Proteja su entorno con la seguridad invisible de Nutanix

Proteja sus aplicaciones y datos para evitar la propagación de malware en las clouds híbridas

PRINCIPALES BENEFICIOS

Proteja sus datos y evite violaciones de seguridad

- Cifre datos en reposo
- Controle y restrinja el acceso a los datos sensibles
- Analice y audite las configuraciones de seguridad
- Asegure sus clouds híbridas
- Evite la propagación de ransomware

Segmente y asegure las redes

- Implemente en minutos la microsegmentación y la inspección de la red
- Separe los entornos regulados con controles de software automatizados

Simplifique los esfuerzos de regulación y cumplimiento

- Automatice las configuraciones de línea de base de seguridad de la plataforma
- Valide el cumplimiento de las políticas regulatorias (HIPAA, PCI, NIST, etc)

LA SEGURIDAD EN LA CLOUD HÍBRIDA COMIENZA CON UNA SÓLIDA BASE DE INFRAESTRUCTURA

Mantener la seguridad en los entornos actuales es un reto por varias razones. Muchos stacks de infraestructura tradicionales se componen de productos de múltiples proveedores, cada uno desvinculado del stack, lo que proporciona una visión reducida y limitada de la seguridad. La validación y el mantenimiento de una línea de base de seguridad mediante continuas actualizaciones de software lleva mucho tiempo y a menudo implica procesos manuales propensos a errores que restan innovación y productividad.

En la era de la cloud, la seguridad debe estar arraigada en la cultura y las consideraciones de seguridad deben ser una parte esencial de la toma de decisiones de la empresa para cumplir con el alto nivel de regulación normativa, así como para abordar los desafíos de un panorama de amenazas para la seguridad en evolución. Las empresas deben esforzarse por incorporar la automatización en el proceso de mantenimiento de la seguridad en la infraestructura, para evitar los errores humanos y poder ofrecer una escalabilidad perfecta sin comprometer la seguridad en un entorno en constante cambio.

REPENSAR LA SEGURIDAD PARA UN FUTURO DE CLOUD HÍBRIDA

La seguridad en la cloud híbrida comienza con una base de infraestructura sólida. Aquí es donde la solución líder del sector de Nutanix no solo proporciona valor operativo y financiero, sino que también ayuda a mejorar la postura de seguridad y a prevenir las filtraciones de datos al apoyar un enfoque de defensa en profundidad para la seguridad de la cloud híbrida.

Platform Security

Application and Network Security

SecOps and Compliance

NUTANIX

ESTÁNDARES Y CERTIFICACIONES

Nutanix emplea múltiples estándares de seguridad y programas de validación. Cumple con los estándares internacionales más estrictos, incluidos numerosos estándares ISO, SOC y FIPS, para garantizar a los gobiernos y empresas de todo el mundo que los productos Nutanix funcionan como se espera y trabajan con su tecnología existente.

Visite nutanix.com/trust para conocer todos los detalles

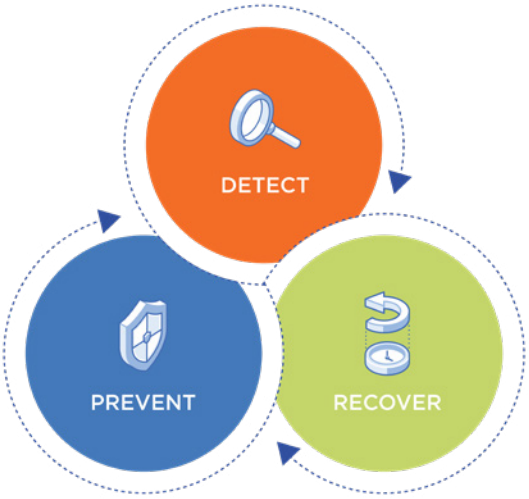
DEFENSA A TODOS LOS NIVELES

Seguridad de la plataforma: La seguridad es un aspecto fundamental del diseño de producto en Nutanix, empezando por las prácticas de endurecimiento de la seguridad (como el cifrado de datos en reposo, los controles de acceso exhaustivos, etc.) incorporadas a la plataforma de cloud empresarial. Las buenas prácticas del sector y las normas gubernamentales se incorporan a un proceso automatizado de supervisión de la configuración y de reparación autónoma que respalda los objetivos de regulación. Las pruebas estrictas de las vulnerabilidades más comunes y los frecuentes lanzamientos de parches minimizan el riesgo de filtración de datos. Las incoherencias se registran y se revierten a la línea de base garantizando la coherencia de la configuración de seguridad.

Seguridad de aplicaciones y redes: Nutanix Flow ofrece seguridad de red avanzada en el centro de datos, proporcionando visibilidad de las aplicaciones y protección contra la propagación de ciberataques como el ransomware. Las redes y las aplicaciones se pueden segmentar fácilmente mediante una política definida por software, sin necesidad de hardware adicional ni de complejas configuraciones de red. La funcionalidad de microsegmentación de red nativa proporciona un modelo de descubrimiento, visualización y aplicación de políticas que simplifica y automatiza la aplicación de políticas de red granulares (microsegmentación) entre máquinas virtuales.

SecOps, regulación y auditoría: Flow Security Central proporciona visibilidad de la postura de seguridad de cloud híbrida, asistencia para la gestión de políticas, auditorías de configuración y validación de la regulación para Nutanix HCI. Security Central utiliza un conjunto de auditorías de seguridad automatizadas para detectar y corregir vulnerabilidades de seguridad de la infraestructura y errores de configuración. Los administradores de seguridad pueden crear políticas automatizadas para solucionar vulnerabilidades en tiempo real. Security Central también ayuda a validar el nivel de cumplimiento de las directrices regulatorias como PCI-DSS, HIPAA, NIST, etc., ofreciendo una solución de regulación de seguridad siempre activa.

Prevenir, detectar y recuperar: No hay una sola acción, solución de software o control de seguridad que pueda proteger por completo a su empresa de las amenazas de malware y ransomware. La mejor solución es un enfoque de múltiples capas, comúnmente llamado estrategia de "defensa en profundidad". Para minimizar tanto sus costes operativos como financieros, su plan integral debe incluir todas las capacidades integradas de Nutanix que trabajan junto con controles y protecciones que pueden existir en su centro de datos.



NUTANIX

CONFÍE EN NUTANIX COMO PARTE DE SU ESTRATEGIA DE CIBERDEFENSA

Plataforma HCI

- Línea de base de la configuración de seguridad de recuperación autónoma
- Instantáneas de almacenamiento y puntos de recuperación
- Protección de datos, replicación y automatización de runbook
- Cifrado de datos en reposo validado por FIPS 140-2
- Segmentación de plano de datos y plano de control
- Virtualización nativa: creada para la seguridad

Parches y actualizaciones

- Aplicación de parches CVE mediante un solo clic, actualizaciones de plataforma y gestión del ciclo de vida
- Firmware y gestión de la actualización de la BIOS

Gestión y automatización

- Control de acceso basado en roles (RBAC)
- Gestión de identidades y accesos
- Analíticas de recursos, información y detección de anomalías
- Automatización sin código y activadores de eventos
- Planos de aplicación y automatización para garantizar una aplicación de políticas consistente

Redes y seguridad

- Segmentación de red y aplicaciones
- Visibilidad de aplicaciones y redes
- Inspección profunda de paquetes e integraciones de partners de inteligencia de amenazas
- Política y registro de eventos
- Herramientas de auditoría y regulación de la seguridad

Servicios de almacenamiento

- Políticas de bloqueo de tipos de archivos
- Detección de anomalías en la actividad de los archivos
- Soporte ICAP para la integración de antivirus
- Soporte de políticas WORM inmutables

Copia de seguridad, continuidad del negocio y recuperación ante desastres

- Replicación nativa y protección de datos
- Solución de archivo y copia de seguridad para el almacenamiento secundario
- Recuperación ante desastres como servicio

NUTANIX™
YOUR ENTERPRISE CLOUD

T. 855.NUTANIX (855.688.2649) | F. 408.916.4039
info@nutanix.com | www.nutanix.com | @nutanix