INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Account Protector

¿Es el propietario de la cuenta o un impostor?
Los clientes confían en que sepa la diferencia.

El crecimiento de su negocio digital depende de su capacidad para generar confianza y mantenerla en un entorno en el que esta no es habitual sin que haya conflicto con la experiencia del cliente. ¿Podría lograrlo con los sistemas actuales?

Los fraudes relacionados con cuentas, como el robo de cuentas, se han convertido en un problema caro y difícil para las empresas de todos los sectores. El ataque parece llevarlo a cabo una persona con credenciales válidas, tal y como está previsto que funcione el proceso. Pero al igual que sucede con gemelos idénticos que, al mirarlos detenidamente, muestran pequeñas y sutiles señales de que no se trata de la misma persona, estas credenciales presentan también indicaciones de que no son tan válidas como parece. Account Protector evalúa múltiples señales de riesgo y confianza para identificar lo que otros sistemas podrían pasar por alto y detectar si la persona que inicia sesión en la cuenta es el propietario o un impostor.

Los riesgos y las repercusiones del robo de cuentas nunca han sido tan relevantes, a medida que el comercio y los nuevos activos digitales se han convertido en algo cada vez más habitual.

El comercio digital está en pleno auge. Y aunque ahora realizamos más transacciones online, la confianza en las experiencias digitales se ha visto mermada significativamente. En general, los usuarios confían menos que nunca en los sistemas y las instituciones existentes. El fraude online, las campañas de desinformación, los deepfakes y los ataques de ciberseguridad proliferan.

Con el incremento de la actividad online, hemos observado un notable aumento de los activos digitales irreemplazables. Existen mercados secundarios rentables para activos online, como tarjetas regalo, puntos de fidelización y millas aéreas. Además, existen nuevas y valiosas clases de activos exclusivamente digitales, como criptomonedas (p. ej., Bitcoin), monedas de juegos y elementos de juego poco comunes, y obras de arte únicamente digitales, entre otros. Si se roban, muchos de estos activos no se pueden reemplazar.

Haga crecer su negocio con confianza

Si los activos importantes de sus clientes están expuestos a riesgos, debe proteger tanto a estos como a su organización frente al robo de cuentas y los ataques de bots relacionados, como el Credential Stuffing o la manipulación de inventario, entre otros. También debe asegurarse de que la seguridad no comprometa la experiencia positiva online del cliente. Hemos diseñado Account Protector para detectar impostores en el borde de Internet y, así, permitir acceder a sus clientes sin obstáculos adicionales. Además, al reducir el robo de cuentas y los fraudes relacionados con bots, no solo protegerá a sus clientes, sino que reducirá el coste y la frustración que estos ataques conllevan. Puede beneficiarse de un crecimiento exponencial en el terreno digital sin hacer concesiones en cuanto a coste o protección.

Account Protector ofrece una solución completa diseñada para prevenir los inicios de sesión fraudulentos por parte de usuarios no autorizados y mitigar los sofisticados ataques de bots que a menudo preceden a los intentos de robo de cuenta. Esta solución emplea técnicas para comprender el comportamiento de los propietarios legítimos de las cuentas y, después, evaluar el riesgo de cada solicitud de autenticación basándose en desviaciones del perfil de comportamiento y los dispositivos habituales, así como en otras formas de detección avanzadas.

VENTAJAS PARA SU EMPRESA

Mejore su confianza: la suya y la de sus clientes
Descubra qué interacciones son legítimas, reduzca los obstáculos para los usuarios y protéjalos de la actividad fraudulenta para fomentar la confianza entre los consumidores, los partners y su organización.

Desarrolle protecciones adaptadas exclusivamente a su negocio
La optimización automática del sistema de detección de bots y la posibilidad de comprender los perfiles de grupos de usuarios en función del modo en que interactúan con su sitio le ofrece una protección y detección frente a anomalías más personalizada.

Obtenga información y visibilidad detalladas
Los equipos de seguridad y de lucha contra el fraude pueden tomar medidas con confianza gracias a señales e indicadores transparentes, en lugar de depender de análisis de caja negra basados en respuestas de tipo “sí o no”.

Reduzca las consecuencias de las correcciones
Reduzca el coste financiero y los recursos destinados a la investigación de cuentas comprometidas, la sustitución de activos robados, el restablecimiento de las cuentas existentes de clientes afectados, las denuncias ante las autoridades legales y normativas (cuando sea necesario) y la resolución de quejas de usuarios.

Tome mejores decisiones de seguridad y con respecto a la identidad basadas en datos
Se integra con herramientas antifraude, SIEM y otras soluciones de seguridad para permitir el uso de las señales de riesgo y confianza de Account Protector para aumentar la precisión y mejorar su inversión en esas herramientas. Si opta por integrarlo con su flujo de trabajo de autenticación de usuarios, podrá tomar decisiones más estratégicas y creativas sobre la ejecución, por ejemplo, cuándo poner en marcha una autenticación incremental.

