INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Account Protector

Mantenga alejados a los estafadores (y la reputación de su empresa intacta) con la protección contra la usurpación de cuentas.

¿Cómo puede saber si un usuario es auténtico o un impostor? Sus clientes confían en que sepa diferenciarlos

Cada vez hay más transacciones y recursos digitales, por lo que los riesgos y las consecuencias de que una cuenta se vea vulnerada son mayores que nunca. Su capacidad para expandir su negocio digital y proteger a sus clientes se basa en preservar la confianza, a pesar de las nuevas y mayores tácticas de fraude.

Los abusos relacionados con las cuentas, como la apertura fraudulenta de cuentas (fraude de nuevas cuentas) y el robo de cuentas (ATO), plantean retos y costes importantes para las empresas de todos los sectores. Las cuentas comprometidas y falsas pueden tener graves consecuencias financieras y de reputación para las organizaciones. Cuando una cuenta se ve vulnerada, los atacantes pueden explotarla libremente con el fin de agotar los saldos, realizar transacciones fraudulentas, desactivar funciones de seguridad como la autenticación multifactorial (MFA) o robar información personal confidencial. Las cuentas falsas, por otro lado, se pueden utilizar para aprovechar las promociones como pruebas y créditos gratuitos, ejecutar ataques de SMS pumping e inundar plataformas con spam o contenido inapropiado. El impacto de estos ataques es significativo, y las empresas se enfrentan a la posibilidad de menoscabar la confianza de los clientes, perder millones en fraudes y lidiar con multas regulatorias y daños a la reputación.

Akamai Account Protector

Account Protector está diseñada para evitar el abuso de cuentas en todo el ciclo de vida de una cuenta. La solución de seguridad usa el aprendizaje automático y un sinfín de datos sobre indicadores de riesgo y confianza para determinar la legitimidad de una solicitud de usuario. Además, analiza el comportamiento en tiempo real para identificar signos sutiles de actividad fraudulenta, desde la creación de la cuenta hasta el inicio de sesión y más allá. Si se detecta un comportamiento sospechoso o anómalo, Account Protector proporciona opciones de mitigación inmediatas para preservar una experiencia de usuario óptima, como bloquear y tomar medidas en el Edge, responder a desafíos criptográficos y de comportamiento, ofrecer contenido alternativo y mucho más.

Ventajas para su empresa

Mejore la confianza: la suya y la de sus clientes
Descubra qué interacciones son legítimas, reduzca los problemas de los usuarios y protéjalos de la actividad fraudulenta.

Desarrolle protecciones perfectamente adaptadas a su empresa
Aproveche los mecanismos de detección de bots personalizados y la capacidad de comprender los perfiles de grupos de usuarios en función del modo en que interactúan con su sitio.

Obtenga información y visibilidad detalladas
Tome medidas con confianza basadas en señales e indicadores transparentes.

Disminuya las consecuencias de las correcciones
Reduzca el coste financiero y los recursos destinados a la investigación de cuentas comprometidas, la sustitución de recursos robados y mucho más.

Tome mejores decisiones de seguridad y con respecto a la identidad basadas en datos
Se integra con herramientas antifraude, de gestión de información y eventos de seguridad (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 la inversión en esas herramientas.

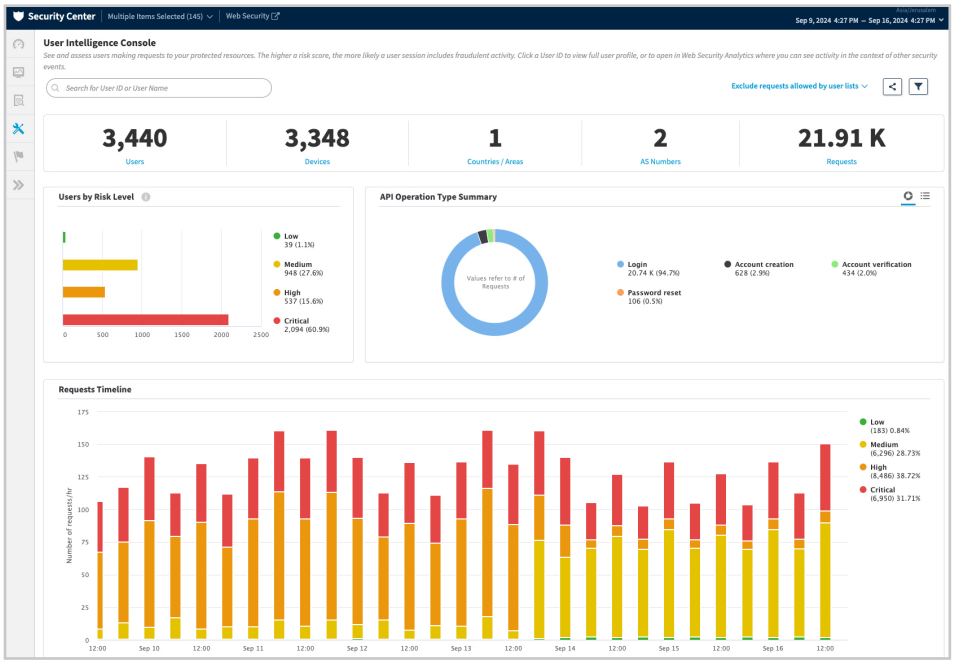
Obtenga una defensa integral contra el abuso de cuentas

Proteja las cuentas de usuario a lo largo de todo su ciclo de vida con protección avanzada contra amenazas, como la apertura abusiva de cuentas o la usurpación de cuentas de usuarios, así como otros esquemas de ataque.

