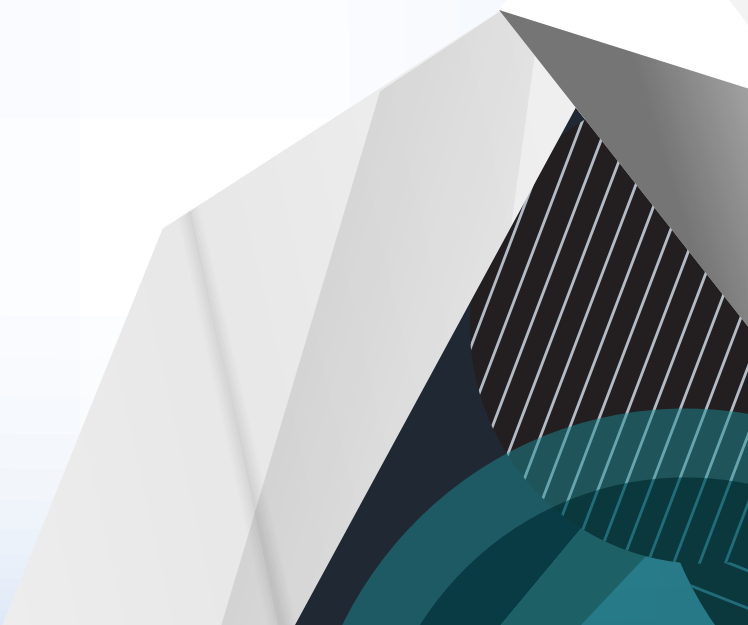
FIREEYE™

INFORME TÉCNICO

Orquestación de microsegmentación y seguridad para obtener una defensa inexpugnable en la nube



Índice

La nube está bajo ataque

Muchas empresas, desde las pequeñas hasta las multinacionales, modernizan sus entornos informáticos con un cambio a nubes públicas y privadas. El centrarse en el cliente, la agilidad empresarial y la reducción de costos son los principales impulsores de esta transformación de la infraestructura. Pero los centros de datos y las arquitecturas basadas en la nube están siendo atacadas, al igual que los centros de datos y las infraestructuras convencionales. Ambos entornos son vulnerables a las amenazas que se desplazan lateralmente.

Consideraciones sobre la solución

Configuración de controles y visibilidad

Para limitar el impacto potencial de las amenazas, su organización debe identificar los riesgos potenciales de malware y acabar con los mismos rápidamente. Esto requiere una visibilidad confiable y consistente de todos los aspectos de su entorno. Para la nube, esto puede ser difícil, ya que el 37 % de los participantes en una encuesta informó que la "falta de visibilidad de la seguridad de la infraestructura" es su "mayor preocupación en la nube".

Los dispositivos de perímetro de red convencionales y las estrategias de seguridad de red tradicionales tienen menos probabilidades de tener éxito en entornos de nube. Una vez que se sobrepase el firewall, hay poco que se pueda hacer para detener a los atacantes.

Todos los principales proveedores de la nube ofrecen controles integrados que permiten la toma de decisiones de seguridad antes de que el tráfico llegue a las cargas de trabajo. Por el contrario, las defensas perimetrales basadas en sistemas operativos tradicionales se encuentran dentro de la zona de ataque, lo que conlleva un mayor riesgo, ya que las decisiones de seguridad no se toman hasta que el flujo de datos llega a la máquina virtual. El enfoque granular, a nivel de carga de trabajo y de elaboración de listas blancas de los controles nativos de la nube debe configurarse explícitamente antes de que los datos puedan entrar o salir de una carga de trabajo, instancia o contenedor. Las configuraciones con controles de acceso con menor nivel de privilegios son esenciales para una seguridad exitosa.

Configuración incorrecta y gestión deficiente de los controles de seguridad

Se debe considerar cuidadosamente la propiedad y el funcionamiento de los controles de seguridad nativos de la nube. Al principio, los equipos de Desarrollo y Operaciones (*Development and Operations*, DevOps) del proveedor de la nube pueden codificar los controles de seguridad en sus scripts de orquestación, pero la escalabilidad puede convertirse en un problema:

- Es posible que los equipos de seguridad no tengan la visibilidad ni la comprensión de los controles que se han implementado, incluso con respecto a la consola del proveedor de la nube.
- Los equipos de DevOps pueden utilizar configuraciones genéricas para controles complejos que tienen como resultado demasiado acceso y representan un mayor riesgo para la empresa.
- A pesar de que la nube es un entorno explícitamente incluido en la lista blanca, los equipos de DevOps pueden, con frecuencia, realizar una configuración incorrecta con muy poco acceso.
- La gestión y el control limitados con respecto a la configuración de seguridad significa que el equipo de DevOps debe participar continuamente en las actualizaciones de la configuración a medida que aumentan las cargas de trabajo.
- El desarrollo y la implementación son lentos porque los equipos de seguridad no cuentan con una manera sencilla de ajustar las políticas existentes en múltiples aplicaciones sin codificación ni scripting complejos.

"Las amenazas específicas avanzadas eluden la protección tradicional basada en firmas y perímetro, lo que crea la necesidad de que los controles de seguridad se vuelvan automatizables y adaptables".

Fuente: Gartner

CONTROLES DE SEGURIDAD NATIVOS EN LA NUBE:
"La posición de Gartner sobre la seguridad de la nube ha sido clara: los servicios de nube pública ofrecidos por los principales proveedores de la nube son seguros. Utilice los controles de seguridad nativos del proveedor de IaaS".

