tenable.io
Container Security

HOJA DE DATOS

INTEGRE LA SEGURIDAD EN LOS PROCESOS EN DESARROLLO DE DEVOPS

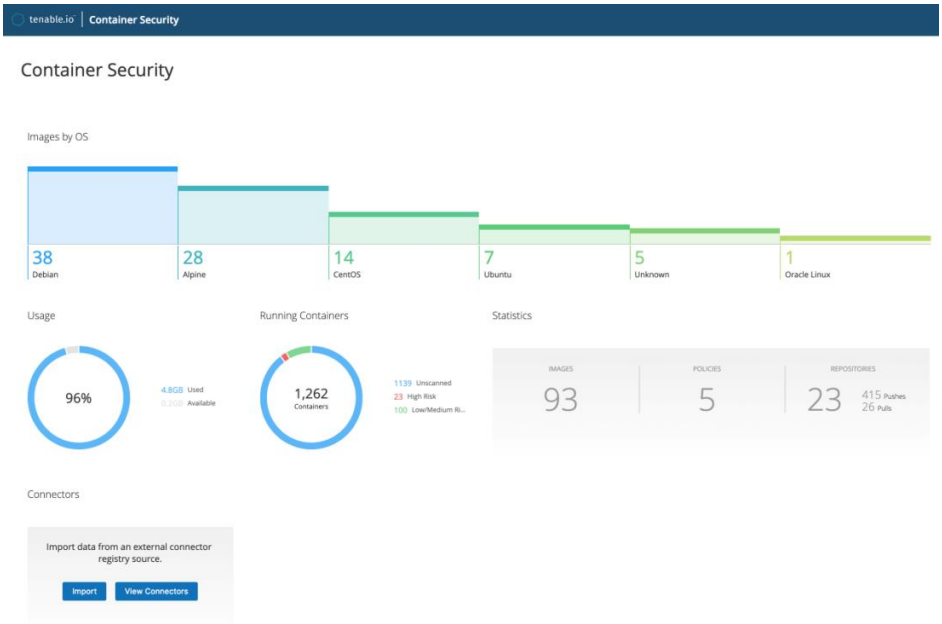
En la medida en que las organizaciones dependen cada vez más del software para proporcionar una ventaja competitiva, los requisitos empresariales para la entrega segura, rápida y eficiente del software nunca han sido tantos. Los equipos de DevOps están respondiendo al requisito de velocidad y agilidad de las empresas mediante la optimización de los procesos de entrega de software. Cada vez más, utilizan contenedores Docker para construir y respaldar rápidamente nuevos servicios y aplicaciones. Sin embargo, los contenedores presentan importantes riesgos para la seguridad. La falta de direccionalidad de IP, la corta vida útil y el gran volumen y variedad de contenedores hacen que protegerlos sea un desafío constante.

Obtener una visibilidad de los contenedores previa a la producción es fundamental para que pueda comprender los riesgos potenciales de las aplicaciones en contenedor antes de que sean implementadas. Los equipos de DevOps obtienen la información que necesitan para reparar rápidamente las vulnerabilidades y el malware en imágenes en contenedor lo antes posible en el proceso de desarrollo, lo que reduce el riesgo antes de la implementación y acelera el desarrollo.

Tenable.io Container Security se integra en el pipeline de DevOps para eliminar los puntos ciegos de seguridad, sin desacelerar el desarrollo de software. Tenable.io Container Security proporciona visibilidad de extremo a extremo de imágenes de contenedores Docker, brindando evaluación de vulnerabilidades, detección de malware y aplicación de políticas antes y después de la implementación. Compatible con la toolchain de DevOps que sus desarrolladores ya utilizan, Tenable.io Container Security brinda visibilidad y seguridad proactivas para resolver los desafíos de seguridad de los contenedores a la velocidad de desarrollo y operaciones.

BENEFICIOS PRINCIPALES

- **Acelere de forma segura DevOps**
  Evalúe las imágenes de los contenedores en busca de vulnerabilidades y malware en menos de 30 segundos desde la toolchain de DevOps para evitar reducir la velocidad del código.
- **Disminuya los costos de reparación**
  Reduzca drásticamente los costos de reparación hasta en un 85 % al descubrir y reparar los defectos del software durante el desarrollo antes del lanzamiento de la aplicación.
- **Obtenga una visibilidad precisa y detallada**
  Comprenda las capas individuales de las imágenes de los contenedores para obtener una visión precisa del riesgo cibernético, reducir los falsos positivos y proporcionar una guía de reparación detallada.
- **Proteja los contenedores en ejecución**
  Obtenga visibilidad hacia los contenedores en ejecución y detecte nuevas vulnerabilidades y los problemas de seguridad que puedan surgir después de la implementación.
- **Aplique políticas de seguridad**
  Bloquee los nuevos desarrollos de contenedores que superen los umbrales de riesgo de su organización para garantizar que los contenedores cumplan con sus políticas de seguridad antes de la implementación.