Akamai

A continuación, es posible aplicar una respuesta adecuada a cada solicitud, incluida la puesta en marcha de medidas en el borde de Internet, en tiempo real y sin que afecte a la experiencia de los usuarios legítimos de las cuentas. También puede utilizar los informes y los análisis de Account Protector de forma independiente o junto con sus herramientas de análisis y antifraude existentes para obtener información más detallada.

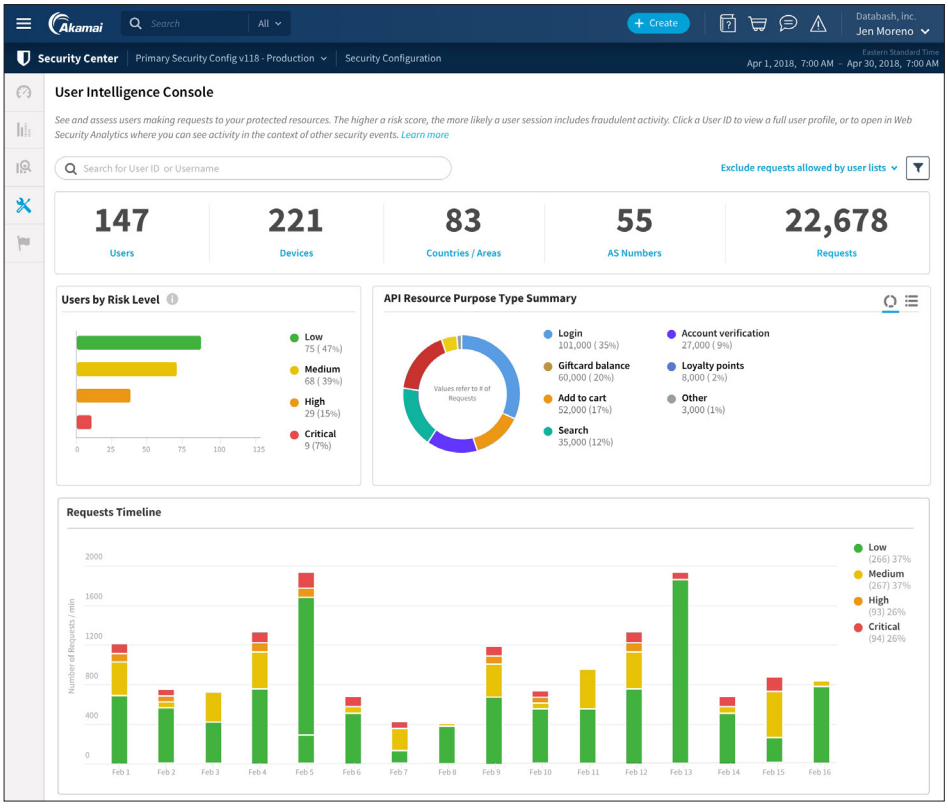
Account Protector le permite confiar en la validez de los inicios de sesión de usuario sin añadir obstáculos adicionales. Esta confianza, sumada a una experiencia de cliente fluida y sin pasos de autenticación adicionales innecesarios, se transformará en más ventas y en un mayor valor del tiempo de vida de los clientes.

Bloquee el robo de cuentas y los ataques de bots

Account Protector utiliza la detección de comportamientos para crear un perfil de los patrones de actividad de los propietarios de las cuentas, las anomalías en dispositivos y la reputación de las fuentes. A medida que se reciben solicitudes de inicio de sesión, Account Protector evalúa en tiempo real el riesgo de que la solicitud no proceda del propietario legítimo de la cuenta mediante la detección de anomalías con respecto al comportamiento habitual del usuario. Los perfiles de comportamiento pueden incluir los dispositivos que se usan habitualmente, las direcciones IP, las redes, las ubicaciones y la frecuencia y la hora de los inicios de sesión, entre otros. Funciona incluso la primera vez que un usuario inicia sesión, puesto que puede detectar anomalías en el primer inicio de sesión a partir del perfil de comportamiento de todo el grupo de clientes.

Account Protector ofrece protección frente a bots sofisticados dirigidos a su organización mediante ataques automatizados a gran escala. La solución detecta y mitiga los bots dañinos mediante técnicas y modelos de aprendizaje automático e IA, que incluyen el análisis de telemetría/comportamiento del usuario, huella dactilar del navegador, detección automática del navegador, detección de anomalías de HTTP e índices elevados de solicitudes, entre otras.

Las ventajas de Account Protector van más allá de la interrupción inmediata de los intentos de robo de cuentas. Account Protector proporciona una completa fuente de información sobre comportamiento y riesgo que puede incorporar a sus motores de detección de fraude existentes para profundizar en el análisis y poner en marcha medidas de mitigación adicionales, aumentando el valor y la eficacia de sus inversiones actuales.



Funcionamiento

Perfiles de usuario
Detecte impostores en función de anomalías en indicadores como el perfil de dispositivos, ubicaciones, redes y momentos de actividad de un usuario observados previamente.

