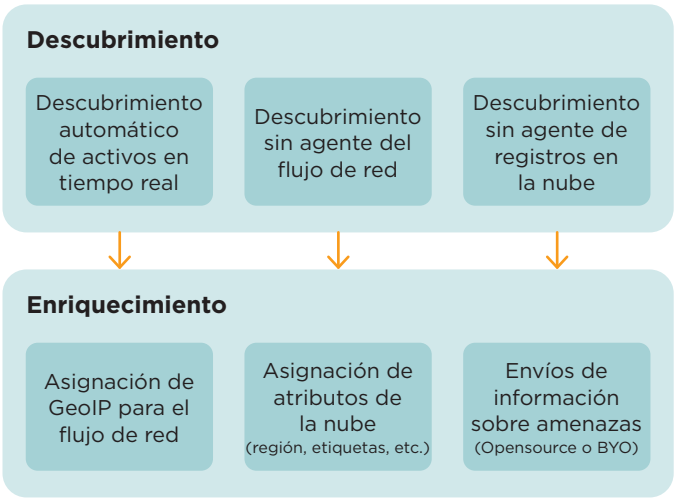
FIREEYE™

FICHA TÉCNICA

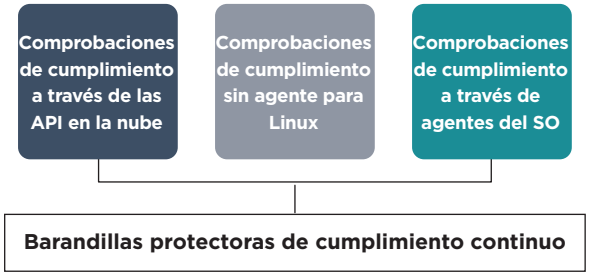
Cloudvisory

Seguridad integral multinube de la carga de trabajo a través de una visibilidad profunda, cumplimiento continuo y gestión corporativa inteligente



Cumplimiento

Supervisión automática del cumplimiento de seguridad con más de 1300 comprobaciones integradas. Gestión corporativa de mejores prácticas, marcos y políticas personalizadas tales como CIS, GDPR, HIPAA, NIST, PCI DSS y otros.

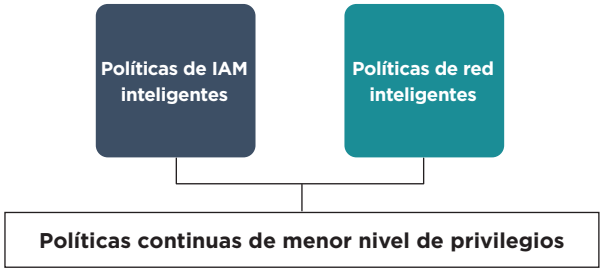


Visibilidad

Descubrimiento continuo y asignación de activos empresariales, controles de seguridad y mapeo de eventos de seguridad en nubes públicas y privadas. El aprendizaje automático aprovecha el contexto para identificar riesgos y amenazas.

Gestión corporativa

Prácticas de gestión corporativa mejoradas con inteligencia artificial. Capacidad para reducir las superficies de ataque y prevenir intrusiones aprendiendo, probando e implementando de manera eficiente políticas inteligentes de menor nivel de privilegios a cualquier escala.



Nube pública: Azure

Visibilidad

Cuentas, usuarios/grupos/funciones de IAM, regiones, grupos de recursos, servicios, suscripciones, subredes.

Cargas de trabajo descubiertas

Pods AKS, servicios de aplicaciones, entornos de servicio de aplicaciones, Cosmos, cuentas de bases de datos, zonas DNS, funciones, equilibradores de carga, memorias caché de Redis, clústeres de Service Fabric, cuentas de almacenamiento, máquinas virtuales y más...

Nube pública: AWS

Visibilidad

Cuentas, usuarios/grupos/funciones de IAM, regiones, servicios, subredes, VPC.

Cargas de trabajo descubiertas

Instancias EC2, sistemas de archivos EFS, pods EKS, equilibradores de carga elásticos, transmisiones Kineses, funciones Lambda, puertas de enlace NAT, clústeres RDS, zonas alojadas Route53, depósitos de S3, temas SNS y más...

Nube privada: OpenStack

Visibilidad

Clústeres, instancias, Keystone, red, proyectos (usuarios), servicios de regiones.

Descubra, analice y gestione grupos de seguridad de red para instancias OpenStack (Nova) y pods Kubernetes. Supervise los flujos de red para detectar amenazas casi en tiempo real.

Nube privada: Kubernetes

Visibilidad

Clústeres, implementaciones, usuarios/grupos/funciones de identidad, espacios de nombres, redes, pods.

Centro de datos tradicional

Sistemas operativos

- Ubuntu Linux
- Redhat
- CentOS

Integraciones de automatización

Sistemas externos (de terceros)

Alertas configurables y automatizadas, análisis histórico de eventos de seguridad (como SIEM, Elasticsearch), análisis y generación de informes de cumplimiento basados en eventos/activados por API, recepción de registros para fuentes alternativas de eventos de seguridad (como dispositivos de red tradicionales, proveedores de identidad).

Gartner Cool Vendor 2018

Gartner nombró a Cloudvisory como "Proveedor Genial" (Cool Vendor) en Cloud Security 2018.

CIO APPLICATIONS TOP 25 AMAZON SOLUTION PROVIDERS-2017

Cloudvisory es reconocido por CIO Applications entre los 25 principales proveedores de soluciones de Amazon.

AICPA SOC

Cloudvisory-SaaS con certificación independiente SOC2.

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

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 nación-estado 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 ante los ataques cibernéticos, además de prevenirlos.

FIREEYE™