Google Cloud

Seguridad de las API: Estadísticas más recientes y tendencias clave

Informe de investigación 2022

Cómo la seguridad de las API afecta el ritmo de innovación en las empresas y qué hacen los líderes de TI para mitigar los riesgos.

Índice

Resumen ejecutivo

Con la creciente adopción de las experiencias digitales, el uso de interfaces de programación de aplicaciones, o API, está en ascenso. Como tales, las API representan un área significativa de vulnerabilidad para las organizaciones a nivel mundial. En el siguiente informe, se examina el panorama de las amenazas de seguridad de las API y su impacto en el ritmo de innovación. Asimismo, se profundiza en la visión mundial de los líderes de tecnología, que se relaciona con la posición y estrategia de seguridad de las API, y se ofrece una perspectiva sobre las oportunidades para mejorar el estado de seguridad de estas.

Este informe se basa en la investigación que realizó Google Cloud entre mayo y junio de 2022 entre líderes de tecnología de empresas en los Estados Unidos, con al menos 1,500 empleados, que tienen una influencia significativa o autoridad en la toma de decisiones sobre compras de soluciones de tecnología relacionadas con las iniciativas de API dentro de su organización.

En “Por qué la seguridad de las API es un elemento clave de una estrategia de API más amplia”, se explica que la posición de seguridad de las API es una creciente preocupación para los ejecutivos de TI debido a la prevalencia de amenazas, y que la mayoría de las organizaciones todavía deben mejorar su estrategia de seguridad de las API. Existe una necesidad de capacidades y medidas proactivas de seguridad, así como de soluciones de seguridad de las API de extremo a extremo como Apigee, una plataforma de administración de API de ciclo de vida completo.

El panorama de amenazas

Las amenazas abundan

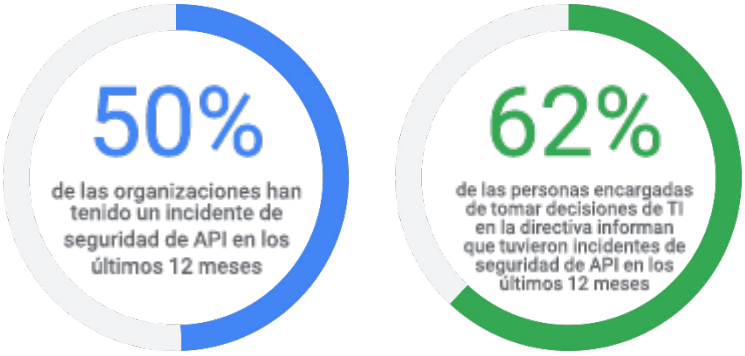
Las empresas a nivel mundial dependen de las interfaces de programación de aplicaciones, o API, para facilitar las experiencias digitales y liberar la energía potencial de sus propios datos y procesos. Las API son un vínculo esencial en la combinación de datos propietarios de las empresas con recursos de terceros. También desempeñan una función crucial en la carrera para modernizar aplicaciones, lo que alimenta la interoperabilidad y, a su vez, las funciones eficientes.

Pero la proliferación y la importancia de las API conllevan un riesgo. Como puerta de enlace a una riqueza de información y sistemas, las API se han convertido en el blanco favorito de los hackers.

Nuestra investigación confirma el amplio impacto de estas amenazas. Encuestamos a más de 500 líderes de tecnología en los Estados Unidos. La mitad de ellos afirmó haber experimentado un incidente de seguridad de API en los últimos 12 meses. Ese porcentaje es más alto o más bajo según a quién se le pregunte. El 62% de los directores indicaron que tuvieron un incidente de seguridad en los últimos 12 meses, mientras que solo el 37% de aquellos que se encuentran dos niveles por debajo de los directores dijeron lo mismo.

Esta situación podría apuntar al limitado alcance de los equipos funcionales de TI, o podría ser un indicador de lo notorio que es el problema para aquellos con mayores responsabilidades. O ambas opciones.

Incidentes de seguridad de las API



Más de tres de cinco personas encargadas de tomar decisiones en puestos directivos informan haber experimentado incidentes de seguridad de API en los últimos 12 meses.

