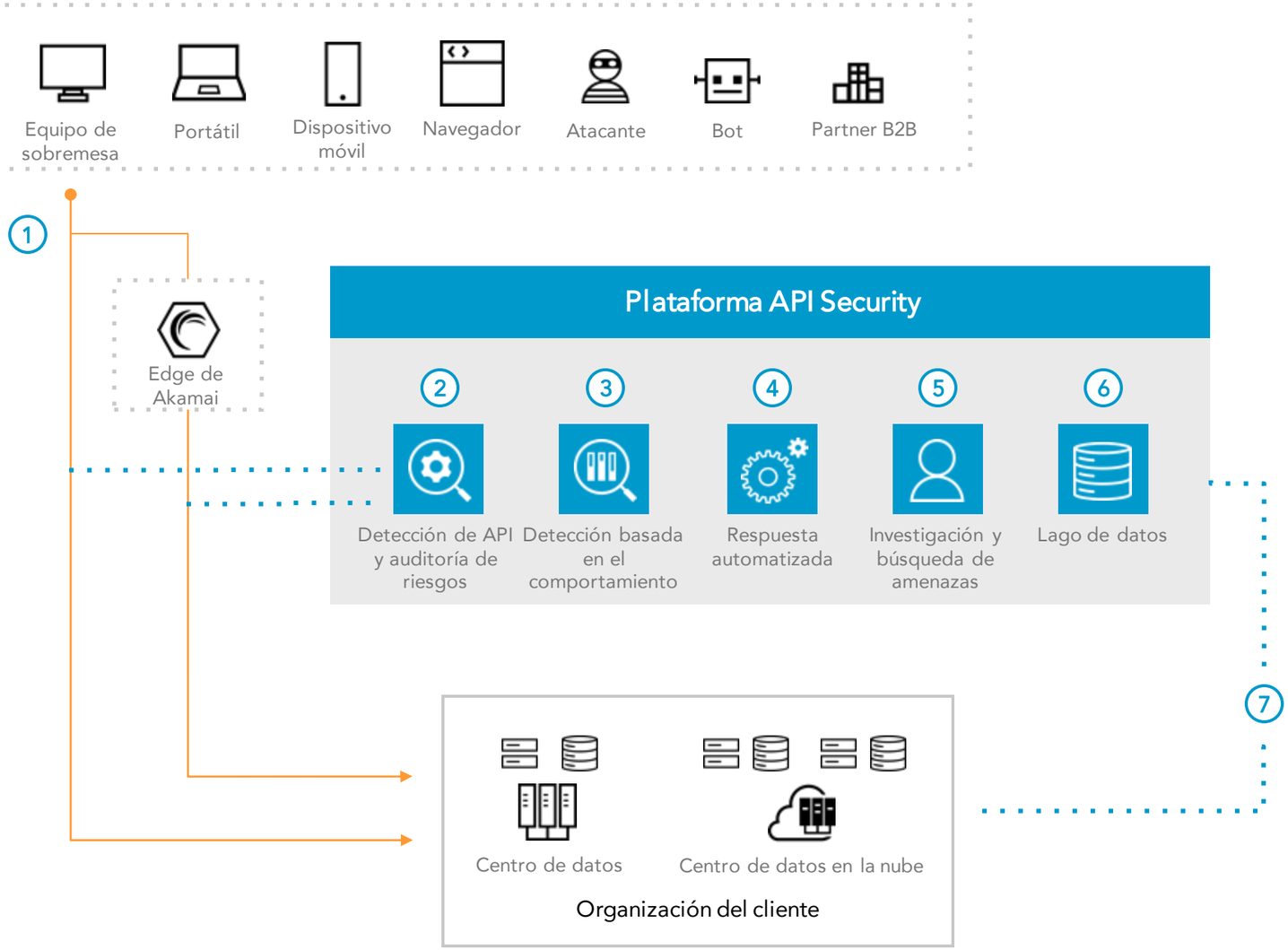
API SECURITY

Cómo funciona



OVERVIEW

Akamai API Security detecta y audita todas las API, y supervisa su actividad mediante análisis de comportamiento para detectar amenazas y abusos y responder a ellos. La solución proporciona mecanismos de detección contextuales para proteger contra el abuso de lógica y los ataques de API que las soluciones basadas en firmas no son capaces de detectar.

1. El tráfico fluye desde la organización del cliente o a través de la plataforma en el Edge de Akamai
2. Se envía una copia de ese tráfico a la plataforma API Security, donde se detectan todas las API
3. El sistema de detección del comportamiento establece un patrón de lo que es normal para identificar anomalías y abusos de lógica
4. El sistema de respuesta automatizada puede enviar información crítica a los equipos de seguridad o bloquear el tráfico en el Edge de Akamai
5. Los equipos de seguridad pueden utilizar los datos contextuales del comportamiento para investigar y buscar amenazas dentro del tráfico de API o utilizar un servicio gestionado de búsqueda de amenazas
6. La actividad histórica de API se almacena en nuestro lago de datos y ayuda en la investigación y las iniciativas de búsqueda de amenazas
7. API Security también tiene una visibilidad completa de las API y su actividad en la organización del cliente

PRODUCTOS CLAVE

Protección de API ► Akamai API Security

Búsqueda de amenazas gestionadas ► Akamai API Security ShadowHunt

Visite akamai.com/products/api-security

Publicado en abril de 2024