HOJA DE DATOS

CA Risk Authentication

Resumen

CA Risk Authentication le permite proporcionar protección en tiempo real contra robo de identidad y fraude en línea a través de la autenticación inteligente basada en riesgos. Recopila silenciosamente datos y evalúa el potencial de fraude de las transacciones móviles o en línea confidenciales. Evalúa el riesgo basándose en un conjunto amplio de variables y también puede aprender los patrones de comportamiento individuales del usuario y detectar cuando se desvían de la norma. Cuando una calificación de riesgo excede un umbral definido, puede iniciar la autenticación incremental o bloquear la transacción. La solución funciona con CA Strong Authentication para proporcionar credenciales de autenticación de varios factores. También se integra con toda nuestra cartera de Identity y Access Management.

Resultados o beneficios clave

- Proporciona experiencia del cliente sin fricción mediante un análisis de riesgo transparente.
- Reduce la exposición a las infracciones de datos, el acceso indebido y el robo de identidad.
- Baja el costo de las operaciones al reducir el fraude en línea.
- Ayuda a cumplir con las regulaciones gubernamentales y las directrices del sector sobre autenticación más sólida.

Características clave

- Proporciona conjuntos de reglas de mejores prácticas predeterminados que cubren patrones de fraude típicos.
- Habilita las personalización rápida y sencilla de reglas y políticas, y las reglas se pueden implementar dinámicamente.
- Realiza una evaluación del riesgo transparente y en tiempo real que incluye la identificación del dispositivo, la geolocalización, comprobaciones de velocidad y perfiles de comportamiento del usuario.
- Integra los datos desde la web y los canales móviles para la administración del fraude.
- Aprende el comportamiento del usuario final y sugiere la autenticación incremental cuando hay una desviación de la norma.
- Incluye el sistema basado en políticas para revisar y administrar casos de actividad sospechosa.
- Está diseñado con latencia extremadamente baja para admitir millones de usuarios sin degradar su aplicación web o rendimiento de la red.
- Está disponible como una solución local o basada en la nube.

Retos empresariales

Identificar el robo de identidad y el fraude es un muy buen negocio. Parece que todos los días las noticias informan que ha ocurrido una nueva violación de seguridad. Si bien las instituciones financieras continúan viendo ataques más sofisticados, los delincuentes expandieron su alcance más allá de los objetivos tradicionales de las transacciones bancarias y tarjetas de crédito del consumidor. Ahora buscan recolectar información valiosa de organizaciones gubernamentales y datos empresariales confidenciales accesibles en línea. Las organizaciones intentan aumentar la seguridad para proteger sus datos sin incrementar los costos de soporte o sin crear una carga para los usuarios.

Las normas de cumplimiento y directrices del sector están acentuando el énfasis en la autenticación más fuerte para proteger datos. Las organizaciones no quieren implementar sistemas de autenticación excesiva que requieren la interacción repetitiva del usuario debido al efecto negativo en la experiencia del usuario, que afecta la adopción de servicios en línea y la lealtad del cliente. El reto general es detectar y bloquear la actividad fraudulenta antes de que ocurran pérdidas por fraude, sin afectar a los usuarios. Simplemente agregar una evaluación de riesgo transparente proporciona mayor seguridad de que el usuario es quien dice ser, sin afectar a los usuarios legítimos.

