SUSE® NeuVector

Juego de ventas: seguridad de contenedores de confianza cero

¿Cuál es la historia?

La computación en la nube y el cambio a las infraestructuras de contenedores están generando ventajas significativas para las empresas de hoy, acelerando el desarrollo y permitiendo que las propias empresas se muevan más rápidamente en sus mercados. Sin embargo, esta agilidad tiene sus desventajas: los contenedores no son fáciles de asegurar de manera efectiva. Defender una red tradicional requiere un enfoque de seguridad en capas que incluya tecnologías como análisis de vulnerabilidades, firewalls, puertas de enlace, DLP, etc. Pero esas herramientas no funcionan para defender Kubernetes porque las conexiones de red están ocultas y no se puede actuar de forma proactiva como un resultado. SUSE NeuVector ofrece el tipo de plataforma de seguridad que las empresas han conocido durante años en el lado de la infraestructura tradicional y aplica muchas de esas capacidades tan necesarias a los contenedores, protegiendo en las capas de proceso, acceso a archivos y red. SUSE NeuVector permite a las organizaciones globales asegurar de manera integral sus aplicaciones nativas de K8 sin comprometer la velocidad del negocio. Simplifica y automatiza la seguridad al mismo tiempo que brinda una defensa en profundidad para las aplicaciones nativas de Kubernetes desde la canalización hasta la producción... brindando visibilidad y protección de la red inigualables, automatización optimizada y cumplimiento para los equipos de seguridad, DevOps e infraestructura. La plataforma unificada de seguridad y cumplimiento de SUSE NeuVector permite a los clientes:

ÿ Simplifique y automatice la seguridad, con software que aprende a identificar lo que la infraestructura necesita para protegerla y luego crea y define automáticamente políticas que toman inmediatamente una postura protectora contra amenazas.

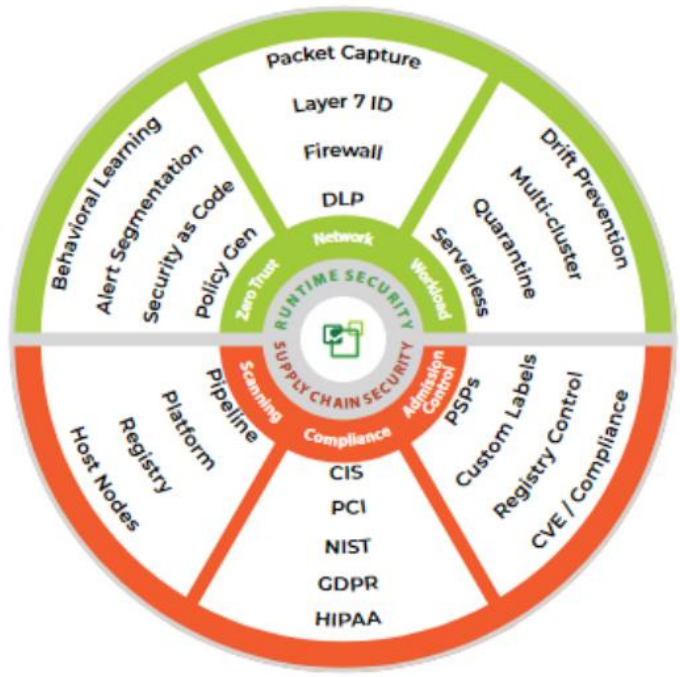
ÿ Proporcione seguridad de confianza cero para las aplicaciones nativas de Kubernetes desde la canalización de desarrollo todo el camino a través de la producción.

ÿ Proteja proactivamente las capas de proceso, acceso a archivos y red. ÿ Haga que

sea lo más fácil posible para los desarrolladores proteger las aplicaciones: SUSE NeuVector producir un archivo de código yaml para desarrolladores que replicará políticas de seguridad predefinidas específicas. Esto brinda a los equipos de seguridad la confianza que necesitan para ejecutar contenedores de manera segura y hace que la aplicación de políticas de seguridad sea una tarea automatizada y sin interrupciones para los

equipos de DevOps. ÿ Haga más que escanear y aplicar parches para mantener el entorno seguro: Evite que se produzcan daños en primer lugar con políticas inteligentes basadas en software que aprende y protege de forma proactiva contra las amenazas.

ÿ Incluye muchas de las funciones que los clientes empresariales reconocerán de las suites de seguridad tradicionales, incluido el cortafuegos, la prevención de pérdida de datos (DLP), el cortafuegos de aplicaciones web (WAF), la inspección profunda de paquetes (DPI) y los registros de alerta... todo adaptado al entorno del contenedor.



La plataforma de cumplimiento y seguridad de contenedores SUSE NeuVector lleva la seguridad de los contenedores al nivel de seguridad tradicional, proporcionando una cobertura amplia y profunda para ofrecer una observabilidad, seguridad y automatización únicas en todas las principales plataformas y orquestadores en la nube.

