CEQUENCE

FICHA DE DATO

Seguridad de API de Cequence

Plataforma de protección de aplicaciones, APIs e IA

El mundo actual, impulsado por el software, funciona con aplicaciones conectadas mediante APIs. Estas APIs brindan acceso a las aplicaciones y a los datos sensibles de una organización y se han convertido en uno de los principales objetivos de los atacantes. Las organizaciones necesitan visibilidad y control de su huella de APIs como parte de un programa de seguridad sólido. La rápida proliferación de APIs ha expuesto una amplia gama de desafíos de seguridad que pueden derivar en pérdida de datos, incumplimientos normativos y fraude:

- APIs ocultas, desactualizadas y de terceros no gestionadas (Shadow APIs)
- Exposición de datos confidenciales o sensibles
- Errores de codificación que permiten escalación de privilegios
- Abuso de la lógica empresarial

Estos desafíos requieren una solución especializada que pueda descubrir e inventariar APIs nuevas y existentes, evaluar su cumplimiento con normativas y especificaciones aplicables, y protegerlas a lo largo de todo su ciclo de vida, desde el desarrollo hasta la producción.

Seguridad de API de Cequence de un Vistazo

- **Descubrimiento completo de APIs** mediante integración con la infraestructura y/o sensores en línea y escaneo de dominios
- **Enmascaramiento de datos sensibles,** detección de exposición y prevención de fugas.
- **Visibilidad continua de riesgos,** identificando errores de codificación y configuraciones incorrectas.
- **Pruebas de seguridad de API integradas** en preproducción y en tiempo de ejecución.
- **Protección de aplicaciones y APIs** para prevenir la pérdida de datos, el robo y el fraude.

Visión General de la Seguridad de API

Cequence descubre, monitorea y prueba APIs, evaluando una amplia gama de riesgos que a menudo derivan en problemas de cumplimiento o gobernanza, pérdida de datos e interrupciones del negocio. Al proporcionar visibilidad completa y monitoreo de APIs internas, externas y de terceros, Cequence ayuda a las organizaciones a mantener el ritmo de los cambios en APIs y servicios, revela exposiciones de datos sensibles e identifica vulnerabilidades y riesgos de seguridad del OWASP API Security Top 10. Las pruebas de seguridad de API son un componente central de API Security, lo que permite a las organizaciones probar sus APIs de preproducción y en tiempo de ejecución contra las especificaciones —y generarlas automáticamente si no están disponibles. API Security puede implementarse como SaaS, en las instalaciones o en un modelo híbrido.

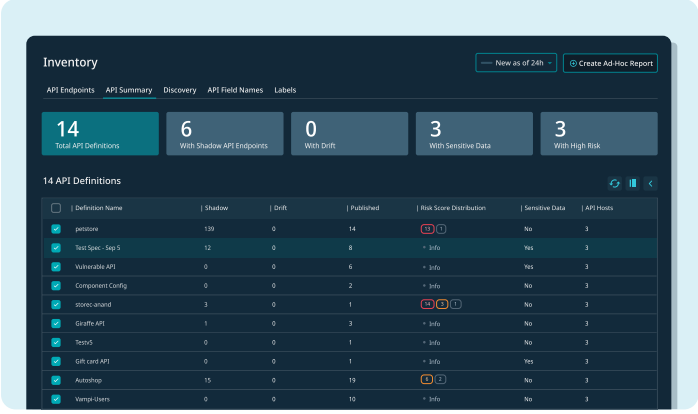
Cequence permite a las organizaciones:

- **Descubra todas las APIs en uso,** incluidas las APIs shadow y zombie, sin necesidad de especificaciones de API.
- **Obtenga información sobre el uso de las APIs,** incluida la ubicación geográfica, encabezados, parámetros de consulta y elementos del cuerpo.
- **Genere automáticamente especificaciones** OpenAPI a partir de las APIs descubiertas y garantice su cumplimiento.
- **Evalúe dinámicamente el riesgo con base en categorías de riesgo** predefinidas y personalizables, como OWASP API Security Top 10 y Automated Top 10.
- **Pruebe APIs en entornos de preproducción** con tráfico sintético para detectar riesgos de OWASP y otras vulnerabilidades.
- **Proteja las APIs contra ataques** mediante la integración con infraestructuras de terceros, como WAFs y gateways de API.

