HOJA DE DATOS

CA Advanced Authentication

Resumen

CA Advanced Authentication proporciona una forma segura, rentable y conveniente para el usuario de proteger las aplicaciones móviles y web. La solución les permite a las organizaciones recolectar datos de forma transparente y silenciosa, y evaluar el riesgo en función de la identificación del dispositivo, la geolocalización y el comportamiento del usuario, entre otros factores. CA Advanced Authentication también ofrece una amplia variedad de credenciales de autenticación de dos factores basadas en software para mejorar la seguridad de los inicios de sesión. La combinación de la evaluación de riesgo con credenciales de múltiples factores permite una estrategia de seguridad inteligente en capas para evitar el acceso indebido y el fraude de identidad en línea, sin afectar la experiencia del usuario.

Resultados o beneficios clave

- Proporciona una experiencia de usuario sin fricción mediante un análisis de riesgo transparente y una credencial de dos factores (2FA) basada en software.
- 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 normas gubernamentales y las directrices del sector para una autenticación más sólida.

Características clave

- Realiza evaluaciones de riesgo en tiempo real para proteger los inicios de sesión y las transacciones confidenciales.
- Evalúa el riesgo en función de la identificación del dispositivo, la geolocalización, el comportamiento del usuario y otros factores.
- Admite métodos fuera de banda, como la entrega de notificaciones push y contraseñas de un solo uso (OTP) a través de correo electrónico, mensaje de texto o de voz para la autenticación incremental.
- Proporciona conjuntos de reglas predeterminadas que cubren los patrones de fraude típicos y son fáciles de utilizar y de personalizar.
- Admite una gran variedad de credenciales: desde contraseñas y preguntas de seguridad, hasta software 2FA y tokens de hardware.
- Protege los canales web y móviles e integra los datos para una administración integral de fraudes.
- Acelera la innovación al permitir un DevOps seguro mediante interfaces RESTful fáciles de usar y de implementar.
- Se integra perfectamente con CA Single Sign-On y CA Mobile API Gateway.

Retos empresariales

Sus empleados, socios y clientes necesitan un fácil acceso a las aplicaciones en línea, y usted necesita proteger sus datos confidenciales contra el acceso indebido. Las organizaciones como la suya deben:

Mejorar la seguridad para las transacciones en línea. Las contraseñas se pueden comprometer fácilmente. Las organizaciones necesitan una forma adaptable de identificar a los usuarios y de protegerse contra el acceso indebido.

Habilitar los dispositivos móviles en forma segura. Las aplicaciones y dispositivos móviles se están convirtiendo en el método preferido por los usuarios para interactuar con el negocio. Las organizaciones necesitan una estrategia de autenticación consistente que se adapte a todos los canales de acceso y dispositivos.

Cumplir con las directivas de cumplimiento normativo. Muchas normas y directrices del sector están recomendando o exigiendo mecanismos de autenticación más sólidos. Las organizaciones deben responder a estos requisitos de una manera rentable.

Proporcionar una experiencia de usuario superior. Los usuarios son inconstantes e impacientes. Las organizaciones necesitan incrementar la seguridad sin afectar la experiencia del usuario.

Descripción general de la solución

CA Advanced Authentication es una solución en paquete que combina dos productos de autenticación principales:

CA Advanced Authentication realiza un análisis de riesgo inteligente y transparente para proporcionar mayores garantías de que el usuario es quien dice ser. El software evalúa el riesgo en función del dispositivo, la geolocalización y el comportamiento del usuario para cualquier transacción en línea, y puede iniciar una autenticación incremental cuando el puntaje de riesgo supera los umbrales definidos.

CA Strong Authentication proporciona una autenticación multifactor para las aplicaciones web y móviles con una amplia gama de credenciales y métodos. El software le permite implementar la credencial adecuada con el nivel adecuado de seguridad en función de la aplicación a la que se está accediendo, y así cumplir con las normas de una manera rentable y centralizada.