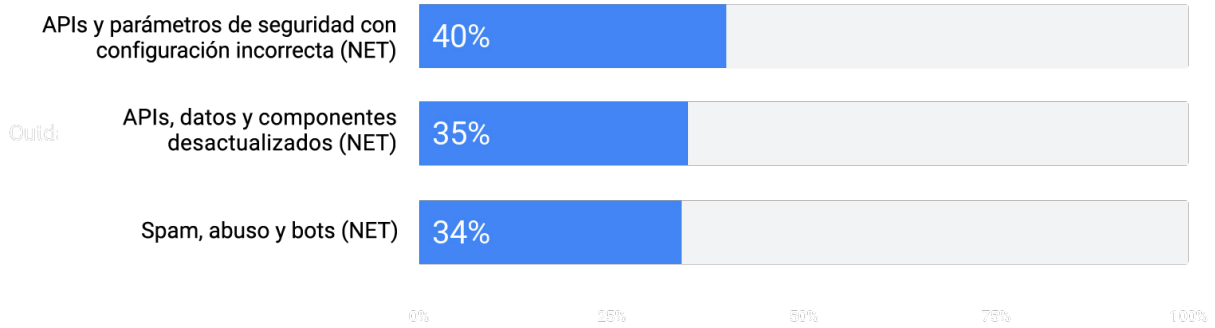
"El ritmo al que se desarrollan las APIs actualmente supera el ritmo al que nuestra organización puede garantizar la seguridad de cada una de estas APIs".

- Supervisor/gerente de TI, Servicios de hardware y software para computadoras

Para agravar el problema, las amenazas surgen de una cantidad enorme de áreas de seguridad de las API, de las que los líderes de TI deben identificar más de tres áreas en promedio. Si bien no hay un área que se destaque como una vulnerabilidad evidente, las tres fuentes más comunes de amenazas potenciales son: *configuración de seguridad incorrecta; componentes, APIs y datos desactualizados, y spam, bots y abuso.*

La configuración incorrecta, como categoría, es el área de amenazas más identificada, ya que 2 de cada 5 líderes de TI seleccionan la *configuración de seguridad incorrecta* o *la configuración de API incorrecta*.

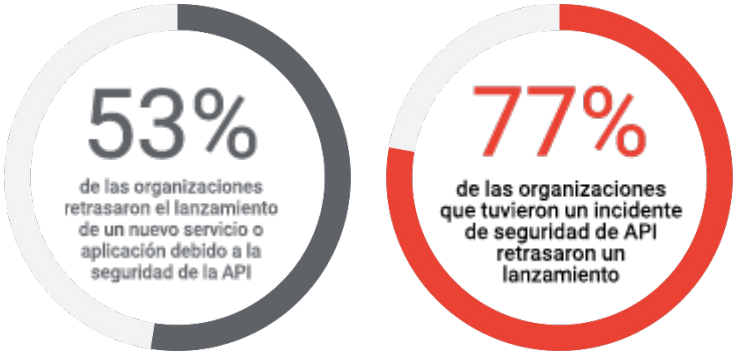
Fuentes de amenazas de seguridad de las API



Impacto en el ritmo de innovación

Estos incidentes y amenazas tienen implicaciones en el mundo real. La seguridad de las API está frenando el ritmo de innovación de muchas organizaciones. Más de la mitad (un 53%) de las organizaciones retrasaron el lanzamiento de un nuevo servicio o aplicación debido a preocupaciones de seguridad de las API. Para aquellas que experimentaron un incidente en los últimos 12 meses, más de la tercera cuarta parte (un 77%) retrasó el lanzamiento de un nuevo servicio o aplicación.

Retraso en lanzamiento de un nuevo servicio o aplicación debido a preocupaciones de seguridad de las API