Problema / Desafío (Dolor) Motivo	del Problema	Impacto organizacional negativo Cómo resolvemos el problema	Beneficio para el cliente
Falta de visibilidad del tráfico de red en contenedores	Kubernetes oscurece todo el tráfico de la red, incluido el tráfico de este a oeste dentro de un entorno de contenedor. Los contenedores son un entorno de movimiento extremadamente rápido: es posible que un contenedor solo exista durante minutos o incluso segundos.	Los equipos de seguridad deben confiar únicamente en el análisis de vulnerabilidades y en la supervisión de algunos procesos. Si no pueden ver el tráfico este-oeste, no pueden promulgar políticas de seguridad de red dentro del entorno, lo que deja a las aplicaciones en contenedores y los microservicios vulnerables a muchos tipos diferentes de ataques.	**SUSE NeuVector se despliega como un contenedor y tiene la capacidad única (única en el mercado) de poder inspeccionar el tráfico de red, incluido el ingreso y salida de este a oeste y de norte a sur. Esto permite que NeuVector actúe sobre ese tráfico alertando y/o bloqueando esa red.** **tráfico *antes* de que llegue al núcleo y cause daños.**	Vea y actúe sobre el tráfico de la red para alertar y bloquear proactivamente las amenazas detectadas en los entornos de contenedores antes de que se produzcan daños en el proceso, el acceso a los archivos y, lo que es más importante, en la capa de red. Realice una inspección profunda de paquetes y prevención de pérdida de datos al poder ver el tráfico este-oeste en Kubernetes.
Necesita simplificar el cumplimiento	Es importante que las empresas que operan en industrias reguladas proporcionen pruebas de cumplimiento para el entorno de contenedores.	Es posible que los clientes que operan en industrias altamente reguladas no puedan responder a las preguntas del auditor sobre el entorno del contenedor. Es posible que los clientes nuevos en contenedores no sepan que deben tener en cuenta el cumplimiento.	**SUSE NeuVector ingiere todos los puntos de referencia de CIS, los analiza en áreas de cumplimiento específicas y luego escanea para certificar su posición.** **SUSE NeuVector también demuestra el cumplimiento de SOC2 y otros marcos de cumplimiento a través de su capacidad de prevención de pérdida de datos (DLP).**	Acceda e informe sobre todos los estándares principales, incluidos PCI, NIST, GDPR, HIPAA. Acceda e informe contra estándares personalizados para la certificación de cumplimiento específica de la industria. Demuestre el cumplimiento de SOC2 (y otros) a los auditores con DLP.
No se puede proteger en la capa de red	Sin visibilidad de la Capa 7 (la capa de aplicación de la pila de redes donde se definen las actividades y los protocolos de la red), los administradores no pueden defender de manera proactiva un entorno de Kubernetes de los ataques basados en la red. Las correcciones de compatibilidad del kernel, los agentes y otras tecnologías reclaman visibilidad, pero solo pueden *inferir* lo que *ya sucedió* en la red a nivel de proceso.	La única forma de bloquear los ataques a la red es verlos primero. Sin NeuVector, los clientes deben confiar en las alertas de eventos *después de* que hayan ocurrido. La visibilidad posterior no es útil: los clientes no pueden detener algo que ya sucedió.	**SUSE NeuVector proporciona visibilidad real de la capa de red, identificando y visualizando las conexiones de red y las políticas de seguridad utilizadas para protegerlas. SUSE NeuVector crea automáticamente políticas de seguridad para aislar y proteger implementaciones e inspecciona y supervisa contenedores y hosts en busca de actividad sospechosa en el proceso, el acceso a archivos y, lo que es más importante, la capa de red.**	Obtenga una vista en vivo de las conexiones de red. La visibilidad de la red de nivel 7 dentro y entre los pods de Kubernetes utiliza el tráfico de la red como la fuente de la verdad. Identifique y valide los protocolos de aplicación para evitar la tunelización y los ataques de día cero. Detecte amenazas provenientes de la red con inspecciones profundas de paquetes patentadas. Bloquee automáticamente tanto las amenazas conocidas como las desconocidas.
Hacer que DevOps maneje la seguridad	La seguridad de los contenedores a menudo comienza en el nivel de la aplicación, en DevOps. De hecho, los equipos de seguridad están presionando a los desarrolladores y equipos de DevOps para que construyan su infraestructura y aplicaciones de forma segura a medida que se desarrollan. Los equipos de desarrolladores y DevOps no siempre tienen la experiencia o los recursos para hacerlo de manera efectiva.	Puede generar una fricción significativa entre los equipos de DevOps y Seguridad. Es posible que DevOps no sepa cómo proteger adecuadamente los contenedores o las aplicaciones. Los equipos de DevOps pierden un valioso tiempo de codificación, ya que deben crear manualmente políticas de seguridad para cada entorno.	**SUSE NeuVector utiliza *seguridad como código* para crear y exportar automáticamente todas las políticas que DevOps necesita en un archivo yaml que pueden aplicar fácilmente a las aplicaciones y luego replicar en todos los entornos requeridos. La seguridad puede brindar a DevOps las políticas que desean implementar para que estén seguros de lo que se está haciendo. Y DevOps puede enfocarse en administrar los entornos en lugar de escribir políticas de seguridad.**	Implemente políticas de seguridad detalladas automáticamente sin distraer ni ralentizar DevOps. Escanee automáticamente en busca de vulnerabilidades y aplique seguridad en tiempo de ejecución para proteger las aplicaciones desde la canalización hasta la producción.