Tenable.io Container Security proporciona una vista rápida de su entorno de contenedores, incluidas las imágenes, las políticas, los repositorios y la información operativa clave.

tenable.io Container Security

HOJA DE DATOS

CAPACIDADES PRINCIPALES

PARA LOS EQUIPOS DE SEGURIDAD:

Panel de vista rápida

Los paneles de Tenable.io Container Security brindan a los gerentes de seguridad de TI una vista rápida de la seguridad y el inventario de imágenes de contendores. Los equipos de seguridad pueden ver la vulnerabilidad, el malware y otros datos de seguridad de todas las imágenes de los contenedores, así como la distribución de las vulnerabilidades entre las imágenes según la puntuación de CVSS y el nivel de riesgo. El producto también muestra el sistema operativo, la versión del sistema operativo y la arquitectura de cada imagen.

Protección contra malware para contenedores

Tenable.io Container Security es una de las únicas soluciones de seguridad de los contenedores que evalúan el código fuente de las imágenes de contenedores en busca de malware. Utiliza un motor de detección de malware personalizado para analizar el código fuente de las imágenes de contenedores y ayudar a garantizar que estén libres de malware.

Aplicación de políticas empresariales

Opcionalmente, se puede exigir el cumplimiento de políticas empresariales mediante el monitoreo de las imágenes de contenedores para factores como la puntuación general de riesgos y la presencia de malware. Si se crea una imagen que excede el umbral de riesgo de la organización, se puede notificar de inmediato a los desarrolladores, con información específica de la capa provista para ayudarlos a reparar rápidamente. Las infracciones de las políticas pueden activar alertas u, opcionalmente, bloquear la implementación de imágenes específicas. Las políticas pueden aplicarse a nivel global o solo a imágenes en repositorios específicos.

Sincronización de imágenes de registros de terceros

Obtenga información instantánea sobre los riesgos de seguridad de los contenedores mediante la sincronización de sus imágenes de registros existentes en Tenable.io Container Security con un simple paso. El producto se integra con Docker Registry, Docker Trusted Registry, JFrog Artifactory y Amazon EC2 Container Registry.

Escaneo de contenedores en ejecución

Obtenga visibilidad hacia la postura de seguridad de sus contenedores en ejecución con Tenable.io Container Security. Acceda a importantes datos operativos de los contenedores, tales como las direcciones IP, el ID del contenedor, el estado de escaneo y la puntuación de riesgos. El producto identifica las imágenes de contenedores en ejecución y en producción que aún no han sido probados en busca de vulnerabilidades. Además, detecta si los contenedores han cambiado después de la implementación, con detalles sobre cuáles fueron los paquetes que se modificaron.

La evaluación continua identifica nuevas amenazas

En el cambiante panorama tecnológico, cada día se identifican nuevas vulnerabilidades. Tenable.io Container Security ayuda a los equipos de seguridad a responder rápidamente a los nuevos riesgos mediante el monitoreo continuo de las bases de datos de vulnerabilidades en busca de nuevas vulnerabilidades. Cuando se identifica una, Tenable.io Container Security vuelve a evaluar automáticamente todas las imágenes de contenedores almacenadas contra la nueva vulnerabilidad.

Seguridad de los contenedores y gestión de vulnerabilidades integradas

La seguridad de los contenedores no es un requisito independiente, sino una parte integral de un programa de gestión de vulnerabilidades. Tenable fue el primer proveedor de gestión de vulnerabilidades en ofrecer seguridad de los contenedores integrada con Tenable.io Container Security, un elemento modular de la plataforma de Cyber Exposure de Tenable.

PARA LOS EQUIPOS DE DEVOPS:

Avisos de reparación específicos

Tenable.io Container Security proporciona información sin precedentes a las áreas de desarrollo y operaciones sobre la seguridad de las imágenes de sus contenedores Docker. Además de proporcionar una vista de las imágenes por repositorio, realiza una evaluación detallada de vulnerabilidades de cada imagen de contenedor cuando esta se envía a Tenable.io Container Security. Realiza un inventario de los componentes de contenedores, así como una evaluación de las imágenes antes de que se implementen, y elabora una lista de todas las capas y los componentes, que incluye la aplicación, las dependencias, las bibliotecas y los archivos binarios. Esta visión rápida y completa de las vulnerabilidades, combinada con la inteligencia de la jerarquía de capas, proporciona una evaluación detallada del riesgo de las imágenes de contenedores, por repositorio. Así, asegura que los desarrolladores no pierdan el tiempo buscando vulnerabilidades o reparando problemas que se mitigan en una capa superior. Esto les permite reparar rápidamente los riesgos potenciales de los contenedores e insertar código seguro aún más rápido.

Integración en la toolchain de DevOps

En entornos de DevOps, Tenable.io Container Security puede, opcionalmente y sin complicaciones, integrar las pruebas de seguridad en las herramientas de desarrollo de software, sin bloquear ni interrumpir los procesos de desarrollo de software y los flujos de trabajo existentes. El producto se integra con sistemas de automatización comunes, como Jenkins, Bamboo, Shippable, Travis CI y otros, así como con otras herramientas de integración continua/implementación continua utilizadas por los desarrolladores de software. Tenable.io Container Security también incluye una API REST robusta y totalmente documentada para integraciones personalizadas con herramientas de DevOps adicionales, o exportación de datos a las herramientas de generación de informes utilizadas por el equipo de seguridad.

Para obtener más información: visite **tenable.com**
Contáctenos: envíenos un correo electrónico a **sales@tenable.com** o visite **tenable.com/contact**