

SDP PARA GCP

Seguridad adaptable y enfocada en la identidad para las nubes públicas

La seguridad en la nube es una responsabilidad compartida, tal como lo es con Google Cloud Platform (GCP). Los proveedores de la nube protegen la infraestructura subyacente y los clientes protegen sus datos. Este modelo presenta desafíos únicos que no se alinean con los principios de Zero Trust (confianza cero).

Zero Trust es un marco de seguridad que se funda sobre los principios de acceso menos privilegiado a los recursos de la red. Para alcanzar la confianza cero es esencial implementar un modelo de acceso centrado en la identidad. Con GCP, los equipos de seguridad deben confiar en grupos de seguridad, que son simples firewalls basados en la IP. Con ellos, los equipos de seguridad de información centrada en la identidad no necesitan controlar el acceso de los usuarios a Google Compute Engine o a los recursos de almacenamiento en la nube. Es prácticamente imposible que los equipos de seguridad controlen y amplíen el acceso utilizando direcciones estáticas de IP y asignación de puertos.

Los desafíos de seguridad de GCP

- Los entornos de nube son dinámicos, porque los servidores se crean y finalizan continuamente.
- Los usuarios tienen acceso disponible en la red corporativa.
- Los usuarios reciben atributos amplios para los servicios que operan todas las instancias dentro del entorno de nube, en lugar de recibir acceso menos privilegiado.

BENEFICIOS

Se alinea con los principios Zero Trust de acceso centrado en la identidad

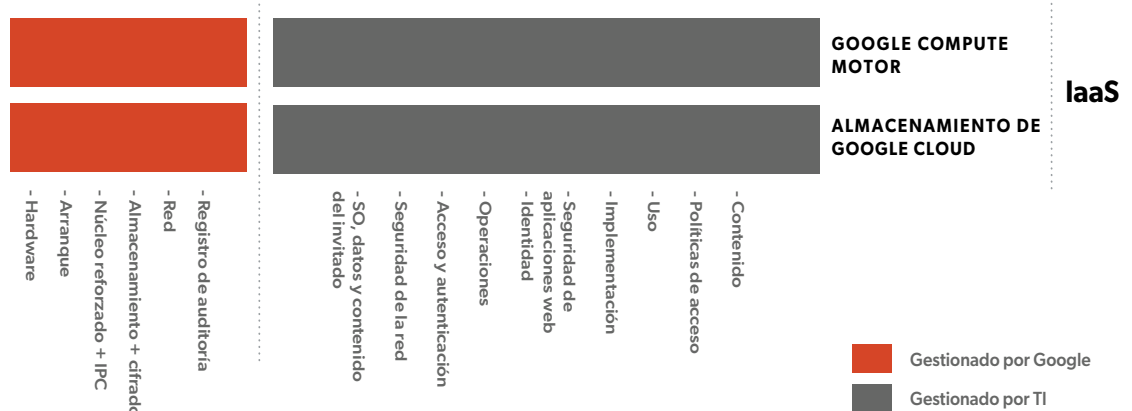
Proporciona una conexión segura y cifrada entre los usuarios y los recursos aprobados de GCP

Hace que todo el entorno de GCP sea totalmente invisible

Apoya a DevOps, porque es fácil de implementar y se adapta a instancias agregadas o eliminadas en tiempo real

Creado como la nube para la nube, de manera masiva se puede ampliar, distribuir y es resiliente

MODELO DE SEGURIDAD COMPARTIDO:
Donde termina Google y comienzan los controles de TI





Appgate SDP: seguridad adaptable y enfocada en la identidad

Appgate SDP para GCP ofrece acceso seguro a la red con menos privilegios. Crea dinámicamente un segmento de red cifrado y seguro a partir de uno personalizado para cada sesión de usuario. Simplifica el problema del acceso a la nube de los usuarios y elimina el acceso excesivo a la red.