SUSE® NeuVector

Juego de ventas: seguridad de contenedores de confianza cero

Perfil del Cliente para una Buena Oportunidad **Cualquier cliente que utilice contenedores.** La seguridad es imprescindible para cualquiera que use contenedores en la empresa.

Con quién hablar:

• Arquitecto de seguridad: se preocupa por la visibilidad de la red • Ingeniero de seguridad: se preocupa por la automatización y la seguridad como código • Seguridad de las aplicaciones: demasiado específico: Ascienda en la cadena de decisiones • SOC: interesado en alertas para la gestión de amenazas • Desarrolladores: no quieren ser responsable de asegurar los contenedores; conseguir ellos para traer Provisecurity a la mesa

Nota: *Siempre* traiga al equipo de seguridad a la conversación; si no lo hace, perderá el trato. DevOps se enfoca solo en escanear. Seguridad sabe mejor y apreciará lo que tenemos para ofrecer.

Competidores Principales

Competidor #1 de **Aquasec ;**
no tiene visibilidad de tiempo de ejecución o confianza cero: deja a los usuarios vulnerables a ataques de día cero, sin protección de red.

Prisma / Twistlock (Palo Alto)
No tiene visibilidad de red ni confianza cero. Sin seguridad como código. Buen escáner y se integra con la suite de productos Palo.

Proveedores de Service Mesh
No competimos, solo complementamos.

StackRox (sombrero rojo)
No tiene visibilidad en tiempo de ejecución ni confianza cero. OpenShift es propietario: no hay garantías de que Red Hat sea compatible con K8 nativo, Rancher, EKS y otros orquestadores y distribuciones de código abierto.

Sysdig
no tiene visibilidad de tiempo de ejecución ni confianza cero. El enfoque de solo monitoreo no puede proteger o hacer cumplir la seguridad. Basado en agentes: no es una buena opción para el entorno de contenedores.

Diferenciadores defendibles

diferenciador	Beneficio	Enfoque alternativo	Debilidad de la alternativa
Automatiza Automatización de Kubernetes	Solo SUSE NeuVector proporciona microsegmentación de confianza cero. Crea y aplica automáticamente políticas de seguridad inteligentes... y luego se bloquea para alertar o bloquear cualquier anomalía en las capas de proceso, acceso a archivos y red. SUSE NeuVector permite a los clientes crear seguridad como código mediante la creación automática de políticas de seguridad exportables para usar en otros entornos.	Se basa en alertas después de que se ha producido un ataque o no se emite en absoluto, si no se han implementado protecciones. Debe crear manualmente políticas de seguridad para cada entorno individual.	No hay capacidad para bloquear antes de que ocurra un ataque. No hay medidas proactivas contra los días cero. Requiere horas de redacción y auditoría de políticas de seguridad en todo el entorno.
Utiliza el tráfico de red como una fuente de verdad para proteger la red	Con su vista en vivo de las conexiones de red, SUSE NeuVector puede proporcionar visibilidad de la red de capa 7 dentro y entre los pods de Kubernetes. Los administradores pueden detectar amenazas de red y bloquear automáticamente amenazas conocidas y desconocidas.	Los competidores usan eBPF como tecnología para ver la actividad dentro de los contenedores, pero eso se limita solo a la actividad basada en procesos (no a la capa de red) y se basa en la información recibida *después de* un ataque ya ha afectado al núcleo.	No puede proporcionar una visibilidad completa de los contenedores y solo informa sobre los eventos después de que ya han llegado al kernel.

Preguntas de Business Discovery **Falta de visibilidad del tráfico de red en contenedores** ÿ ¿Qué tan importante es para usted ver el tráfico de red dentro de los K8? ÿ ¿Puede ver el interior del entorno de su contenedor? ÿ ¿Qué tan bien puede monitorear el tráfico este-oeste? ÿ ¿Qué políticas de seguridad de red puede aplicar dentro de ese ¿medioambiente?

ÿ ¿Qué tan vulnerable es el entorno de su contenedor a múltiples tipos de ataca por eso?