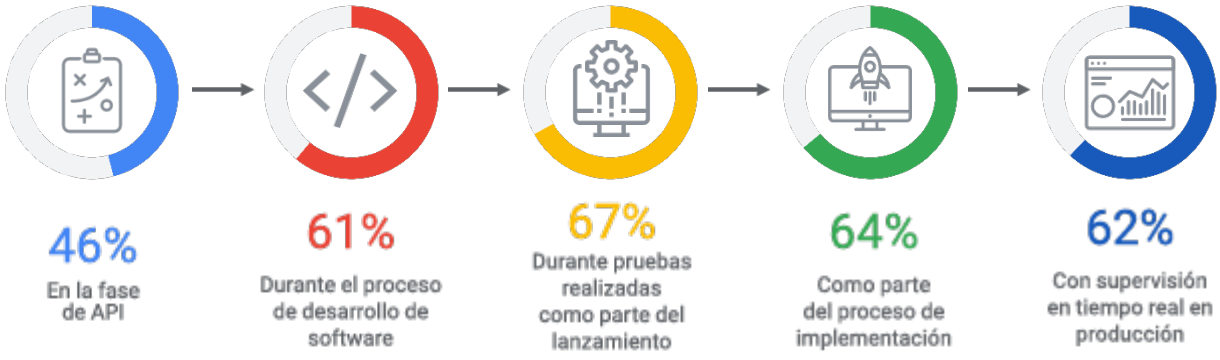
Se requiere una posición activa de seguridad de las API

Con la introducción de vulnerabilidades de seguridad provenientes de una variedad de fuentes en todo el desarrollo, no resultará sorprendente que los problemas de seguridad se identifiquen en cada fase del ciclo de vida de la API, desde el diseño y las pruebas, hasta la implementación y otras etapas. Por supuesto, los problemas de seguridad se descubren más comúnmente durante las pruebas que se realizan como parte del proceso de administración del lanzamiento (un 67%), pero una cantidad sustancial de vulnerabilidades se identifica como parte del proceso de implementación en producción (un 64%). Esto indicaba un área de riesgo para que las vulnerabilidades se implementaran en la producción, ya que un porcentaje considerable de problemas de seguridad se identifican en etapas posteriores del ciclo de vida de las API.

Los directores encuestados tenían más probabilidades de decir que las vulnerabilidades se detectan durante el proceso de desarrollo de software (un 66%) que los líderes de TI subordinados de los ejecutivos.

Evidentemente, tres de cada cinco (un 62%) líderes de TI identifican los problemas y las vulnerabilidades con supervisión en tiempo real en la producción, lo que enfatiza la necesidad de contar con una posición de seguridad activa en este entorno.

Etapa del ciclo de vida de la API en la que se identifican problemas y vulnerabilidades de seguridad



Evaluación actual

Confianza frente a las amenazas

A pesar del precario panorama de las amenazas para API, la mayoría de las organizaciones considera que tienen las herramientas y las soluciones para garantizar la seguridad de las API de extremo a extremo. De hecho, más de la tercera cuarta parte (un 77%) de los encuestados indicaron que cuentan con las herramientas y soluciones necesarias, mientras que otro 16% afirmó que cuentan parcialmente con lo requerido para implementar la seguridad de las API de extremo a extremo. Muy pocos dijeron que no tienen las herramientas necesarias.

Lo que resulta más interesante es que la mayoría de los líderes de tecnología (un 66%) calificarían su posición de seguridad como *avanzada*. Específicamente, ellos creen que cuentan con un excelente centro de seguridad de API integral y centralizado, y que sus herramientas y soluciones de seguridad no están disociadas de ninguna manera.

Algunos grupos tienen más confianza en su posición de seguridad que otros. Los siguientes califican su seguridad de las API como *avanzada*:

- Nativo de la nube (71%)
- Entorno de nube híbrida (71%)
- Ejecutivos de TI entre sus directores (71%)
- Tuvo un incidente en los últimos 12 meses (71%)

Las organizaciones nativas de la nube respondieron en la encuesta que su posición de seguridad progresó a un ritmo más acelerado, a pesar de tener más probabilidades de haber registrado un incidente y retrasado un lanzamiento el año pasado.

Posición avanzada de seguridad de las API

¿Esta confianza está mal fundada?

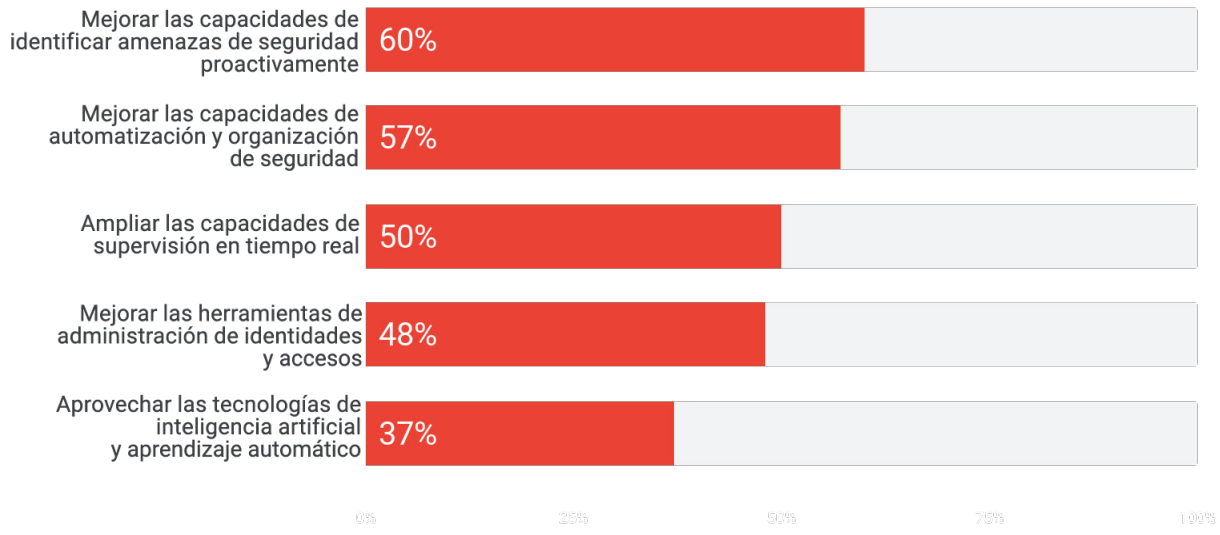
Pareciera que hay una brecha entre la existencia de los incidentes de seguridad y la confianza en que las herramientas están haciendo su trabajo. ¿Podría ser que las organizaciones están ignorando la prevalencia de los incidentes de seguridad (un 50% tuvo un incidente el año pasado), así como el impacto que la seguridad de las API tiene sobre la innovación (un 53% retrasó un lanzamiento el año pasado)? ¿O es simplemente que se aceptan los incidentes de seguridad como un costo de hacer negocios en el espacio digital?

Los hechos se sitúan en algún punto entre estas dos preguntas. Algunas organizaciones podrían estar subestimando las amenazas y el punto hasta el cual estas las afectan, a la vez que son realistas en cuanto a que la seguridad de las API cambia constantemente y que las amenazas son parte de la vida.

Las empresas priorizan ser proactivas con la seguridad de las API

Para estar en la vanguardia en temas de amenazas de seguridad, muchas organizaciones buscan soluciones que les permitan ser proactivas, a la vez que minimizan la carga de sus equipos de seguridad. De acuerdo con nuestra investigación, las capacidades que identifican de manera proactiva las amenazas de seguridad (un 60%) y mejoran la automatización (un 57%) se encuentran en el primer puesto de las listas de deseos de la mayoría de los líderes de TI para el próximo año. Sin embargo, la mayoría aún no están listas o dispuestas a priorizar dar el salto que implica incorporar inteligencia artificial o aprendizaje automático en su seguridad de las API.

Prioridades de las tecnologías para la seguridad de las API



Oportunidades

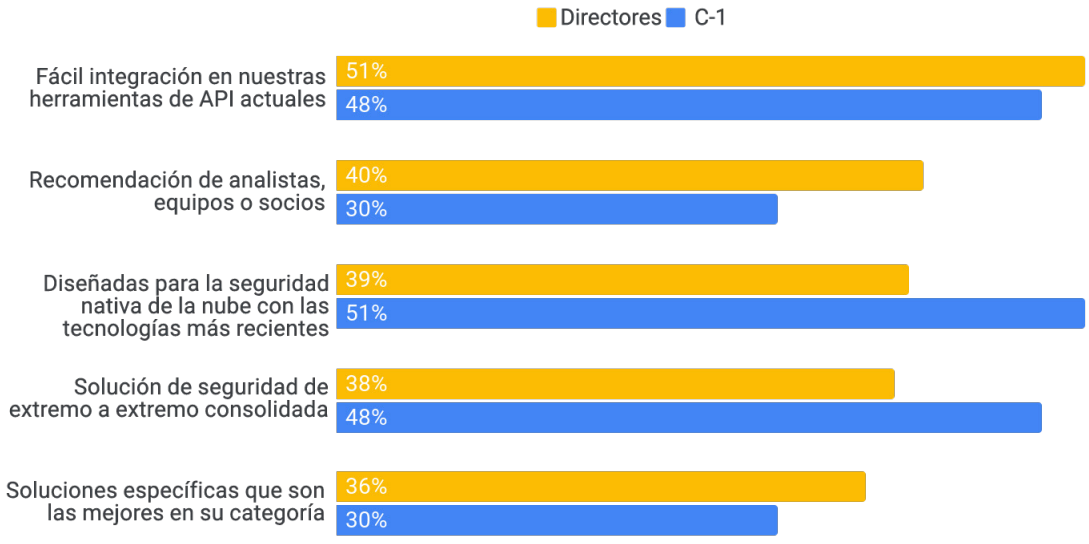
Se requiere consolidación, supervisión de extremo a extremo y vigilancia

Entonces, ¿qué buscan los líderes de TI en una solución de seguridad de las API ante un panorama de amenazas constantes y una letanía de vulnerabilidades para considerar cada etapa del ciclo de vida de la API?

Aparte de los factores que son casi esenciales, como la integración sencilla en herramientas existentes y la compatibilidad con las tecnologías más recientes, la consolidación y las soluciones de extremo a extremo son algunos de los factores más importantes que se buscan cuando se evalúan soluciones de seguridad de las APIs. Esto se aplica en particular a aquellos subordinados de los directores (C-1). Si bien los propios directores se enfocan más en la fácil integración en las herramientas de API existentes, el nivel inferior a ellos también busca una solución que tenga gran cobertura.

Cuando se evalúan las soluciones de seguridad de las API, los directores tienden a valorar las recomendaciones de terceros más que las de C-1, mientras que este último nivel valora las soluciones que se diseñan para la seguridad nativa de la nube con las tecnologías más recientes. Además, un porcentaje considerablemente más alto de C-1 prefieren soluciones consolidadas de seguridad de las API en comparación con las soluciones específicas.

Factores usados a fin de evaluar las soluciones de seguridad para API (5 principales)



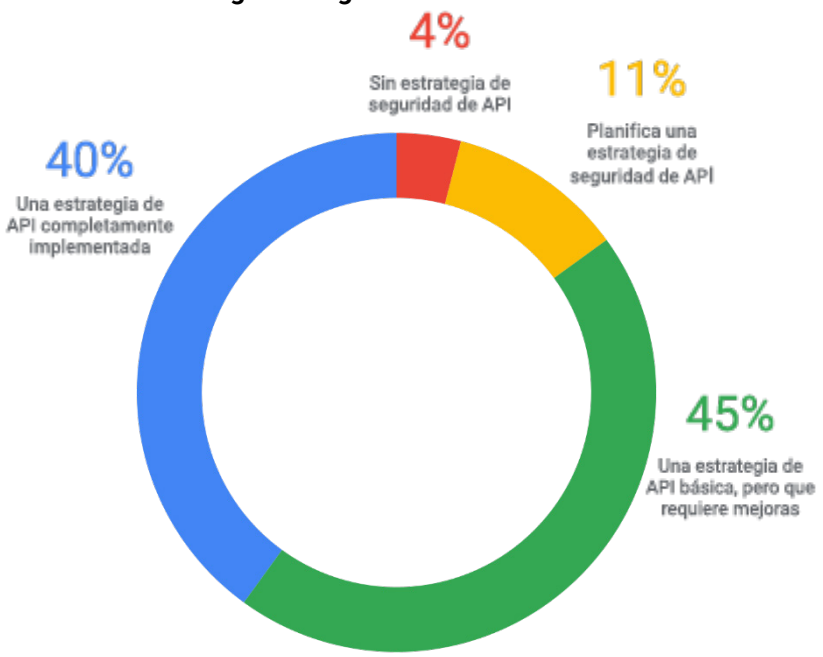
Se requiere más capacitaciones y certificaciones en este espacio

Además de las soluciones tecnológicas, muchas organizaciones ven la capacitación y las mejoras procedimentales como un medio para combatir las amenazas. Las prioridades principales de la seguridad para API incluyen establecer un estándar de aprendizaje y certificación sobre seguridad de API (un 38%), mejorar su documentación para incorporar prácticas recomendadas sobre seguridad (un 38%) y modificar los procesos existentes a fin de detectar problemas de seguridad y vulnerabilidad de API (un 37%). Pero los líderes de TI tienden a adoptar un enfoque de aceptación para mejorar su seguridad de API sin una sola iniciativa que destaque de otras.

La mayoría acepta que su estrategia requiere mejoras

Según nuestra investigación, la mayoría de las organizaciones no tienen una estrategia de seguridad de API completa implementada. Una mayoría (un 60%) diría que su estrategia debe mejorar como mínimo.

Estado de la estrategia de seguridad de API



60% de las organizaciones indican que su estrategia de API requiere mejoras

Al igual que en otras áreas de seguridad, hay una ligera desconexión entre las percepciones de los líderes de TI en la dirección y aquellos que son sus subordinados (C-1). En este caso, el 53% de los directores diría que su estrategia de seguridad de API debe mejorar. Esa cifra aumenta al 61% para quienes son subordinados de los directores (C-1) y a 69% entre aquellos que se encuentran dos niveles más abajo (C-2).

La estrategia de seguridad para API requiere mejoras

La estrategia de seguridad de las API no siempre es la prioridad principal

Si bien muchas organizaciones carecen de los recursos y la experiencia para establecer una estrategia integral, los líderes de TI de esas organizaciones, a menudo, sienten como si la seguridad de las API no se priorizara. Esto puede conllevar ciertas incomodidades en los rangos del equipo de seguridad.

Incluso en el caso de aquellos con un plan, es probable que tengan soluciones de seguridad de API repartidas por toda su organización con responsabilidades, por lo general, divididas entre equipos. De hecho, las responsabilidades de seguridad de las API con frecuencia varían entre empresas, según las necesidades, la industria y la estructura de estas.

> "El vicepresidente no lo ve como una prioridad dentro del presupuesto".
>
> - Supervisor/gerente de TI, Servicios financieros

> No tenemos una estrategia "debido a la falta de información y liderazgo organizacional".
>
> - Director/vicepresidente de TI, Cuidado de la salud

El impacto de la administración de las API y las soluciones de puerta de enlace de las API

Más de la tercera cuarta parte (un 78%) de las organizaciones indican que tienen una solución de solución de administración de APIs y de puerta de enlace de APIs implementada en toda la organización.

