accès à l'infrastructure de l'entreprise.
- Elle fournit au département informatique et à ses responsables des outils de contrôle de la sécurité et de gestion de la visibilité et des risques.

Prise en charge des plates-formes

Systèmes d'exploitation :
- Windows
- Linux

IaaS:
- Google Cloud Platform
- AWS
- Microsoft Azure

Plateformes de conteneurisation :
- Docker
- Conteneurs Windows

Plates-formes de virtualisation :
- VMWare vSphere et NSX
- Microsoft HyperV
- Citrix Server et applications et postes de travail virtuels
- KVM (Kernel-based Virtual Machine) :
- Nutanix AHV

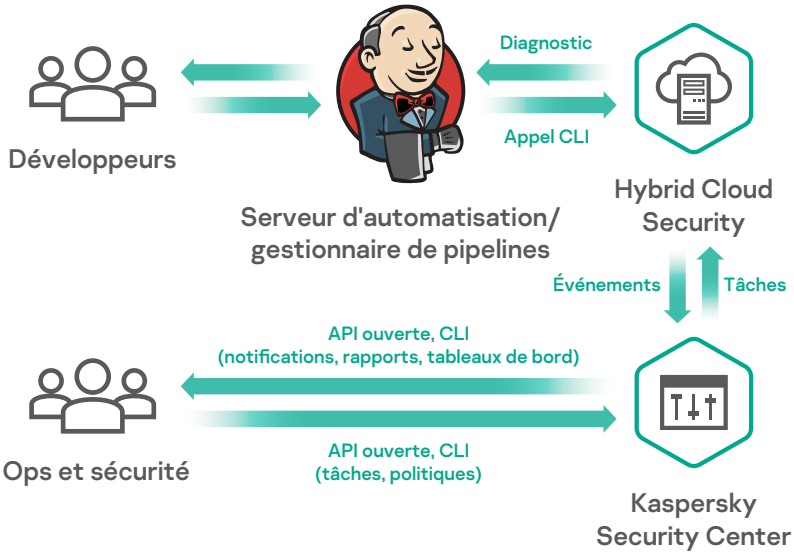
Orchestration et pipelines CI/CD :
- Jenkins
- TeamCity

Interface
- CLI :
- API ouverte

Kaspersky Hybrid Cloud Security favorise une approche de « sécurité en tant que code » :

- Protection de l'exécution et de la mémoire pour les plateformes de conteneurisation
- Sécurité par défaut, par l'analyse des images et des conteneurs
- Favorise l'orchestration des tests de sécurité
- « Shift-left » : intégration des routines de sécurité dans la phase de développement des pipelines CI/CD
- Multiples options d'intégration favorisant une approche « tout en tant que code »

- Elle offre des fonctionnalités avancées de génération de rapports et un fonctionnement basé sur les stratégies.
- Elle fournit des interfaces d'intégration pour l'automatisation et la création de pipelines, afin d'aider DevOps à maintenir des référentiels d'entreprise sains et de favoriser le nettoyage des entités émanant des référentiels publics.



Des options d'intégration multiples

Kaspersky Hybrid Cloud Security contribue également à associer les pratiques logicielles lean à la création, au packaging et à la diffusion « juste à temps » des applications de manière contrôlée et sécurisée, sans ralentir les processus.

- Les intégrations aux plateformes CI/CD (par exemple, Jenkins) simplifient la création et l'automatisation des pipelines.
- L'analyse en temps réel (OAS) et l'analyse à la demande (ODS) des conteneurs, des images et des référentiels locaux et distants facilitent l'entretien de référentiels propres pour les développeurs.
- La surveillance des espaces de nommage, le contrôle flexible du champ d'application des analyses basé sur les masques et la capacité à analyser différentes couches de conteneurs contribuent à faire appliquer les meilleures pratiques en matière de développement sécurisé.

Disponibilité sur les sites de vente de clouds publics

Kaspersky Hybrid Cloud Security est disponible sur la plupart des sites de vente de clouds publics et offre de nombreuses options de tarification, du modèle BYOL à l'abonnement à long terme. Un essai gratuit est également disponible avec un déploiement automatisé pour faciliter l'évaluation.

Sécurité pour DevOps : kaspersky.com/devops
Sécurité pour AWS : kaspersky.com/aws
Hybrid Cloud Security : kaspersky.com/hybrid
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise-security

www.kaspersky.fr