ÿ ¿Actualmente está escaneando sus contenedores? ¿Que usas? ¿Qué usas además de escanear?

Necesita simplificar el cumplimiento

ÿ ¿Qué tan importante es el cumplimiento normativo para la industria en la que opera? ¿en?

ÿ ¿A qué normas está sujeta su organización? ¿Cuáles son los consecuencias de no poder demostrar el cumplimiento a los auditores?

ÿ ¿Cómo proporciona pruebas de cumplimiento para todos los contenedores? funcionando en su infraestructura? ¿Cuánto tiempo se tarda? ¿Cuál es tu proceso para hacer esto?

No se puede proteger en la capa de red ÿ

Cuando se trata de contenedores, ¿qué tan lejos a lo largo de la pila de red puede ¿ver? ¿Tiene visibilidad en la capa 7?

ÿ La capa 7 es la pila de aplicaciones, donde se definen las actividades y los protocolos de la red. ¿Cómo defiende su entorno de Kubernetes de los ataques basados en la red?

ÿ Si está utilizando correcciones de compatibilidad del kernel, agentes o cualquier otra cosa para ganar visibilidad en su entorno de Kubernetes, ¿cuánto puede ver realmente? ¿Puede ver una inferencia de lo que ya sucedió, o puede identificar y visualizar sus conexiones de red, así como las políticas de seguridad utilizadas para protegerlas?

Hacer que DevOps maneje la seguridad ÿ

¿Cuánto de la seguridad de su contenedor comienza en la capa de aplicación? ÿ ¿Qué tanto presionan los equipos de seguridad a los equipos de DevOps para que asuman el trabajo de proteger las aplicaciones que se ejecutan en contenedores? ÿ ¿Cuánta experiencia en seguridad tiene su equipo de DevOps?

ÿ ¿Cuánta fricción causa esta expectativa entre los equipos de seguridad? y DevOps?

ÿ ¿Cuánto tiempo les lleva a los desarrolladores concentrarse en el escaneo de seguridad, la codificación y otras actividades? ¿Cuánto más eficaz podría ser DevOps para la empresa si pudieran centrarse en la codificación de aplicaciones empresariales?

Manejo de objeciones *"¿Cómo puede automatizar la seguridad de Kubernetes?"* ÿ Lo hacemos usando una combinación de aprendizaje conductual y Kubernetes integración con definiciones de recursos personalizadas (CRD) que implementamos como código de seguridad. ÿ Es posible que deba realizar alguna configuración o personalización manual inicial, pero una vez que se activa el interruptor de producción y Kubernetes comienza a administrar los pods, su seguridad debe automatizarse, adaptarse y escalar con su implementación.

"¿Cómo se puede brindar seguridad en un panorama de amenazas tan amplio?" ÿ Al proporcionar seguridad en tiempo de ejecución de múltiples vectores, combinando un Kubernetes Cortafuegos de contenedores con inspección de contenedores y seguridad del host: podemos detectar y prevenir las actividades en la cadena de eliminación de seguridad.

ÿ SUSE NeuVector se implementa como un contenedor. Ese contenedor se encuentra al lado de su contenedores de aplicaciones, que proporcionan seguridad siempre activa y en ejecución sin introducir latencia en el entorno.

ÿ Debido a la naturaleza declarativa de las aplicaciones basadas en contenedores y la amplia integración disponible para Kubernetes, podemos aplicar controles de seguridad avanzados incluso en el entorno de contenedores hiperdinámicos. ÿ Al integrarse con Kubernetes e incorporar el aprendizaje del comportamiento en entornos multivectoriales, SUSE NeuVector hace posible la automatización de la seguridad en todo el proceso y en la producción.

"¿Cómo puede la seguridad como código facilitar la implementación para mis desarrolladores?"

ÿ Los desarrolladores están siendo presionados por los equipos de seguridad para asumir la seguridad en el nivel de aplicación del contenedor. Los desarrolladores pueden hacer poco más que escanear el código que incluyen en cada contenedor: es un nivel limitado de seguridad del contenedor que es lo mínimo que podemos hacer.

ÿ Pero SUSE NeuVector define qué comportamientos de la aplicación deben ser en un Archivo yaml nativo de Kubernetes que puede hacer cumplir las reglas de seguridad global, tener en cuenta RBAC y aplicar políticas para conexiones y protocolos de red, controles de entrada/salida, actividad del sistema de archivos y procesos, y más. ÿ Todo lo que tiene que hacer la seguridad es dar estos archivos yaml al desarrollo. Todo lo que los desarrolladores tienen que hacer es aplicar esos archivos. El resultado: la empresa adopta un enfoque de seguridad como código consistente y exigente que les brinda un control de seguridad detallado sin interrumpir la atención y los objetivos del desarrollador.