Funciones de Seguridad de API de Cequence

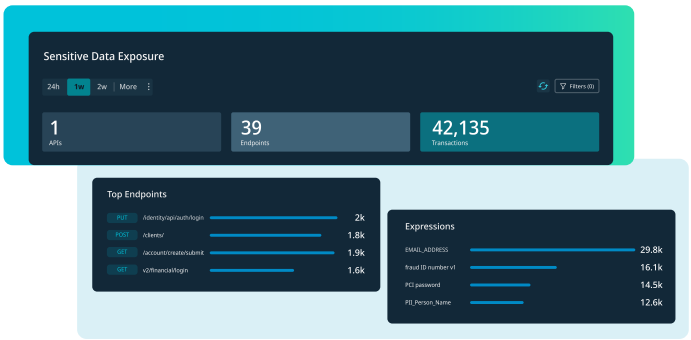
Visibilidad Completa y Continua del Ecosistema de APIs

Uno de los mayores desafíos de seguridad de API que enfrentan las organizaciones es saber qué APIs tienen, dónde se encuentran y quién tiene acceso. Cequence adopta un enfoque único para proporcionar visibilidad completa y continua de la huella de APIs en tiempo de ejecución de una organización, desplegando sensores diseñados específicamente a nivel de red e integrándose con su infraestructura existente, incluidos CDNs y gateways de API. Cequence API Security también ofrece una perspectiva externa, escaneando sus dominios y subdominios para identificar hosts y endpoints de APIs de acceso público, incluso si no están en uso. Esta técnica de "vista del atacante" también descubre proveedores de edge, infraestructura y hosting.



El descubrimiento continuo, el seguimiento del inventario y la categorización de riesgos te ayudan a controlar tu huella de APIs.

API Security no requiere agentes en el servidor o cliente, JavaScript o integración de SDK, garantizando que el descubrimiento de APIs no esté limitado al software instrumentado, lo que también elimina penalizaciones posteriores como ciclos de desarrollo extendidos, carga lenta de páginas e incremento de costos en la nube. La solución crea un catálogo de APIs en tiempo de ejecución y genera automáticamente especificaciones de API si aún no existen, reduciendo drásticamente los esfuerzos manuales. Los paneles muestran las APIs categorizadas por nivel de riesgo, con métricas detalladas que incluyen la distribución geográfica del uso de APIs por país, dirección IP y organización.



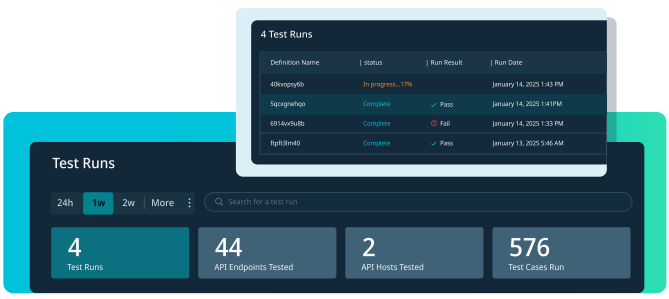
Prevención de la Exposición de Datos Sensibles

Cequence incluye potentes capacidades para prevenir la exposición de datos sensibles. Su funcionalidad de baselining descubre las APIs y comprende su contexto de negocio en cuestión de horas tras la implementación, identificando aquellas APIs que procesan información sensible. Cequence detecta automáticamente datos sensibles mediante patrones predefinidos (por ejemplo, números de tarjetas de crédito o de seguridad social) y patrones personalizables. Los patrones de datos sensibles son compatibles a nivel mundial; por ejemplo, Cequence puede diferenciar automáticamente entre un número de licencia de conducir de EE. UU. y un número de identificación nacional de Arabia Saudita.

El aprendizaje automático basado en Procesamiento de Lenguaje Natural (NLP) complementa los patrones predefinidos y reduce los falsos positivos al identificar datos sensibles a través de señales contextuales, como la presencia de palabras clave cercanas al valor detectado. El panel de Exposición de Datos Sensibles muestra los resultados de forma gráfica, con detalles como la API de origen y los códigos de respuesta que están filtrando los datos, el patrón identificado y la información subyacente de la dirección IP. Se pueden enviar notificaciones a los equipos de desarrollo para una remediación rápida mediante alertas predefinidas para herramientas como Slack, PagerDuty y correo electrónico. Cequence también ofrece enmascaramiento de datos sensibles mediante cifrado con preservación de formato (FPE), que se aplica antes de que el producto "vea" los datos, garantizando que la información sensible permanezca privada.