"Aprovechar estos controles nos permitió migrar de una red segura de cargas de trabajo a una red de cargas de trabajo seguras".

— Vicepresidente sénior de Infraestructura.

"Hasta el 2020, el 80 % de las brechas en la nube se deberá a una configuración incorrecta y a una gestión deficiente, no a vulnerabilidades de los proveedores".

Fuente: Gartner

Planificación de la nube dinámica y elástica

La gestión de políticas de seguridad puede volverse compleja, imprecisa e ineficiente en cualquier entorno que involucre una nube, ya que las cargas de trabajo se desplazan, cambian y escalan con frecuencia.

Los equipos de DevOps pueden intentar aprender los controles de diferentes proveedores y diseñar scripts para responder a los requisitos cambiantes, pero esto puede provocar retrasos en la implementación y generar riesgos internos e inquietudes de auditoría.

Un diseño de seguridad sólido requiere un plan que incluya:

- **Visibilidad mejorada:** visualización de toda la infraestructura y sus controles de seguridad para identificar rápidamente los riesgos ambientales y confirmar la implementación correcta de la política.
- **Orquestación y automatización de la seguridad:** aprovisionamiento y desaprovisionamiento automático de controles específicos para reducir los problemas de configuración incorrecta y acelerar las operaciones.
- **Microsegmentación:** manera automática de proporcionar políticas precisas y granulares para máquinas virtuales y contenedores, según la función de la carga de trabajo.
- **Supervisión y gestión corporativa:** mecanismo para hacer un seguimiento del estado de seguridad e identificar riesgos y amenazas potenciales.
- **Adquirir versus desarrollar:** solución confiable disponible comercialmente para cumplir con los requisitos.

Los detalles de un enfoque moderno de seguridad de la nube

En el informe "How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center" (Cómo hacer que las cargas de trabajo de la nube IaaS sean más seguras que su propio centro de datos), realizado por Gartner en junio de 2016, se sugiere lo siguiente:

1. Utilice los controles de seguridad nativos del proveedor de IaaS junto con las prácticas de automatización y de DevOps.
2. Microsegmento de manera predeterminada: migre de una "red segura de cargas de trabajo" a una "red de cargas de trabajo seguras".
3. Los altos niveles de automatización reducen considerablemente la configuración incorrecta y la gestión deficiente, lo que reduce la superficie de ataque, mejorando en gran medida la seguridad.
4. Registre todo y requiera visibilidad persistente: no puede proteger lo que no tiene a la vista.

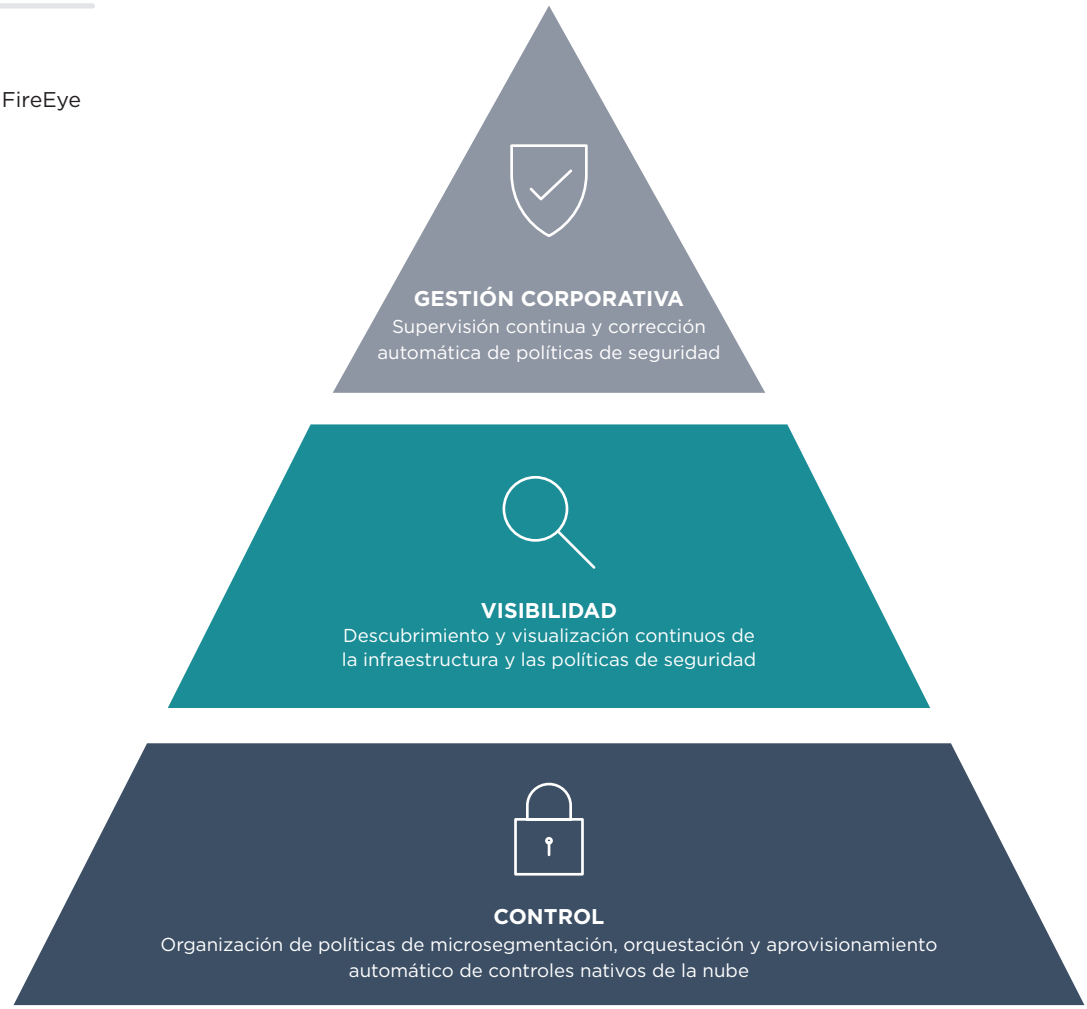
Aprovechar correctamente los controles nativos de la nube junto con la microsegmentación da como resultado cargas de trabajo que están mejor protegidas que en los centros de datos tradicionales

Cloudvisory: La solución integral

La gestión y la orquestación potentes y centralizadas de la seguridad de la nube que utilizan los controles nativos de la nube del proveedor están disponibles a través de FireEye Cloudvisory.

Figura 1.

Elementos de FireEye Cloudvisory.



Cloudvisory funciona en AWS, Azure, GCP, Kubernetes, OpenStack y entornos sin sistema operativo, lo que le permite a su organización acelerar el negocio, adaptarse a cambios dinámicos y reducir el riesgo de una brecha de seguridad.

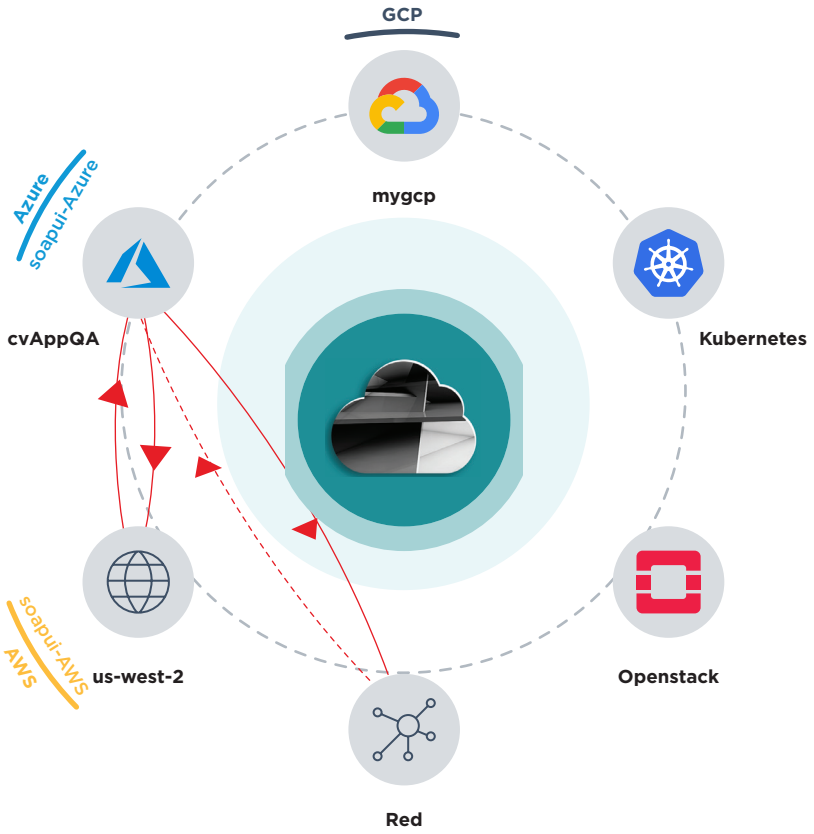
Visibilidad nativa de la nube

Para gestionar, aprovisionar y remediar la seguridad de la carga de trabajo, Cloudvisory descubre de forma continua la infraestructura nativa de la nube y los objetos de seguridad de cada proveedor de la nube, además de definirlos visualmente. Por ejemplo, en AWS esto incluye cuentas, regiones, nubes privadas virtuales (*Virtual Private Clouds*, VPC), cargas de trabajo, grupos de seguridad y los flujos de datos de la red de cargas de trabajo internas. En OpenStack, esto incluye cuentas, regiones, proyectos, cargas de trabajo, grupos de seguridad y flujos de datos.

Los flujos de datos se asignan en tiempo real, se comparan con los controles de seguridad implementados y se diferencian claramente como compatibles o no compatibles para ver el estado del entorno de la aplicación subyacente.

Figura 2.