Apertura abusiva de cuentas. Mitigue la creación de cuentas falsas que se utilizan para aprovechar las promociones, ejecutar ataques de SMS pumping, probar información de tarjetas de crédito robadas, acaparar inventario y mucho más.

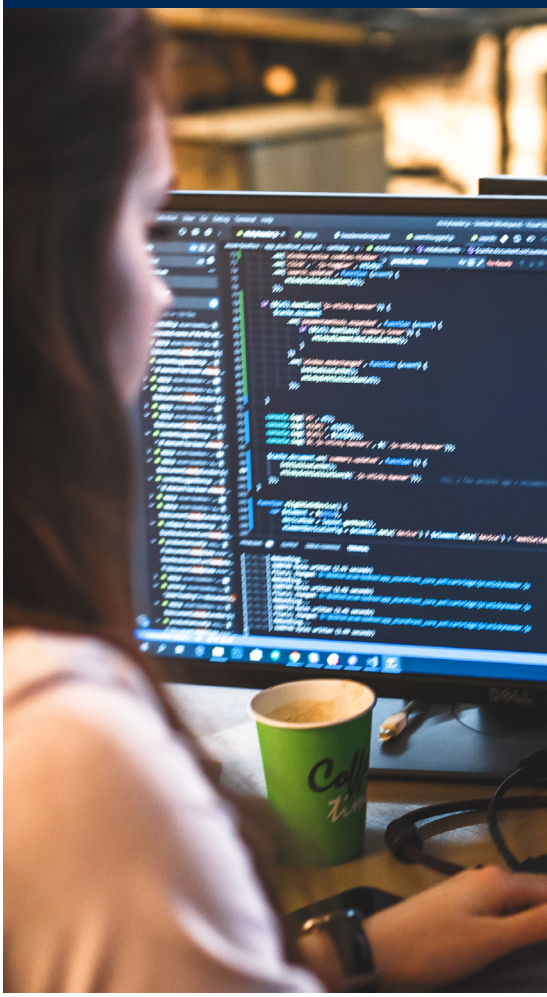
Robo de cuentas. Protéjase frente a impostores que obtienen acceso a cuentas de clientes legítimas para despojarlas de su valor, robar datos confidenciales y realizar transacciones fraudulentas.

Ataques de bots sofisticados. Proteja las cuentas de los usuarios ante Credential Stuffing, manipulación de inventario y otros ataques automatizados que suelen iniciarse a la vez que ataques de apertura abusiva de cuentas o ATO para obtener productos valiosos, dinero u otros activos de valor de los clientes.



Protección, confianza y experiencia de usuario

Analice los riesgos y detenga el abuso en tiempo real con una supervisión constante de las cuentas a lo largo de todo su ciclo de vida para detectar signos de comportamiento sospechoso a medida que se producen.



Funciones clave

Protección integral del ciclo de vida de las cuentas. Identifica y analiza el riesgo de los usuarios en cualquier fase, desde la creación de cuentas hasta las acciones posteriores al inicio de sesión, como las actualizaciones, los cambios de contraseña y los pagos.

Puntuación de riesgo de la sesión del usuario en tiempo real. Evalúa el riesgo y la fiabilidad de la sesión del usuario para sopesar la probabilidad de que una solicitud provenga del propietario legítimo o de un impostor.

Inteligencia de direcciones de correo electrónico. Analiza la sintaxis de una dirección de correo electrónico y el uso anómalo de un mensaje para detectar patrones maliciosos.

Inteligencia de dominios de correo electrónico. Evalúa el patrón de actividad procedente de dominios individuales de correo electrónico, como los dominios desechables y el uso excesivo de un dominio de correo electrónico.

Reconocimiento global de usuarios de confianza. Permite ver el comportamiento de los usuarios en toda la red de Akamai para tomar decisiones más fundamentadas sobre la fiabilidad de un inicio de sesión.

Perfiles de comportamiento del usuario. Crea un perfil de comportamiento del usuario basado en las ubicaciones, las redes, los dispositivos, las direcciones IP y los momentos de actividad observados previamente para reconocer a los usuarios que regresan.

Perfiles de grupo. Combina los perfiles de los usuarios de la organización en un grupo más grande para que las variaciones del comportamiento también puedan 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 la usurpación de cuentas. Los indicadores se proporcionan junto con la puntuación de riesgo del usuario final y se pueden utilizar para realizar análisis.

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 información detallada.

Acciones de respuesta avanzadas. Proporciona un amplio rango de acciones que se pueden poner en marcha para detener los intentos de abuso, como alertar, bloquear, retrasar y proporcionar desafíos criptográficos o de comportamiento u ofrecer contenido alternativo, entre otras. Además, las organizaciones pueden asignar distintas acciones según la URL, la hora del día, la geolocalización, la red o el porcentaje del tráfico.

Inyección de encabezados. Envía información de riesgo del usuario para su análisis y la mitigación en tiempo real. Se 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 buscan una visibilidad más integrada de la seguridad. La información de Account Protector le permite aumentar el valor de sus herramientas existentes.

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