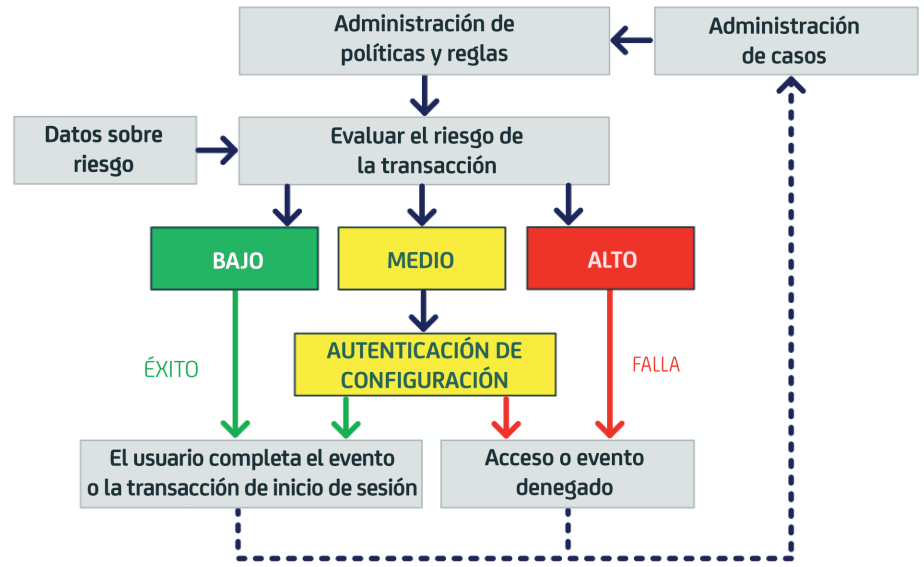
Descripción general de la solución

CA Risk Authentication puede detectar actividades sospechosas en los servicios en línea empresariales y de consumidores sin crear una carga para los usuarios. Esta sólida solución de evaluación de riesgo de canales múltiples detecta y evita, de manera transparente, el fraude antes de que se produzcan pérdidas. Usted establece el equilibrio correcto entre el riesgo y la conveniencia del usuario para su organización, definiendo un proceso que determina el potencial de fraude de cada inicio de sesión en línea o transacción confidencial basada en el nivel de riesgo. Usando un modelo empresarial que entiende el comportamiento legítimo y fraudulento, puede determinar la validez de un usuario en el contexto de lo que es normal para ese individuo. Como resultado del análisis en tiempo real, se puede permitir continuar a los usuarios, se les puede solicitar que proporcionen credenciales de inicio de sesión adicionales o se les puede denegar el acceso. También puede ejecutar diferentes niveles de autenticación según la transacción y la calificación de riesgo. Esto protege a los usuarios de ataques de Internet, ya sea que estén comprando en línea o accediendo a información privada a través de un portal Web o una aplicación móvil.

Diferenciadores clave

- **Perfiles de comportamiento individuales:** Reduce la fricción al aprender los patrones de comportamiento de cada usuario y al detectar cuando este se desvía de la norma
- **Motor de reglas configurable:** Establece el equilibrio de riesgo y la conveniencia del usuario adecuada para cada organización
- **Crear fácilmente reglas para apoyar las políticas comerciales:** Permite a organizaciones personalizar la calificación de riesgo según sus necesidades
- **Reglas abiertas y flexibles que se pueden cambiar sobre la marcha:** Permite a las organizaciones adaptarse rápidamente a nuevas amenazas
- **Conocimiento de por qué se desencadena una acción de riesgo:** Permite a las organizaciones entender por qué los usuarios afrontan retos y ajustar las reglas según corresponda, si es necesario
- **Informar de inmediato los datos disponibles:** Proporciona conocimiento del entorno en tiempo real
- **Integración con CA Strong Authentication:** Permite una estrategia de seguridad en capas que incluye credenciales de dos factores y evaluación del riesgo
- **La integración con CA Single Sign-On (anteriormente CA SiteMinder™)** permite el uso de una calificación de riesgo en toda la sesión del usuario para proporcionar seguridad adicional y hacer cumplir la autenticación incremental según sea necesario

Flujo de evaluación del riesgo.



CA Risk Authentication puede detectar la actividad fraudulenta al proporcionar un segundo nivel de autenticación aun cuando se hayan comprometido las credenciales.

Soluciones o productos relacionados

- **CA Strong Authentication.** Conjunto flexible de credenciales de varios factores para autenticar usuarios a fin de aumentar la seguridad y mejorar el cumplimiento
- **CA Single Sign-On.** Inicio de sesión único en la web en las aplicaciones locales, alojadas o basadas en la nube para sus empleados, clientes y socios.
- **CA Privileged Identity Manager.** Administración de la cuenta privilegiada que protege a servidores, aplicaciones y dispositivos en plataformas y sistemas operativos.

Entornos admitidos

- **Navegador:** Apple Safari, Google Chrome, Internet Explorer® y Mozilla Firefox
- **Dispositivos móviles:** Android, iOS
- **Inicio de sesión único:** CA Single Sign-On, Tivoli® Access Manager, Oracle Access Manager

Para obtener más información, visite **ca.com/ar/multifactor-authentication**.

CA Technologies (NASDAQ: CA) crea un software que impulsa la transformación en las empresas y les permite aprovechar las oportunidades de la economía de la aplicación. El software es el centro de cada empresa, en cada sector. Desde la planificación hasta el desarrollo, la administración y la seguridad, CA trabaja con empresas en todo el mundo para cambiar el estilo de vida, realizar transacciones y comunicarse, mediante entornos móviles, de nube pública y privada, distribuidos y centrales. Obtenga más información en **ca.com/ar**.

Copyright © 2015 CA. Todos los derechos reservados. Tivoli es una marca registrada de International Business Machines Corporation en los Estados Unidos, en otros países, o en ambos. Internet Explorer es una marca comercial registrada de Microsoft Corporation en los Estados Unidos o en otros países. Todas las demás marcas comerciales, los nombres comerciales, las marcas de servicio y los logotipos mencionados en este documento pertenecen a sus respectivas compañías.
CS200_150017_0815