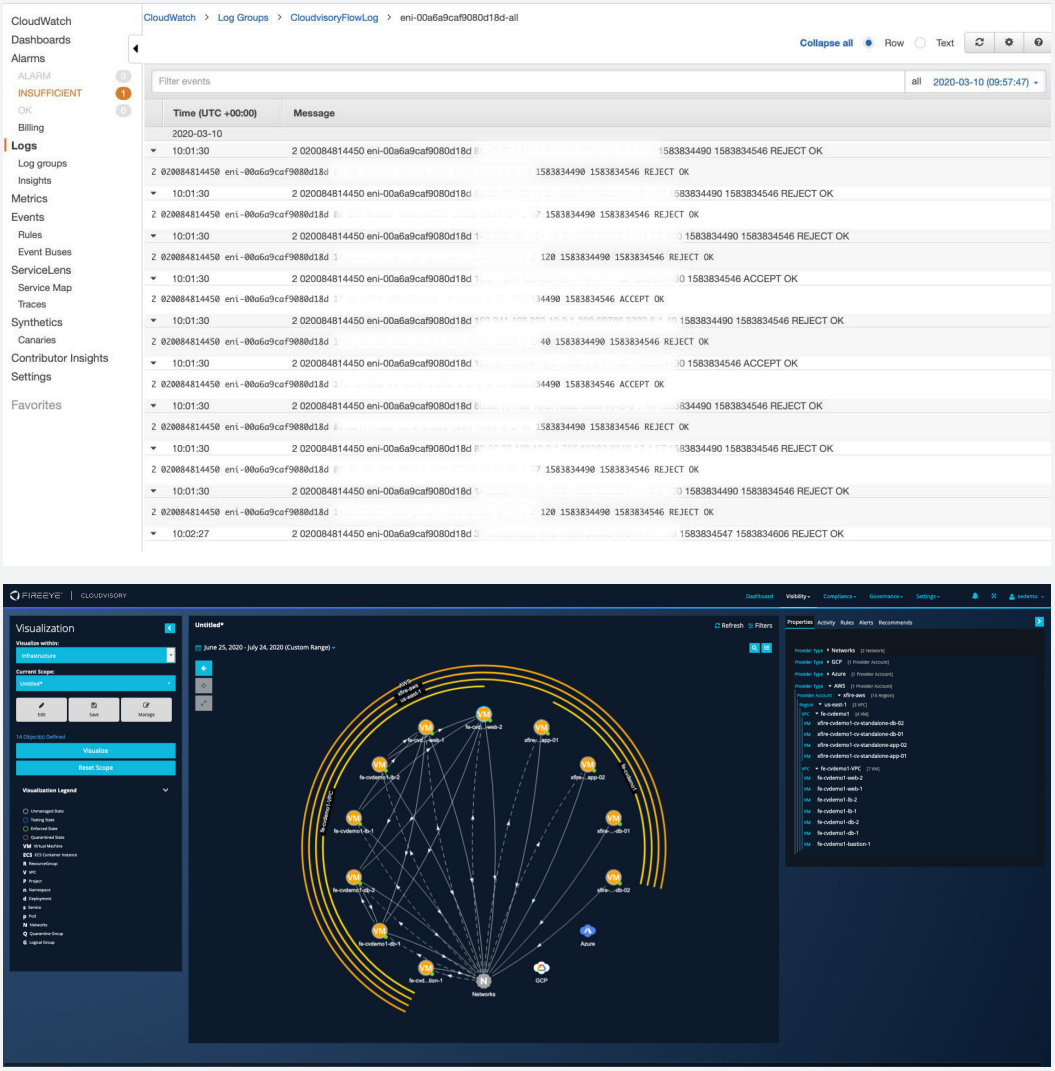
Visualización de Cloudvisory de un entorno híbrido que incluye AWS, Azure, GCP, OpenStack, Kubernetes y un centro de datos tradicional.



Cloudvisory puede actualizar las asignaciones visuales a medida que los activos se desplazan entre los entornos (de desarrollo a producción) o entre proveedores (centro de datos a AWS), o si el propio entorno cambia. Los equipos de DevOps pueden validar la política en un modo de prueba, que no bloquea los flujos de datos.

Figura 3.

Una lista típica de flujos de VPC en AWS (arriba) se puede visualizar con mucha más claridad en Cloudvisory (abajo). El comportamiento incompatible, como los ataques, se puede ver, alertar y poner en cuarentena fácilmente.



Control nativo de la nube

Para crear, organizar y administrar políticas de seguridad para entornos con una o más nubes, la solución ideal:

- Ofrece microsegmentación inteligente y granular
- Simplifica la creación de políticas mediante controles de seguridad nativos de la nube
- Identifica las políticas con configuración incorrecta y ayuda a corregirlas
- Organiza controles de políticas para una seguridad constante, repetible e inmutable en entornos dinámicos
- Automatiza el aprovisionamiento y desaprovisionamiento precisos de políticas en los proveedores

Límites de los enfoques de microsegmentación tradicionales

Las soluciones tradicionales de microsegmentación tienden a ser muy invasivas e inflexibles y no admiten controles nativos de seguridad de la nube. Su dependencia en el sistema operativo o en firewalls en línea coloca el punto de la gestión corporativa de la seguridad dentro de la zona de ataque donde el malware puede poner en riesgo tanto a las cargas de trabajo como a los controles de seguridad. Los firewalls en línea aumentan la complejidad de la configuración de la nube y los problemas de escalabilidad.

La falta de controles nativos obliga a los clientes a configurar manualmente todos los controles de seguridad del proveedor de la nube. Estos proveedores de seguridad no supervisan los puntos de gestión corporativa nativos de la nube, lo que aumenta el riesgo organizacional. Los cambios fraudulentos o accidentales pueden exponer los entornos a los hackers e interrumpir las aplicaciones activas.

Microsegmentación inteligente

Es totalmente posible migrar a una microsegmentación de cargas de trabajo, microservicios y contenedores. Hay varias razones para aspirar a una red de cargas de trabajo seguras de este tipo e implementarla:

- Los procesos actuales de DevOps suelen crear políticas de seguridad incorrectas o demasiado amplias para las cargas de trabajo.
- Demasiado acceso aumenta en gran medida el riesgo de malware y de perpetradores patrocinados por un estado nación.
- El malware que puede desplazarse de manera lateral con facilidad en el entorno eventualmente encontrará objetivos de datos enriquecidos.
- Los perpetradores fraudulentos pueden verse frustrados y bloqueados por las políticas de microsegmentación.

