Sécurisez votre environnement avec la sécurité invisible de Nutanix

Comment sécuriser les applications et les données pour empêcher la propagation de malwares dans les clouds hybrides ?

PRINCIPAUX AVANTAGES

Protéger les données et empêcher les failles

- Chiffrez les données au repos
- Contrôlez et limitez l'accès aux données sensibles
- Analysez et auditez les configurations de sécurité
- Sécurisez vos clouds hybrides
- Empêchez la propagation des ransomwares

Segmenter et sécuriser les réseaux

- Déployez la microsegmentation et l'inspection des réseaux en quelques minutes
- Séparez les environnements réglementés par des contrôles logiciels automatisés

Simplifier les initiatives de réglementation et de conformité

- Automatisez les configurations du niveau de sécurité de base
- Validez la conformité aux politiques réglementaires (HIPAA, PCI, NIST, etc.)

LA SÉCURITÉ D'UN CLOUD HYBRIDE COMMENCE PAR UNE BASE D'INFRASTRUCTURE SOLIDE

Maintenir la sécurité des environnements d'aujourd'hui présente des difficultés pour plusieurs raisons. De nombreuses piles d'infrastructure traditionnelles sont composées de produits émanant de plusieurs fournisseurs, chacun étant découplé de la pile, ce qui donne une vision étroite et limitée de la sécurité. Valider et maintenir un niveau de sécurité de base par des mises à niveau logicielles constantes demande beaucoup de temps et implique souvent des processus manuels propices aux erreurs qui se font au détriment de l'innovation et de la productivité.

À l'ère du cloud, la sécurité doit être ancrée dans la culture, et les considérations de sécurité doivent constituer une partie essentielle du processus décisionnel de l'entreprise afin de répondre aux exigences élevées de conformité réglementaire et aux menaces de sécurité en constante évolution. Il faut que les entreprises s'efforcent d'intégrer l'automatisation dans le processus de maintien de la sécurité de leurs infrastructures, à la fois pour éviter les erreurs humaines et assurer une évolutivité transparente sans compromis sur la sécurité dans un environnement en constante évolution.

REPENSER LA SÉCURITÉ POUR UN AVENIR HYBRIDE

La sécurité d'un cloud hybride commence par une base d'infrastructure solide. C'est pourquoi la solution leader sur le marché offerte par Nutanix apporte non seulement une valeur opérationnelle et financière, mais aide également à améliorer le dispositif de sécurité et à prévenir les violations d'accès aux données en appliquant une stratégie de défense en profondeur pour la sécurité du cloud hybride.

Platform Security

Application and Network Security

SecOps and Compliance

NUTANIX™

NORMES ET CERTIFICATIONS

Nutanix applique plusieurs normes de sécurité et programmes de validation. L'entreprise respecte les normes internationales les plus strictes, y compris de nombreuses normes ISO, SOC et FIPS, afin de garantir aux gouvernements et aux organisations du monde entier que les produits Nutanix offrent les résultats escomptés et fonctionnent avec leur technologie existante.

Rendez-vous sur nutanix.com/trust pour plus de détails.

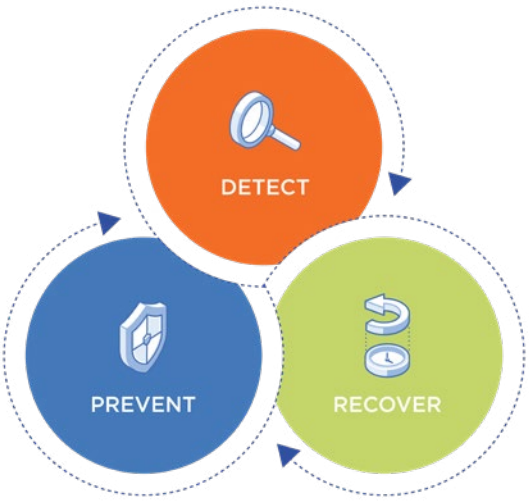
DÉFENSE À TOUS LES NIVEAUX

Sécurité de la plateforme : La sécurité est un aspect fondamental dans la conception des produits de Nutanix, à commencer par les pratiques de sécurité renforcée (comme le chiffrement des données au repos, des contrôles d'accès exhaustifs, etc.) intégrées à la plateforme de cloud d'entreprise. Les bonnes pratiques du secteur et les normes officielles sont intégrées dans un processus automatisé de contrôle de la configuration et d'autoguérison qui vient appuyer les objectifs de conformité. Des tests stricts portant sur les vulnérabilités courantes et la publication fréquente de correctifs minimisent le risque de violation d'accès aux données. Les incohérences sont consignées et ramenées à la ligne de base, ce qui garantit une configuration cohérente de la sécurité.

Sécurité des applications et des réseaux : Nutanix Flow fournit une sécurité réseau avancée au sein du datacenter, offrant une visibilité des applications et une protection contre la propagation des cybermenaces comme les ransomwares. Les réseaux et les applications peuvent être facilement segmentés au moyen d'une politique software-defined, sans matériel supplémentaire ni configuration réseau complexe. La fonctionnalité native de microsegmentation du réseau propose un modèle de découverte, de visualisation et de mise en œuvre des politiques qui simplifie et automatise l'application d'une politique réseau granulaire (microsegmentation) entre les VM.

SecOps, conformité et audit : Flow Security Central fournit une visibilité du dispositif de sécurité du cloud hybride, une aide à la gestion des politiques, des audits de configuration et une validation de la conformité pour Nutanix HCI. Security Central utilise une série d'audits de sécurité automatisés pour détecter et corriger les vulnérabilités de sécurité de l'infrastructure ainsi que les erreurs de configuration. Les administrateurs sécurité peuvent créer des politiques automatisées pour remédier aux vulnérabilités en temps réel. Security Central permet également de valider le niveau de conformité aux directives réglementaires telles que PCI-DSS, HIPAA, ou NIST – offrant ainsi une solution de conformité de la sécurité toujours disponible.

Prévenir, détecter et récupérer : Il n'existe pas d'action, de solution logicielle ou de contrôle de sécurité capable de protéger totalement votre organisation contre la menace des malwares et des ransomwares. La meilleure solution consiste à adopter une approche à plusieurs niveaux, une stratégie que l'on qualifie généralement de « défense en profondeur ». Pour réduire au minimum les coûts opérationnels et financiers, un plan complet doit inclure toutes les fonctionnalités intégrées de Nutanix et les articuler avec les contrôles et mesures de protection déjà en place dans votre datacenter.



NUTANIX

FAITES CONFIANCE À NUTANIX DANS LE CADRE DE VOTRE STRATÉGIE DE CYBERDÉFENSE

Plateforme HCI

- Niveau de sécurité de base avec autoguérison
- Snapshots de stockage et points de récupération
- Fonctions de protection et de réplication des données et d'automatisation de runbook
- Chiffrement des données au repos validé FIPS 140-2
- Segmentation des plans de données et des plans de contrôle
- Virtualisation native, conçue pour la sécurité

Correctifs et mises à niveau

- Application des correctifs CVE, mises à jour de la plateforme et gestion du cycle de vie « en un clic »
- Gestion des mises à niveau des firmwares et du BIOS

Gestion et automatisation

- Contrôle d'accès basé sur les rôles (RBAC)
- Gestion des identités et des accès
- Analyse des ressources, informations et détection des anomalies
- Automatisation sans code et lancement d'actions de sécurité
- Plans et automatisation des applications pour assurer une mise en œuvre cohérente des politiques

Réseau et sécurité

- Segmentation des réseaux et des applications
- Visibilité de l'application et des réseaux
- Inspection approfondie des paquets et intégrations de partenaires d'analyse des menaces
- Enregistrement des politiques et des événements
- Conformité de la sécurité et outils d'audit

Services de stockage

- Politiques de blocage des types de fichiers
- Détection des anomalies liées à l'activité des fichiers
- Prise en charge d'ICAP pour l'intégration d'antivirus
- Prise en charge des politiques WORM immuables

Sauvegarde, continuité des opérations et reprise après sinistre

- Réplication et protection des données natives
- Solution d'archivage et de sauvegarde pour le stockage secondaire
- Reprise après sinistre en tant que service sur le cloud

NUTANIX™
YOUR ENTERPRISE CLOUD

Tél +33 (0)1 82 88 15 90
contact-france@nutanix.com | www.nutanix.fr | @NutanixFrance