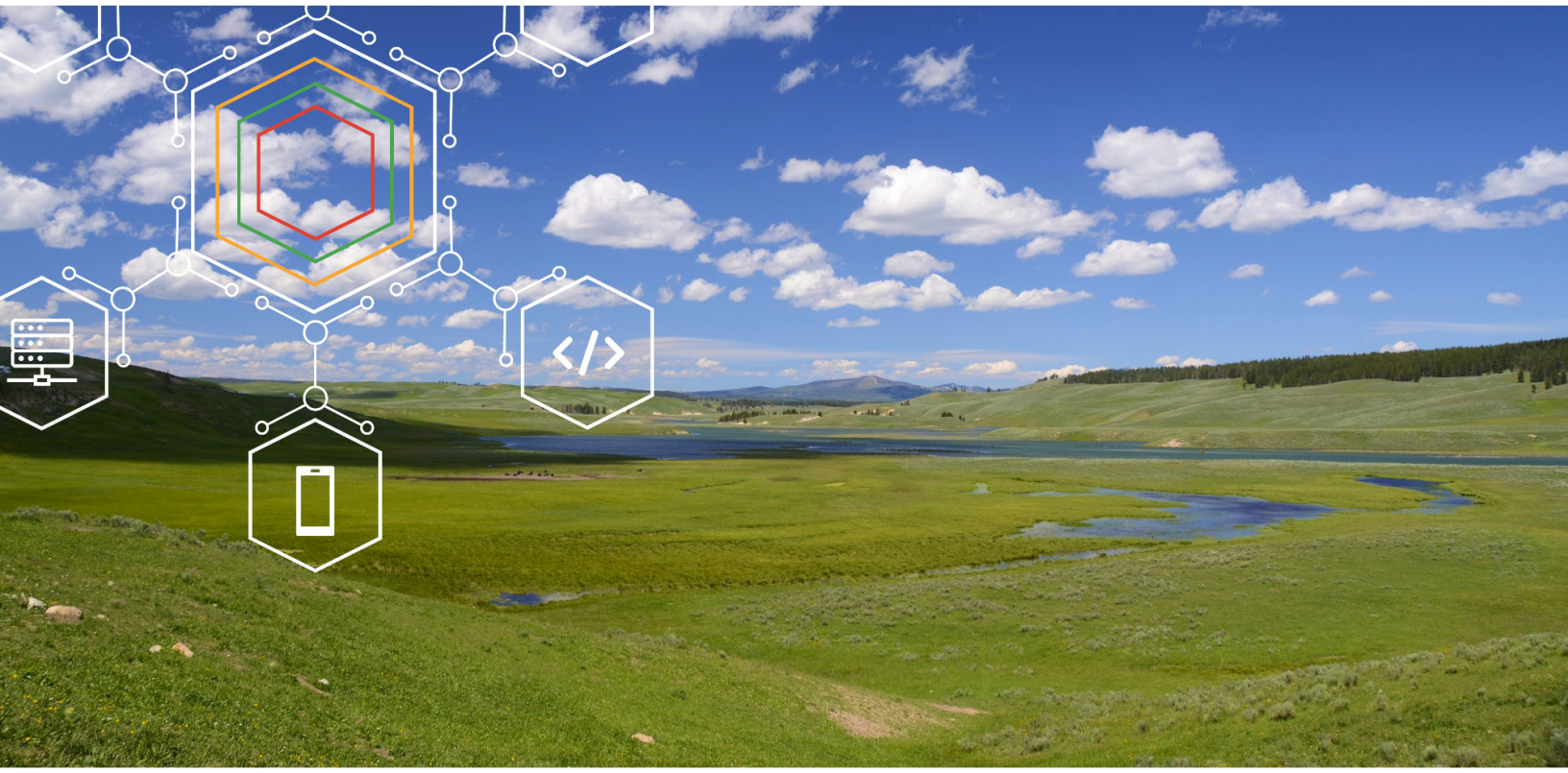
Estas organizaciones tienen menos probabilidades de creer que su estrategia de seguridad requiere mejoras (un 52%), pero es más probable que tengan un centro de excelencia de seguridad de las API integral y centralizado (un 74%) y también que consideren que tienen las herramientas y soluciones necesarias implementadas a fin de garantizar la seguridad de las API de extremo a extremo (un 91%).

Empresas con soluciones de administración de API en toda la organización (APIM) implementadas

La seguridad de las API es un elemento clave de una estrategia de API más amplia

Los ataques a las API son comunes, pero los incidentes no tienen que serlo.

Las soluciones de extremo a extremo les permiten a las organizaciones identificar y proteger las áreas de seguridad de las API vulnerables como la configuración incorrecta y las API, los datos y los componentes desactualizados. Y mientras las soluciones específicas pueden entregar una solución segmentada, queda claro que, debido a la amplitud de los ataques en el ciclo de vida de la API y la variedad de vulnerabilidades, una solución integral ofrece la mejor posibilidad de evitar bloqueos de innovación y retrasos. Las necesidades de seguridad de las API de largo plazo deben priorizarse como parte de un plan de administración de API más grande y, cuando sea posible, de una estrategia de API de toda la organización.



Acerca de la plataforma de administración de API de Apigee

La plataforma de administración de API de Apigee de Google Cloud brinda administración del ciclo de vida de API completo para ayudar a las empresas a aprovechar el valor de los datos y a entregar aplicaciones modernas y experiencias digitales de forma segura. Apigee ofrece un conjunto enriquecido de capacidades para permitirles a las empresas obtener control y visibilidad sobre el tráfico de API, lo que incluye poder automatizar la solución y corrección de problemas, y generar estadísticas a partir del uso de las API.

¿Deseas obtener más información?
Visita cloud.google.com/apigee o escríbenos directamente a apigee@google.com.

Google Cloud