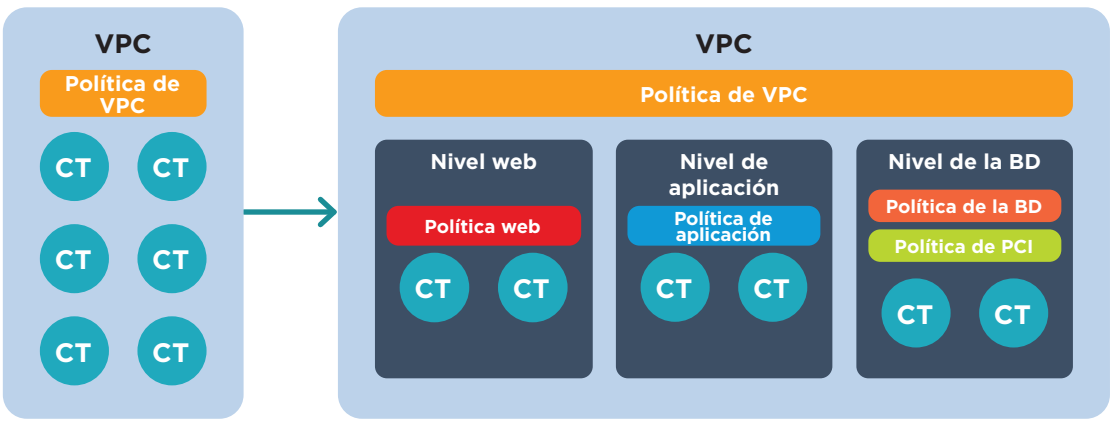
Si se gestiona correctamente, la microsegmentación puede fortalecer la seguridad y poner fin a las amenazas de hackers laterales al aislar grupos de cargas de trabajo más pequeños y discretos.

Elaboración de listas blancas

En la nube, las cargas de trabajo no pueden recibir comunicaciones hasta que se configuran los controles nativos de la nube. Las políticas de elaboración de listas blancas permiten la entrada y salida específicas y granulares, así como las reglas de puerto y protocolo que brindan de manera eficaz un firewall a nivel de la carga de trabajo (Figura 4). Este tipo de seguridad de la carga de trabajo frustra a los hackers y detiene la migración de malware dentro del entorno. Por lo tanto, Cloudvisory habilita las políticas de elaboración de listas blancas automatizando la microsegmentación de la información a través de la gestión de políticas y la infraestructura organizacional.

Figura 4.

Antes y después de la elaboración de listas blancas.



Organizar y orquestar políticas de seguridad

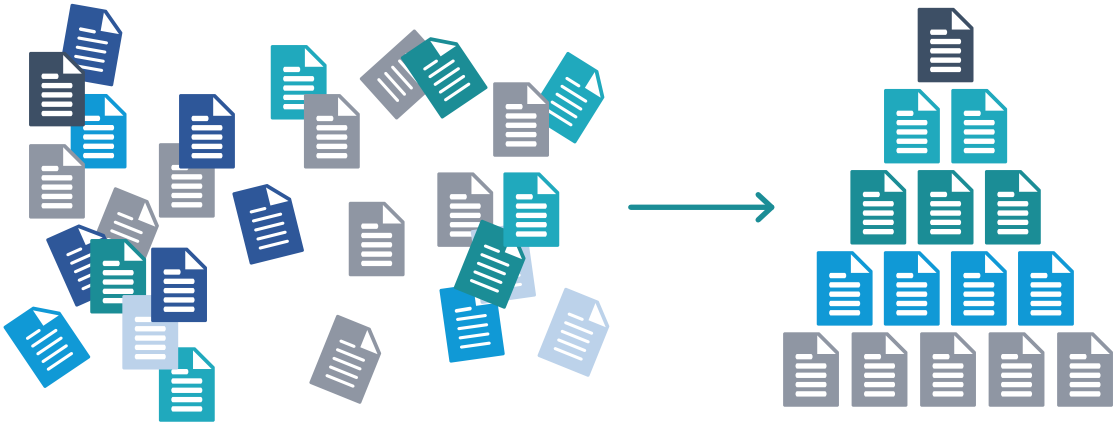
El poder y la escala para operaciones seguras en la nube dependen en gran medida de la organización y orquestación de políticas microsegmentadas.

Cloudvisory puede responder automáticamente a los cambios dinámicos en el entorno y ajustar las políticas de seguridad nativas de la nube para mantener protegidas las cargas de trabajo. Para organizar y gestionar políticas rápidamente, Cloudvisory permite:

- Descubrimiento automático y agrupación de cargas de trabajo según el contexto
- Creación automatizada de políticas, que se utilizan de manera flexible con las cargas de trabajo a través de grupos lógicos

Figura 5.

Visualización de autodescubrimiento y agrupación de cargas de trabajo en función de su contexto.



Descubrimiento automático del contexto de la carga de trabajo

Las definiciones de políticas se asocian en última instancia con las cargas de trabajo según el contexto de la carga de trabajo, que se determina mediante la membresía de grupos lógicos e incluye variables como:

- Proveedor de la nube
- Membresía de la infraestructura
  - Cuenta
  - Región
  - Grupo de recursos, VPC, proyecto
- Aplicación
  - Nivel de aplicaciones
- Requisitos de gestión corporativa tales como
  - CIS, GDPR, HIPAA, NIST, PCI, lista de verificación de seguridad de OpenStack y más
- Prácticamente cualquier agrupación lógica o ad hoc necesaria para gestionar la política

Una capacidad de descubrimiento continuo permite a Cloudvisory descubrir el contexto de una carga de trabajo y agrupar automáticamente las cargas de trabajo con contextos comunes.

Establecimiento y gestión de políticas

Cloudvisory permite dos formas de crear políticas. Ambos métodos son más simples y precisos que escribir código utilizando herramientas de orquestación disponibles comercialmente.

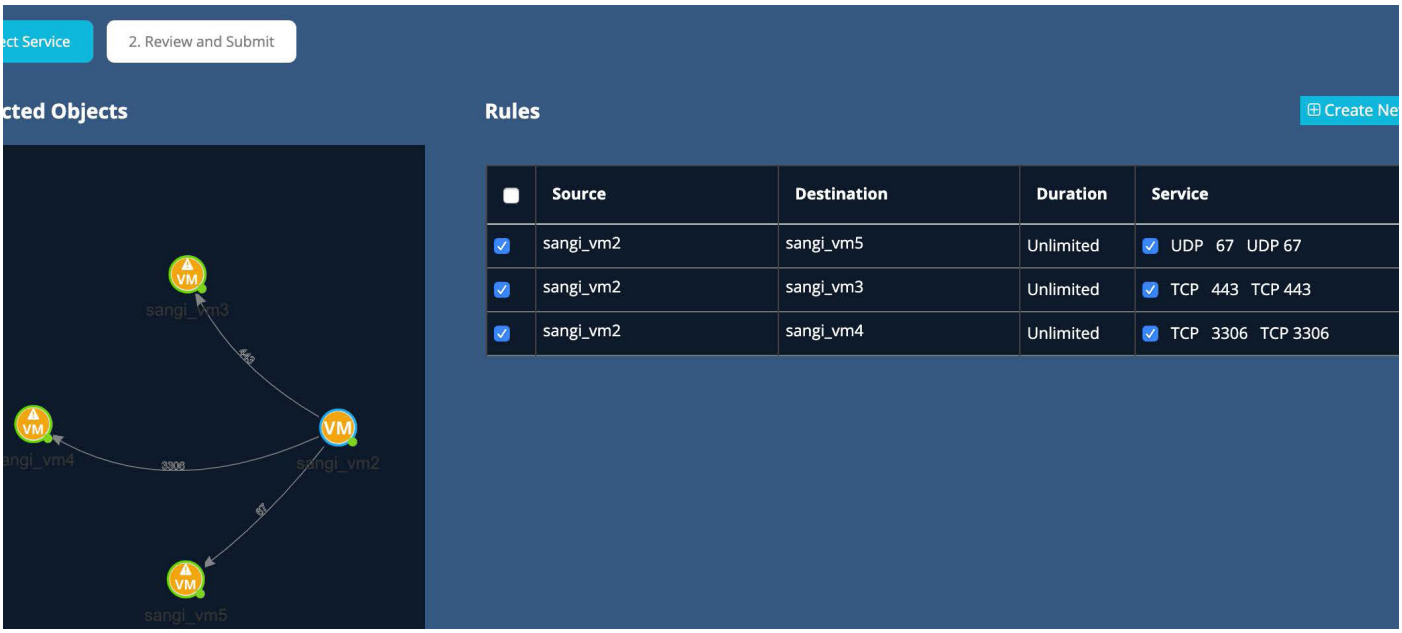
Creación de la interfaz de apuntar y hacer clic

Los usuarios de Cloudvisory no están obligados a ser expertos en los controles de ningún proveedor de la nube en particular. Al hacer clic en una secuencia de pantallas guiadas, los equipos de DevOps pueden crear reglas de políticas generales portátiles.

Descubrimiento de políticas

A menudo, los desarrolladores no están seguros de las reglas exactas que se necesitan para controlar una aplicación. Como resultado, se puede implementar demasiado acceso, lo que aumenta el riesgo para el entorno. Cloudvisory es una de las formas más rápidas de establecer un control de la política con menor nivel de privilegios. Puede descubrir los flujos exactos necesarios para ejecutar una aplicación y utilizar esa información para crear reglas de políticas portátiles y reutilizables.

Figura 6. Pantalla de creación de políticas de descubrimiento de Cloudvisory.



Independientemente de cómo se establezcan las políticas, Cloudvisory traduce las definiciones de políticas en controles nativos de la nube para cualquier proveedor de la nube. Considere una definición de política de PCI que determina qué instancias virtuales pueden comunicarse con la infraestructura de PCI en el centro de datos. Cloudvisory puede traducir esta definición en los distintos controles de proveedores, como los grupos de seguridad de AWS, los grupos de seguridad de red de Azure y los grupos de seguridad de OpenStack. Los parámetros de red dinámicos, como las direcciones IP de los servidores o migrar una aplicación a diferentes servidores, son gestionados automáticamente por Cloudvisory. Estas capacidades liberan a los equipos de DevOps de tener que convertirse en expertos en el conjunto de control de cada proveedor y reducen los requisitos de codificación.

Orquestación automática

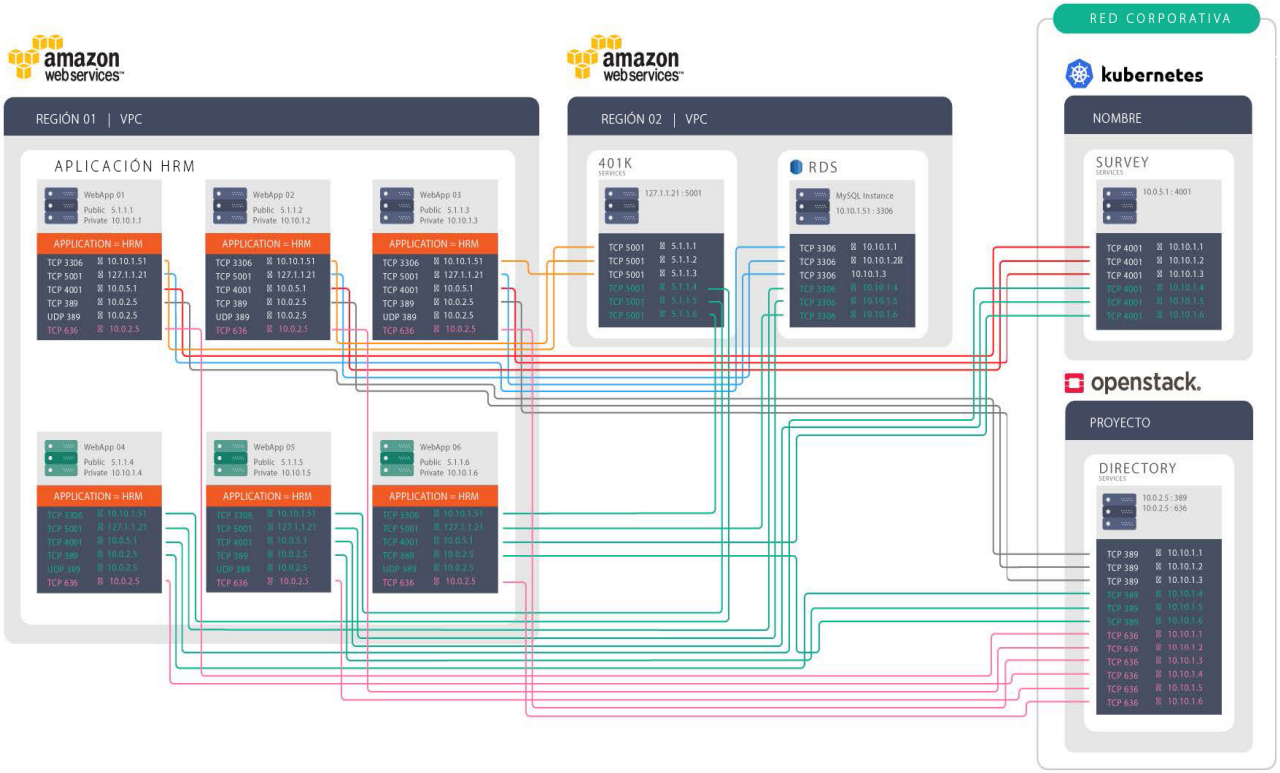
Una vez que Cloudvisory ha establecido los conjuntos de reglas de las políticas, estos se utilizan de manera flexible con el contexto de una carga de trabajo mediante una API o una interfaz de apuntar y hacer clic. Luego las políticas se pueden aprovisionar automática y correctamente a las cargas de trabajo, incluso cuando surgen nuevas, cambian las funciones o migran entre entornos, proveedores u otros grupos lógicos. En todos los casos, Cloudvisory identifica automáticamente los cambios en el contexto y actualiza las políticas de seguridad en tiempo real. No se requiere codificación ni scripting complejo, lo que significa un mayor control de seguridad y una gestión de políticas más precisa.

Gestión rápida de cambios de políticas

Un ejemplo de nube híbrida compleja (Figura 7) que incluye activos de AWS, Azure y OpenStack puede ayudar a ilustrar el poder de Cloudvisory.

En primer lugar, la definición de la política de gestión de recursos humanos establecida por Cloudvisory para la aplicación especifica las reglas de entrada y salida de seguridad para cualquier carga de trabajo que contenga los metadatos “app=HRM”. A medida que surgen cargas de trabajo adicionales con estos metadatos, Cloudvisory calcula y aprovisiona los controles nativos de la nube correctos para cada servicio que forma parte de la aplicación HRM integrada. Al realizar un seguimiento de todas las conexiones necesarias, en última instancia, Cloudvisory aprovisiona políticas precisas.

Figura 7. Nube híbrida compleja con activos en varios entornos.



Los equipos de DevOps encargados de codificar estas políticas o realizar el scripting de las mismas deben realizar un seguimiento de la inmensa complejidad en todos los entornos, direcciones IP públicas y privadas, puertos y protocolos de entrada y salida. Esto lleva un tiempo considerable y puede dar lugar a configuraciones incorrectas y aplicaciones que no funcionan. Cloudvisory automatiza todo el proceso, lo que elimina la complejidad asociada con el aprendizaje, la organización, el aprovisionamiento, el cálculo, la actualización y la gestión de la política de seguridad nativa de la nube. Esto no solo requiere menos tiempo y reduce costos, sino que también brinda una seguridad más consistente y precisa.

Gestión corporativa a través de la supervisión

Una vez que las políticas se organizaron, establecieron y aprovisionaron, los entornos se deben supervisar para detectar posibles vulneraciones y verificar la seguridad inmutable.

Al utilizar la IU de Cloudvisory o sus API, los equipos comerciales, operativos y de seguridad pueden visualizar el tráfico de datos en diferentes niveles de la jerarquía de la infraestructura. Por ejemplo, el usuario puede observar el tráfico de datos entre máquinas virtuales en el mismo hipervisor, diferentes proveedores de la nube, entre la nube y los activos del centro de datos tradicional o en una sola cuenta en la nube. A diferencia de los recopiladores de flujo de redes tradicionales disponibles en conmutadores y enrutadores, los flujos de datos se capturan, almacenan y muestran con información contextual, como proveedor, propiedades de infraestructura, aplicación y atributos definidos por el usuario. Este contexto transmite información que ayuda a comprender el comportamiento de las aplicaciones, solucionar problemas de políticas con configuración incorrecta, analizar y clasificar rápidamente los incidentes de seguridad y simplificar el procesamiento de análisis de datos.

Después del descubrimiento de la infraestructura y el establecimiento de políticas, Cloudvisory supervisa continuamente dos áreas críticas:

- Flujos de datos y recuentos de bytes de cualquier carga de trabajo gestionada
- Puntos de gestión corporativa de políticas nativas para cada carga de trabajo

Violaciones en el flujo de datos

Los flujos de datos se comparan con las políticas implementadas y compatibles. Cualquier flujo de datos que no coincida con las políticas permitidas se marca inmediatamente, se etiqueta como incompatible, se bloquea y se indica claramente en la IU.

Las alertas son configurables y una carga de trabajo infectada se puede poner en cuarentena inmediatamente para neutralizar cualquier amenaza potencial.

Por ejemplo, si una carga de trabajo no está permitida para FTP y está infectada con malware que intenta salir de la carga de trabajo por FTP, Cloudvisory puede detectar el intento de flujo de datos (y cualquier aumento correspondiente en el recuento de bytes promedio) y alertar sobre esta actividad.

La alerta se muestra en el panel de control que se envía como notificaciones por correo electrónico a los administradores y se integra con las soluciones SIEM. El intento de comunicación se bloquea. Cloudvisory se puede configurar para poner la carga de trabajo infectada en cuarentena inmediatamente, suspender todas las políticas de seguridad salientes actuales y bloquear todo el tráfico de red hacia y desde cargas de trabajo seleccionadas. Esto evita el desplazamiento lateral de las amenazas a otras aplicaciones y recursos y cualquier otra infección de red, hasta que los equipos de investigación forense puedan corregir la situación.

Las alertas de tráfico incompatible debido a políticas con configuración incorrecta pueden provocar un mal funcionamiento de la aplicación. Los administradores pueden descubrir rápidamente cualquier brecha en las reglas de la política y resolverlas mediante la interfaz de apuntar y hacer clic de Cloudvisory.

Gestión automática de las violaciones

Cloudvisory comprueba continuamente la configuración de los controles de seguridad nativos establecidos para asegurarse de que siguen en cumplimiento. Si se detecta un cambio no autorizado en las reglas de seguridad nativas, Cloudvisory genera alertas. Las políticas de seguridad se pueden configurar para revertir automáticamente los cambios incompatibles. En este caso, cualquier cambio no autorizado en los controles de seguridad nativos se revierte automáticamente, lo que hace que la gestión corporativa de las políticas vuelva a un estado de cumplimiento. En tales casos, también genera una alerta y una entrada de registro de auditoría para registrar el evento que no está en cumplimiento.

Por ejemplo, si un administrador que usa una consola de Azure elimina accidentalmente las reglas del grupo de seguridad para el acceso al puerto 80, muchos proveedores de la nube no alertarán este cambio. Sin embargo, el resultado sería una aplicación inactiva, ya que no podría contactar con la interfaz web de la aplicación.

Cloudvisory detectaría tales cambios de configuración accidentales o maliciosos y puede revertir inmediatamente el cambio para devolver el entorno a un estado compatible y funcional. Esto reduce o elimina el tiempo de inactividad y la priorización y el riesgo automatizados.

Resumen

Todas las organizaciones, de todos los tamaños y niveles de complejidad, adoptan inexorablemente las nubes públicas y privadas. Para garantizar que la seguridad se mantenga al día con las prácticas operativas, deben mantener la visibilidad de todas las posibles superficies de ataque, configurar la seguridad correctamente incluso a medida que la organización evoluciona y desarrollar diseños de seguridad sólidos que contemplen una nube dinámica y elástica.

Los elementos de dichos planes incluyen orquestación y automatización para una operación más rápida y sin errores, microsegmentación para implementar políticas centradas en la carga de trabajo, supervisión y gestión corporativa para identificar riesgos y amenazas de manera rápida y selección de soluciones disponibles comercialmente para cumplir con los requisitos.

FireEye Cloudvisory es una solución única que satisface todas las necesidades esenciales de seguridad multinube, desde la visibilidad y la gestión de políticas hasta la potencia y la facilidad de uso, para entornos públicos, privados e híbridos.

Para obtener más información sobre FireEye, visite: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Acerca de FireEye, Inc.

FireEye es una empresa de seguridad basada en inteligencia de amenazas. FireEye, que funciona como una extensión escalable y flexible de las operaciones de seguridad del cliente, ofrece una plataforma integral que combina tecnologías innovadoras de seguridad, información sobre amenazas a nivel de estado-nación y los servicios de consultoría de Mandiant® de fama mundial. Gracias a este método, FireEye elimina la complejidad y la carga de la ciberseguridad para las organizaciones que desean estar preparadas y responder a los ataques cibernéticos, además de prevenirlos.

FIREEYE™