Un enfoque moderno de la seguridad en el Cloud con Tufin Iris

Informe de la solución

Automatización de políticas de seguridad para entornos de cloud múltiples

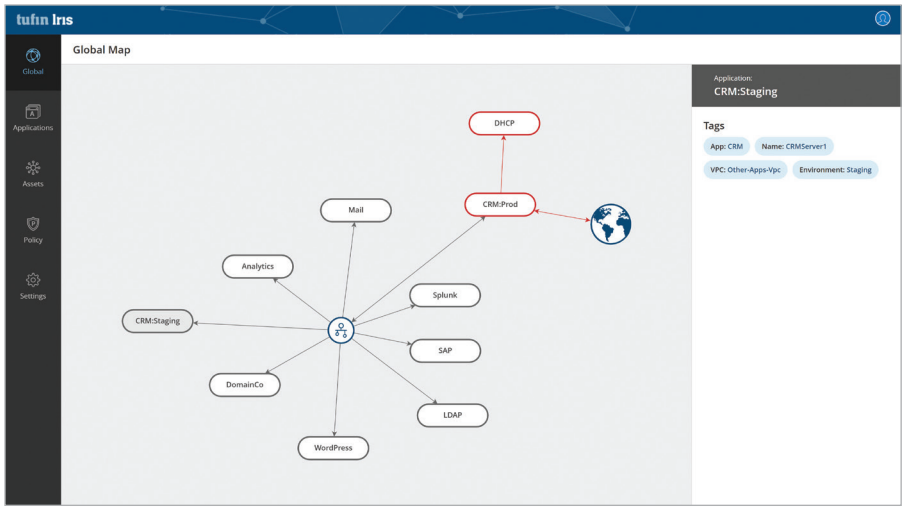
Las plataformas de cloud nativas están impulsando la transformación digital, aumentando la agilidad empresarial y acelerando la innovación. Y en el mundo del Cloud, la necesidad de proteger la información confidencial y asegurar las aplicaciones es tan importante como siempre. Esto resulta cada vez más difícil, ya que los desarrolladores utilizan diversos proveedores de cloud y las aplicaciones se implementan con más frecuencia. Para mantener el rápido ritmo de los cambios, los equipos de seguridad de IT y operaciones en el cloud se precisa nuevas soluciones nativas de cloud para proteger las aplicaciones indispensables. Las soluciones de seguridad heredadas se diseñaron para proteger la infraestructura física y sus equivalentes virtuales. Tufin Iris permite que los equipos de seguridad y operaciones de IT recuperen la visibilidad y controlen las políticas de seguridad en el Cloud, con el impulso de la automatización que se integra con los procesos de DevOps.

Los desafíos

Las herramientas de seguridad tradicionales protegen las aplicaciones al permitir o denegar el acceso según direcciones IP y puertos. En un entorno nativo de cloud, las direcciones IP son altamente transitorias y, por tanto, se suele acceder a los servicios por el nombre, en lugar de la dirección. Además, las políticas de control de acceso se definen mediante una combinación de grupos de seguridad y roles de Administración de Identidades y Acceso (IAM, por sus siglas en inglés) Como resultado, se necesitan nuevas soluciones para proporcionar a la seguridad de IT la visibilidad, el control y la automatización necesarios para proteger el negocio y garantizar el cumplimiento normativo.

Recuperación de la visibilidad

Un solo entorno en el Cloud puede contener cientos, y posiblemente miles, de recursos activos. Debido a su distribución en varias cuentas y proveedores de cloud, puede ser difícil saber qué aplicaciones se implementan y si cumplen con la política de seguridad. Tufin Iris controla de forma inteligente la nube y detecta y muestra todas las aplicaciones en un mapa sencillo de utilizar. Esto ayuda a los equipos de seguridad de IT y de operaciones en el cloud a identificar rápidamente los recursos en riesgo o que no cumplen con la normativa, por lo que precisan atención inmediata.



Principales características y ventajas:

- Obtención de visibilidad de la configuración de seguridad del Cloud público
- Garantía de cumplimiento normativo continuo y de generación de alertas
- Reducción de la complejidad de las políticas mediante protecciones de seguridad
- Políticas de microsegmentación para un control de acceso minucioso
- Solución sin agente entregada como servicio
- Integración con la cadena de herramientas DevOps
- ***Regístrese (en línea) para obtener su cuenta gratuita en: tufin.io***

Acerca de Tufin

Oficinas: Norteamérica, EMEA y Asia-Pacífico

Clientes: Más de 2100 en más de 50 países

Principales mercados verticales: Empresas de finanzas, telecomunicaciones, energía y servicios públicos, sanidad, comercios minoristas, educación, gobierno, fabricación y transporte