Juntos, estos productos permiten una estrategia de seguridad en capas que le ofrece el equilibrio perfecto entre costo, conveniencia y seguridad para proteger sus aplicaciones e identidades de usuario. Esto resulta en mayor seguridad, un mejor perfil de cumplimiento y menores costos operativos.

Diferenciadores clave

La **filosofía de "caja blanca"** le proporciona visibilidad de cada decisión sobre las reglas de riesgo y su resultado, y la capacidad de refinar el equilibrio entre el riesgo y la conveniencia para el usuario que corresponda a su organización.

La **creación de perfiles de comportamiento del usuario** reduce la fricción ya que aprende los patrones de comportamiento del usuario y detecta cuando este se desvía de la norma.

El **motor de reglas flexible** le ofrece un control completo de su entorno: específicamente, le permite crear reglas, políticas y acciones personalizadas para adaptar el motor de riesgo a casos de uso y transacciones específicos.

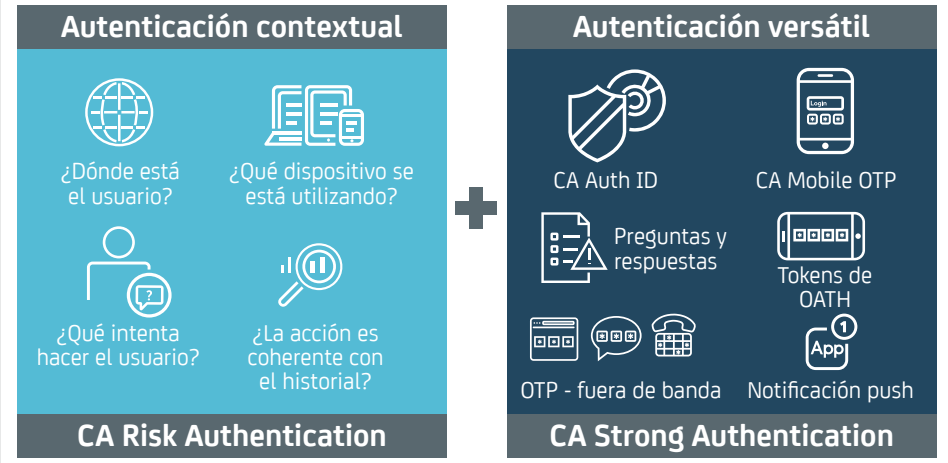
La **autenticación flexible** admite una gran variedad de credenciales y flujos de autenticación, y le permite establecer diferentes métodos de autenticación basados en el nivel de riesgo.

La **administración de casos** incluye un sistema basado en políticas para revisar y administrar los casos de actividad sospechosa.

La **protección con contraseña** elimina el riesgo de robo de archivos de contraseñas, dado que estas nunca se almacenan en el dispositivo del usuario ni en ningún sistema backend; las contraseñas tampoco se transmiten nunca por Internet.

El **camuflaje criptográfico** es una tecnología de ocultamiento de claves patentada que se utiliza para proteger las credenciales únicas de CA Auth ID y CA Mobile OTP de los ataques de fuerza bruta o diccionario.

Dos componentes óptimos en su clase que pueden implementarse individualmente o juntos.



Soluciones o productos relacionados

- **CA Mobile API Gateway** crea relaciones de confianza entre el usuario, la aplicación y el dispositivo, y da seguridad a las comunicaciones entre el dispositivo y los sistemas backend.
- **CA Single Sign-On** ofrece una base de administración de seguridad centralizada que permite el inicio de sesión único en la web en las aplicaciones locales, alojadas o de socios de negocios, para sus clientes y socios de negocios.

Para obtener más información, visite **ca.com/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, pasando por la administración y la seguridad, CA trabaja con empresas en todo el mundo para cambiar el estilo de vida y la forma de realizar transacciones y comunicarse, mediante entornos móviles, de nubes públicas y privadas, de mainframe y distribuidos. Obtenga más información en **ca.com/ar**.

CS200-290570_0717