Perfiles de grupo
Detecte anomalías desde el primer inicio de sesión en función del perfil de comportamiento de todo el grupo de usuarios.

Detecciones de bots sofisticadas
Detecte y mitigue bots adversos incluso en la primera interacción con algoritmos supervisados y sin supervisar.

Datos de reputación
Evalúe la reputación de la fuente en función de la actividad maliciosa anterior observada en todos los clientes de Akamai.

Puntuación de riesgo en tiempo real
Analice y puntúe el riesgo de la sesión del usuario mediante la evaluación de anomalías en el comportamiento del usuario, los dispositivos, la reputación de la red/la dirección IP y otras detecciones avanzadas.

Optimización específica para su organización
Evalúe las solicitudes con aprendizaje automático que se ajusta constantemente de acuerdo con el tráfico individual de su organización y los patrones de comportamiento de los usuarios.

Información detallada
Utilice la información de Account Protector con herramientas para la detección de fraude y SIEM para comprender mejor y de forma más sofisticada los ataques, a los atacantes y los riesgos.

Funciones clave

Puntuación de riesgo de la sesión del usuario en tiempo real: evalúa las señales de riesgo y confianza durante la autenticación, como anomalías en el comportamiento del usuario o el dispositivo y la reputación de la dirección IP y la red para sopesar el riesgo de que una solicitud no provenga del propietario legítimo de la cuenta.

Perfiles de comportamiento del usuario: crea un perfil de comportamiento del usuario basado en las ubicaciones, las redes, los dispositivos y los momentos de actividad observados previamente.

Perfiles de grupo: combina los perfiles de los usuarios de la organización en un grupo más grande, donde las variaciones del comportamiento también pueden compararse con el grupo completo de usuarios para detectar anomalías.

Reputación de la fuente: evalúa la reputación de la fuente según la actividad maliciosa observada anteriormente en todos los clientes de Akamai, incluidos muchos de los sitios web más grandes, de mayor tráfico y con mayor frecuencia de ataques del mundo.

Indicadores: asigna a cada solicitud indicadores de riesgo, confianza y generales para evaluar el riesgo de que la persona que inicia sesión no sea el propietario legítimo de la cuenta. Los indicadores se proporcionan junto con la puntuación de riesgo del usuario final y se pueden utilizar para realizar análisis o enviar al origen.

Directorios de bots conocidos: responde automáticamente a los bots conocidos, y actualizamos continuamente nuestro directorio actual que consta de 1500 bots conocidos.

Detección de bots sofisticados: detecta los bots desconocidos desde la primera interacción gracias a una serie de modelos y técnicas de inteligencia artificial y aprendizaje automático. Estas técnicas incluyen el análisis del comportamiento/la telemetría, la huella dactilar y la detección automática del navegador, la detección de anomalías de HTTP e índices elevados de solicitudes, entre otras.

Análisis y generación de informes: proporciona informes históricos y en tiempo real. Analice la actividad en terminales individuales, investigue a un usuario específico, consulte usuarios por nivel de riesgo y obtenga perspectivas adicionales. El análisis de Account Protector le ofrece estadísticas de alto nivel y un análisis detallado que puede importar a sus herramientas antifraude y de gestión de eventos e información de seguridad (SIEM) para comprender mejor la intención y planificar de forma estratégica, lo que aumenta el valor de sus inversiones en seguridad existentes.

Acciones de respuesta avanzadas: proporciona un amplio rango de acciones que se pueden poner en marcha para detener los intentos de robo de cuentas y de Credential Stuffing, como alertar, bloquear, retrasar y ofrecer contenido alternativo, proporcionar CAPTCHA o desafíos criptográficos, entre otras. Además, las organizaciones pueden asignar distintas acciones en función de la URL, la hora del día o el porcentaje del tráfico.

Inyección de encabezados: envía señales para indicar actividad humana fraudulenta. Inyecta un encabezado de solicitud adicional en la solicitud reenviada con información sobre la puntuación de riesgo del usuario y los indicadores de riesgo, confianza y generales que contribuyeron a la puntuación para un análisis más profundo y mitigación en tiempo real.

Automatización con aprendizaje automático: actualiza automáticamente las características y los comportamientos utilizados para identificar actividad humana y bots fraudulentos, desde patrones de comportamiento hasta las puntuaciones de reputación más recientes en la plataforma de Akamai.

Integración de SIEM (opcional): integra la información de riesgo del usuario en las herramientas SIEM para los clientes que desean una mayor visibilidad de seguridad integrada. La información de Account Protector le permite aumentar el valor de sus herramientas existentes.

Proteger la confianza

Reconozca un intento de robo de cuenta en el momento en el que se produce para poder detenerlo en tiempo real y proteger la experiencia y la confianza de sus usuarios.

Póngase en contacto con su representante de Akamai o visite akamai.com para obtener más información.