Prisma Cloud para GCP

Proteja todos los recursos en su entorno Google Cloud Platform con Prisma Cloud

Beneficios de Prisma Cloud para GCP

- Visualice todos los recursos conectados a través de su entorno GCP completo.
- Mantenga el cumplimiento continuo y genere informes fácilmente a través de todo su entorno GCP.
- Habilite la seguridad de DevOps al configurar protecciones con monitoreo de amenazas en tiempo real como configuraciones riesgosas, actividades confidenciales de usuarios, intrusiones a la red y vulnerabilidades de host.
- Utilice las capacidades de detección de anomalías para erradicar las cuentas comprometidas y las amenazas internas.
- Investigue amenazas actuales o incidentes pasados, y determine rápidamente las causas de origen.
- Reciba alertas contextuales para ayudar a su equipo a priorizar los problemas y responder rápidamente.
- Integre fácilmente servicios nativos de GCP, incluso Cloud Security Command Center.

Prisma Cloud Simplifica la Defensa De Amenazas en la Nube para GCP

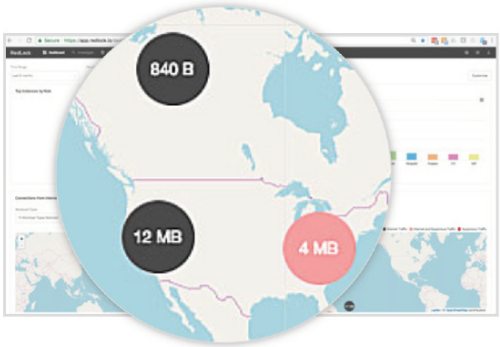
La adopción de computación en la nube pública continúa superando los avances de las defensas de ciberseguridad. La ausencia de un límite físico en las redes de Internet, el riesgo de exposición accidental por parte de usuarios sin experiencia, la visibilidad descentralizada y la naturaleza dinámica de la nube aumentan la superficie de ataque en términos de magnitud. A pesar de que los productos puntuales de seguridad pueden llegar a solucionar desafíos individuales, no son capaces de brindar una protección integral en un entorno donde los recursos cambian constantemente como en Google Cloud.

Prisma™ Cloud (anteriormente denominado RedLock) es un servicio de seguridad y cumplimiento que descubre cambios en los recursos en la nube y correlaciona continuamente las fuentes de datos sin procesar y aislados. Esto incluye las actividades de usuarios, las configuraciones de recursos, el tráfico de red, inteligencia de amenazas e informes de vulnerabilidad para proveer una visión completa de los riesgos en la nube pública. Gracias a su enfoque innovador, impulsado por el aprendizaje automático, Prisma permite a las organizaciones priorizar rápidamente los riesgos, mantener un desarrollo ágil y cumplir de manera eficaz sus obligaciones en el Modelo de Responsabilidad Compartida.

Funciones y Beneficios Clave para Proteger GCP

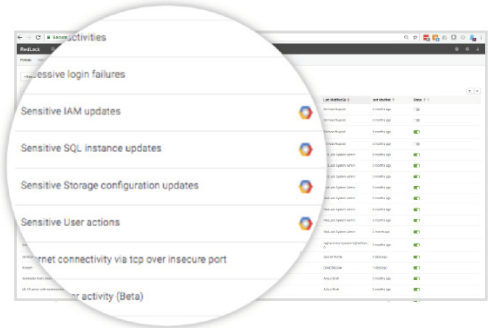
Visibilidad Incomparable

Visualice todo su entorno de Google Cloud Platform (GCP™) hasta el último componente. Prisma Cloud descubre dinámicamente recursos y aplicaciones en la nube al correlacionar continuamente las configuraciones, actividades de usuarios y datos de tráfico en la red. Combinar esta comprensión integral del entorno GCP con datos de fuentes externas, como informes de inteligencia de amenazas y escáneres de vulnerabilidades, permite a Prisma brindar un contexto completo para cada riesgo.



Cumplimiento Simplificado en la Nube

Prisma Cloud cuenta con políticas ya incorporadas acordes a las prácticas recomendadas estándares de la industria como las establecidas por CIS, GDPR, NIST, SOC 2 y PCI. También puede crear políticas personalizadas según las necesidades específicas de su organización. Prisma monitorea continuamente las violaciones a las políticas a través de todos los recursos conectados y permite realizar informes con un solo clic para auditorías simplificadas de su entorno GCP.

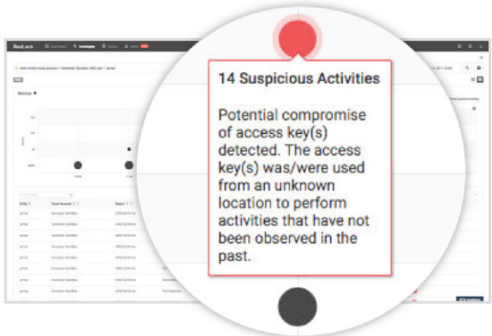


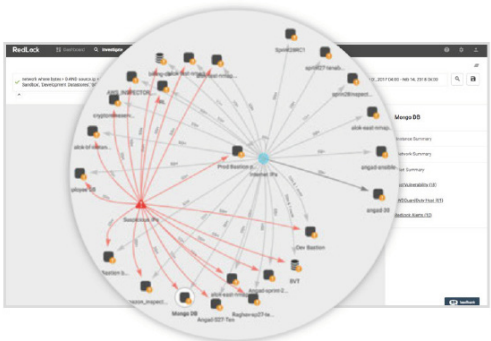
Protecciones de Políticas

Prisma Cloud le permite configurar protecciones para DevOps para mantener un desarrollo ágil sin comprometer la seguridad. Esto le permite detectar amenazas como configuraciones riesgosas, actividades confidenciales de usuarios, intrusiones en la red y vulnerabilidades de host. Prisma asigna automáticamente puntajes de riesgo por cada recurso según la gravedad de los riesgos para el negocio, las violaciones y las anomalías; así ayuda a SecOps a identificar rápidamente los recursos más riesgosos y a priorizar los esfuerzos de soluciones respectivamente.

Threat Detection

Prisma Cloud detecta anomalías automáticamente en el comportamiento de usuarios y otros a través de todo su entorno GCP; así establece bases de referencia de conductas y señala cualquier desviación. Por ejemplo, el potencial compromiso de una clave de acceso se marcará si se determina que un usuario utiliza claves de acceso en dos lugares diferentes en momentos similares que lo hacen geográficamente imposible.



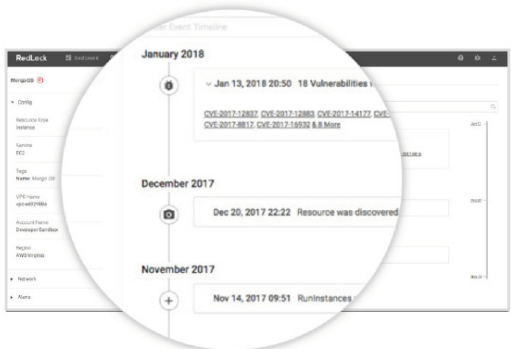


Investigación de Incidentes

Con una profunda comprensión del entorno GCP, Prisma Cloud reduce el tiempo de investigación a segundos. Puede determinar problemas rápidamente, realizar análisis de impacto anterior y posterior, y revisar el historial de cambios a un recurso para una mejor comprensión de la causa raíz de un incidente. Por ejemplo, puede ejecutar una consulta para encontrar todas las bases de datos con comunicación directa en Internet el mes pasado. En el mapa resultante se encontrarán todas estas instancias y se destacarán los recursos potencialmente comprometidos.

Alerta Contextual y Respuesta Adaptativa

Prisma Cloud posibilita que sus equipos puedan responder rápidamente a problemas en base a alertas contextuales. Estas alertas, emitidas a partir de una metodología de puntuación de riesgo con patente en trámite, proveen el contexto de todos los factores de riesgo asociados a un recurso, lo que simplifica la priorización de los problemas más importantes. Usted puede enviar alertas, orquestar las políticas o llevar a cabo reparaciones automáticas. Incluso puede enviar alertas a herramientas como Slack®, Splunk ® y nuestro propio Demisto® para solucionar problemas. En caso de una base de datos riesgosa, Prisma generará una alerta contextual con información sobre los factores de riesgo para habilitar una respuesta automática.



Integración con Cloud Security Command Center

Prisma Cloud se integra con Cloud Security Command Center de Google para proveerle visibilidad sobre los riesgos de seguridad y de cumplimiento a través de todo su entorno GCP. Esto significa que sus equipos de seguridad pueden recopilar los datos rápidamente, identificar amenazas y tomar acciones antes de que se produzcan daños o pérdidas comerciales.

Desarrollo de un Mapa de Defensa de Amenazas en la Nube para GCP

Prisma le permite desarrollar un programa de defensa de amenazas en la nube a través de todo su entorno GCP, desde la concepción hasta su plena madurez, con las siguientes capacidades:

- **Garantía de cumplimiento.** El mapeo de configuraciones de recursos en la nube con marcos de cumplimiento (como CIS, GDPR, PCI DSS y HIPAA) puede consumir mucho tiempo. Al utilizar políticas preempaquetadas, Prisma permite el monitoreo continuo, la reparación automática y la generación de informes con un clic; y, a la vez, simplifica el proceso para mantener el cumplimiento.
- **Control de seguridad.** Una visibilidad incompleta y un impreciso control de cambios en los dinámicos entornos informáticos en la nube pública pueden dificultar los procesos de control de la seguridad. Prisma habilita la validación de arquitectura al establecer protecciones de políticas para detectar y reparar automáticamente riesgos a través de las configuraciones de recursos, arquitecturas de redes y actividades de usuarios. Con Prisma, finalmente puede compatibilizar la agilidad de DevOps sin comprometer la seguridad.
- **Habilitación de SOC.** Los equipos de operaciones de seguridad están desbordados de alertas que incluyen poco contexto sobre los problemas, lo que dificulta solucionarlos oportunamente. Prisma permite identificar vulnerabilidades, detectar amenazas, investigar incidentes actuales o pasados, y solucionar problemas a través de todo su entorno GCP en minutos.

Etapa 1: Adoptar	Etapa 2: Expandir	Etapa 3: Escalar
Huella en la Nube: • Decenas de cargas de trabajo • Pocas cuentas en la nube	**Huella en la Nube:** • Cientos de cargas de trabajo • Muchas cuentas en la nube	**Huella en la Nube:** • Múltiples proveedores de nube • Miles de cargas de trabajo • Decenas de cuentas en la nube
Objetivos: • Garantía de cumplimiento • Control de seguridad	**Objetivos:** • Visibilidad central • Detección de amenazas • Gestión de vulnerabilidades **+ Objetivos de la etapa 1**	**Objetivos:** • Autoreparación • Investigación de incidentes **+ Objetivos de la etapa 1**

Figura 1: Modelo de Madurez de Defensa de Amenazas en la Nube

Prisma Cloud Security Suite

Prisma Cloud brinda visibilidad integral, detección de amenazas y rápida respuesta a través de todo su entorno de nube pública, incluso Google Cloud Platform, Amazon Web Services (AWS®) y Microsoft Azure®. Una combinación única de monitoreo continuo, garantía de cumplimiento y analítica de seguridad permite que los equipos de seguridad respondan más rápidamente a las amenazas más críticas al reemplazar las investigaciones manuales por informes, priorización y solución de amenazas automáticos. Con su enfoque basado en API, Prisma brinda una seguridad superior nativa de la nube.

Prisma Cloud es parte de la Security Operating Platform® de Palo Alto Networks y brinda a las organizaciones un enfoque multidimensional para la seguridad en la nube pública ofrecida a través de tecnologías de protección en línea, basadas en API y hosts, que trabajan juntas para reducir las oportunidades de ataque.

Security Operating Platform extiende la protección a toda su red completa, con protección integral sin importar la ubicación. Sin importar si sus aplicaciones se encuentran en sus instalaciones, fueron virtualizadas y necesitan protección en una nube privada como VMware NSX®, Cisco ACI®, KVM o OpenStack®, se extienden a una nube pública o fueron trasladadas a una aplicación SaaS, podemos protegerlas.

Visite nuestro sitio web para conocer más: www.paloaltonetworks.com.