Partners: Más de 150 partners activos en todo el mundo

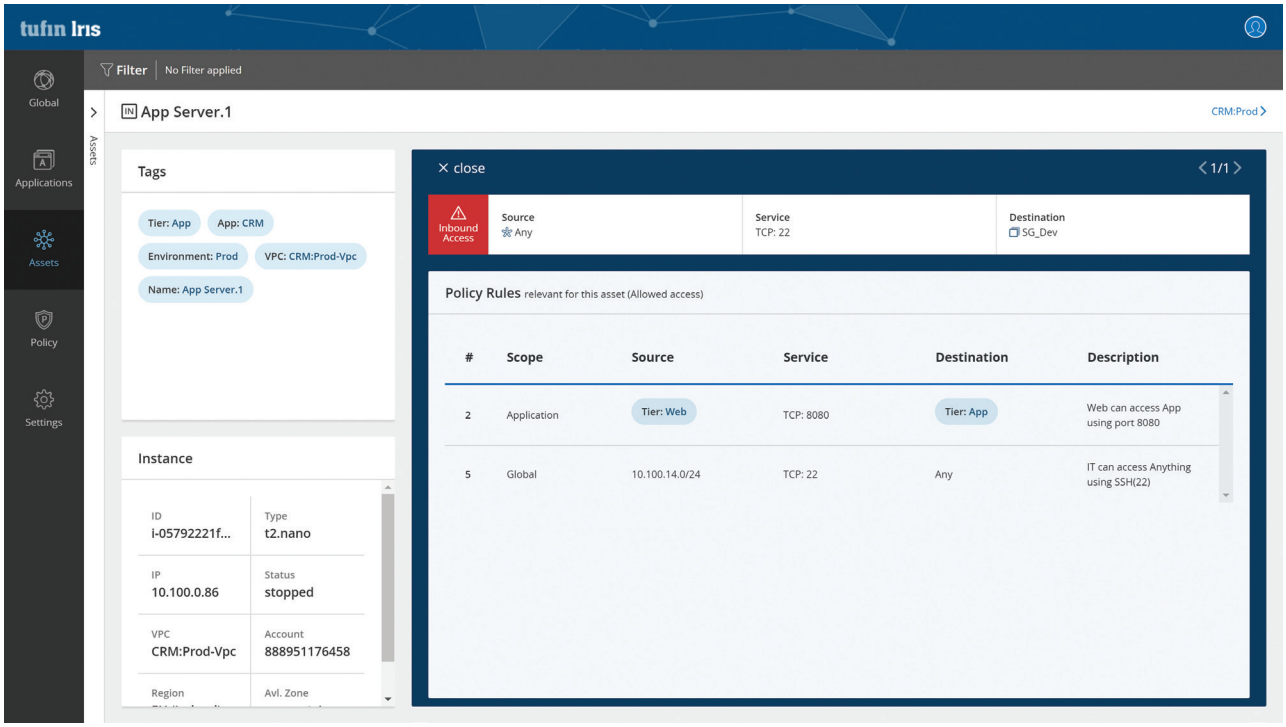
Socios tecnológicos y plataformas compatibles: Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Forcepoint, Juniper Networks, Microsoft Azure, OpenStack, Palo Alto Networks y VMware, entre otros

Azure

amazon web services

Continuidad del cumplimiento normativo

Mediante Tufin Iris, los equipos de seguridad pueden definir fácilmente políticas de seguridad basadas en los requisitos del sector, normativos o empresariales. Para proteger las aplicaciones sin aumentar la complejidad o causar un "sobredimensionamiento de las reglas", el departamento de IT puede establecer protecciones de seguridad que pueden aplicarse de forma global o a un grupo general de recursos. Por ejemplo, una medida podría comprobar que no se puede acceder al almacenamiento de datos desde Internet. Para realizar un control detallado, el departamento de IT puede definir políticas de microsegmentación que limitan de forma sólida el acceso para proteger los recursos críticos, como la restricción del acceso a un servicio que procesa registros privados de clientes.



Automatización de la seguridad

La seguridad en el Cloud mejora mediante la prevención de aplicación temprana, a menudo denominada "desplazamiento hacia la izquierda". En lugar de contar con un acceso directo final programado para la revisión de políticas de seguridad, las revisiones de seguridad se integran desde el comienzo del ciclo de vida del desarrollo y en cada uno de los pasos. Tufin Iris se integra en sus procesos de DevOps a través de herramientas CI/CD comunes como Jenkins para identificar riesgos y verificar el cumplimiento normativo antes de comenzar la producción.

Prueba gratuita

Descubra cómo Tufin Iris puede ayudarle a proteger su entorno de nubes múltiples.
Regístrese (en línea) para obtener su cuenta gratuita: tufin.io

tufin
www.tufin.com

Copyright © 2019 Tufin
Tufin, Unified Security Policy, Tufin Orchestration Suite y el logo de Tufin son marcas registradas de Tufin. Todos los demás nombres de productos aquí mencionados son marcas o marcas registradas de sus respectivos propietarios.

SB-01-19

tufin Iris