Appgate SDP para GCP:

- se integra con AD para brindar autenticación inicial a usuarios y asignar derechos condicionales de acceso. Al momento del acceso, se vuelven a revisar las reclamaciones para asegurar que el usuario sigue cumpliendo con la política de seguridad.
- Proporciona acceso remoto centrado en la identidad con conexiones simultáneas directamente desde el dispositivo del usuario a cualquier cantidad de sitios. Las puertas de enlace de SDP no tienen estado y están creadas para aceptar varios miles de conexiones seguras de clientes (mTLS) en simultáneo. Pueden agruparse para una alta disponibilidad y una escala lineal.
- Asigna políticas a los usuarios según los roles, que incluyen cualquier cantidad de reclamaciones que se evalúan dinámicamente en tiempo real. Appgate SDP establece los derechos de acceso según los metadatos de GCP disponibles y el contexto actual.

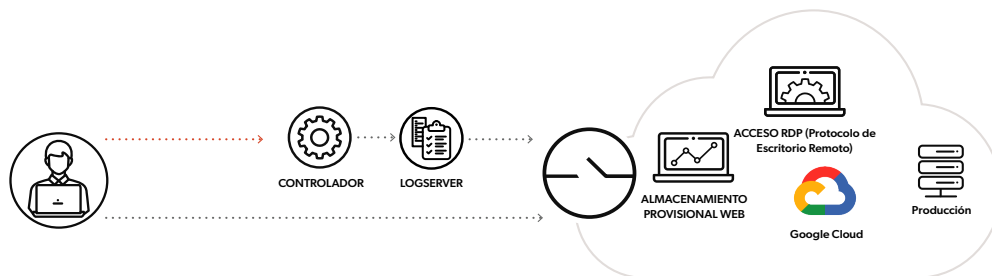
La arquitectura de Appgate SDP para GCP se distribuye, es resiliente y se adapta masivamente. Permite a las empresas implementar sistemas de acceso seguro globales y altamente disponibles en cualquier entorno híbrido con mayor control y una economía mejorada.

¿Qué es Appgate SDP?

Appgate SDP para GCP es un perímetro definido por el software, un modelo de seguridad de redes que crea dinámicamente conexiones directas de red entre los usuarios y las instancias y servicios a los cuales acceden. Appgate SDP para GCP:

- Está diseñado en torno al individuo: autenticación basada en la persona, en el entorno y en la infraestructura. Es consciente del contexto, y adapta dinámicamente la política según los cambios en el entorno, la infraestructura o la organización.
- Está creado para la nube: se distribuye y no tiene estado, creado para una arquitectura a hiper escala y de microservicios, con atributos impulsador por API.
- Se basa en el modelo de Zero Trust (confianza cero): tiene un enfoque de "primero autenticar, luego conectar", para asegurar que únicamente los usuarios autorizados puedan conectarse a través de una conexión cifrada a las instancias y recursos de la nube. Reduce la superficie de ataque y mejora significativamente la seguridad.
- Es capaz de brindar un control de acceso detallado adaptándolo automáticamente según los cambios del contexto.
- Ideado para abarcar todos los recursos de la nube, excepto los que el usuario tiene autorización para acceder. Al hacer invisibles todas las demás instancias, las empresas pueden simplificar su infraestructura de seguridad, a la vez que garantizan el acceso con confianza.

Appgate SDP ofrece un control de acceso detallado, adaptando el acceso automáticamente según los cambios en los metadatos, a la vez que oculta todos los recursos de GCP



Sobre Appgate

Appgate es la empresa de acceso seguro. Potenciamos la forma en que las personas trabajan y se conectan proporcionando soluciones diseñadas específicamente sobre los principios de seguridad Zero Trust. Este enfoque de seguridad definido por las personas permite conexiones rápidas, simples y seguras desde cualquier dispositivo y ubicación a las cargas de trabajo en cualquier infraestructura de TI en entornos híbridos, locales y en la nube. Obtenga más información en appgate.com