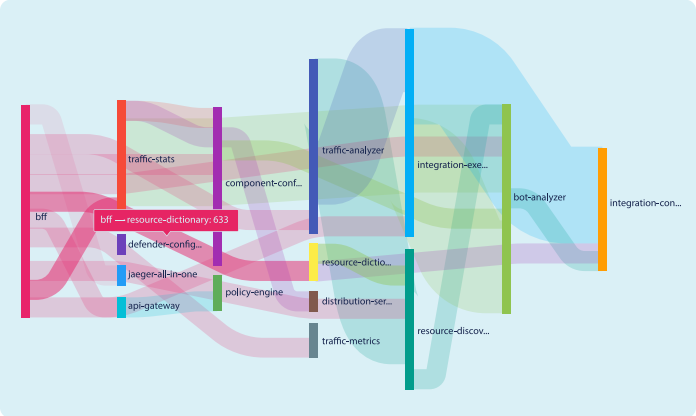
Pruebas Inteligentes de Seguridad de API

Cequence permite a los equipos de TI y desarrollo probar exhaustivamente sus APIs en preproducción y en tiempo de ejecución, identificando errores de codificación, vulnerabilidades y otras desviaciones de las especificaciones. Si no hay especificaciones disponibles, la creación autónoma de pruebas genera especificaciones de API sin intervención humana, lo que potencialmente elimina horas o semanas de trabajo manual. Estas capacidades de pruebas de seguridad pueden integrarse en el pipeline de CI/CD y en los IDEs, o ejecutarse de manera independiente según sea necesario en tiempo de ejecución.



Visualización de Flujos de Tráfico de API

El Cequence Flow Graph visualiza las interacciones entre APIs, permitiendo a los usuarios observar los flujos de comunicación entre ellas. Esto facilita la identificación de APIs internas, de terceros y sus dependencias, la validación de interacciones aprobadas, la detección de anomalías y brechas de seguridad, así como el descubrimiento de Shadow APIs y Rogue APIs.



Protección de APIs contra Amenazas y Ataques

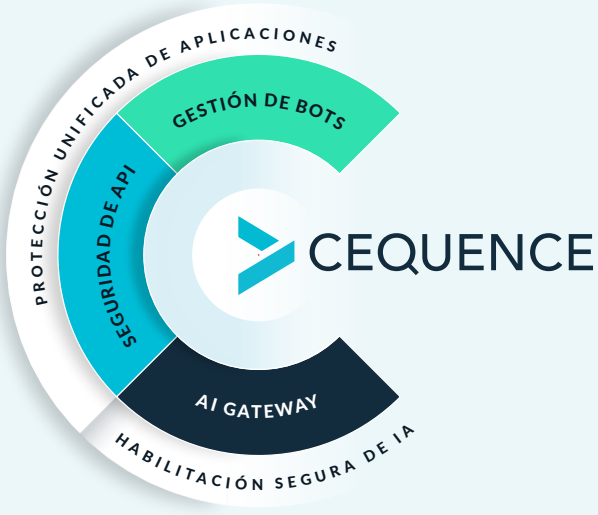
Cequence protege aplicaciones web, móviles y API contra ataques para prevenir la pérdida de datos, el robo y el fraude. La detección de amenazas y análisis impulsados por inteligencia artificial, junto con la integración con soluciones defensivas de terceros como WAF y puertas de enlace API, garantizan protección contra incluso los ataques más sofisticados. Cequence Bot Management proporciona mitigación nativa, incluyendo bloqueo, limitación de velocidad, inyección de encabezados y engaño.

Funciona con Cequence AI Gateway

Cequence AI Gateway habilita el acceso de IA agéntica (basada en agentes) a cualquier aplicación interna, externa o SaaS, en minutos y sin necesidad de código. API Security puede crear automáticamente especificaciones de API que el AI Gateway utiliza para crear servidores MCP, eliminando una cantidad significativa de esfuerzo manual.

La Seguridad de API es Parte de la Plataforma Cequence Unified Application Protection

La plataforma Cequence Unified Application Protection unifica el descubrimiento, el cumplimiento y la protección para defender las aplicaciones y APIs de una organización contra ataques, abuso de lógica empresarial y fraude. Demostrando su valor en minutos —no en días ni semanas—, Cequence ofrece un modelo de implementación flexible que no requiere instrumentación ni modificación de las aplicaciones. Con la confianza de las organizaciones públicas y privadas más grandes y exigentes, Cequence protege más de 10 mil millones de interacciones API diarias y 4 mil millones de cuentas de usuario.



CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai