Mejore la Autenticación sin Generar Fricción con sus Usuarios

A medida que la sociedad pasa cada vez más tiempo en el mundo online y los ciberataques son cada vez más poderosos, la combinación tradicional de Nombre de Usuario/Contraseña realmente ya no es un mecanismo adecuado para proteger a sus clientes. Las organizaciones requieren sofisticadas y amigables estrategias de verificación que ofrezcan protección contra accesos no autorizados y brechas de datos. La solución con la que usted cuenta actualmente debería estar en capacidad de adaptarse a las cambiantes condiciones del cibercrimen sin convertirse, a la vez, en una molestia para sus clientes.

¿Pero qué pasaría si usted pudiera tener lo mejor de ambos mundos: fuerte protección contra ciberamenazas y cero fricción con sus usuarios? Ahora lo puede tener. Gracias a la más avanzada autenticación de usuarios, es posible detener a los criminales con una tecnología tan transparente que sus usuarios ni siquiera sabrán que se encuentra ahí.

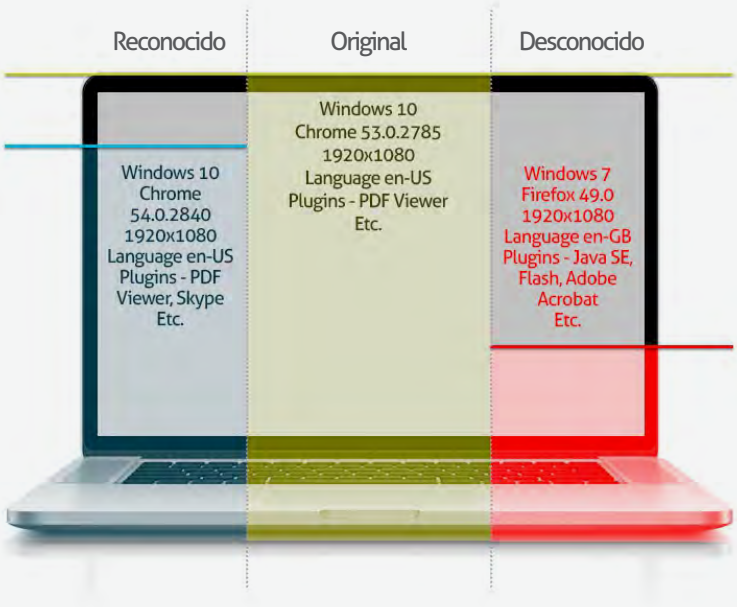
EASYSOLUTIONS®
TOTAL FRAUD PROTECTION

Identificación de Dispositivos: Fuerte Autenticación con Cero Fricción

La reciente explosión en el número de dispositivos en hogares y empresas, incluyendo computadoras de escritorio, portátiles, smartphones, tabletas, televisores inteligentes y módulos IOT (internet en las cosas), ha impulsado a las compañías a buscar métodos para controlar apropiadamente el acceso a sus recursos online. El hecho de que la combinación Nombre de Usuario/Contraseña ya no sea considerada como un nivel de protección hace que la seguridad digital se convierta en una tarea mucho más compleja. Esto está llevando a las empresas a añadir diversos niveles de autenticación para la transmisión de información sensitiva que no comprometan la facilidad de uso.

Las tecnologías de identificación de dispositivos ya han estado disponibles por un buen tiempo, usualmente como uno más de los niveles dispuestos por las entidades para asegurar el acceso mientras se brinda un nivel general de conveniencia. Sin embargo, muchas soluciones de identificación de dispositivos no fueron originalmente creadas para soportar la masiva entrada de nuevos dispositivos, ni para manejar el correspondiente flujo de actualizaciones, aplicaciones, o incluso fuentes, que son añadidas a los dispositivos con el tiempo.

Easy Solutions ofrece un sistema de identificación de navegadores basado en una tecnología heurística única que tiene en cuenta los cambios inesperados para minimizar retos innecesarios o activaciones adicionales de autenticación. Este sistema reduce las tasas de colisión, maximiza la precisión y logra una mejor identificación de los dispositivos conocidos, mientras reduce los falsos positivos.



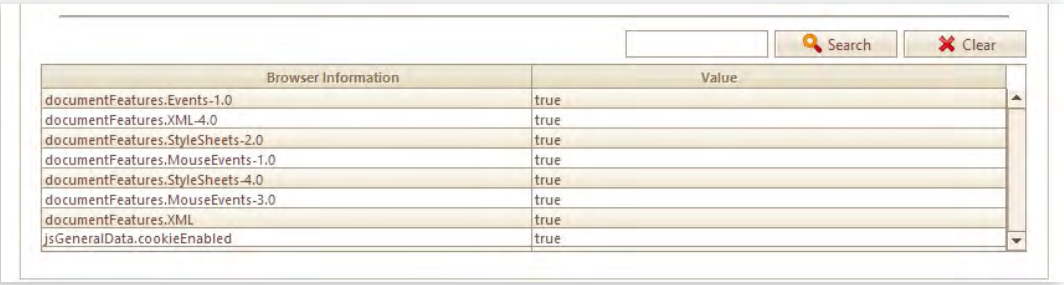
No bloquee a sus clientes legítimos – identifique cambios reales en sus dispositivos, mientras detecta aquellos dispositivos potencialmente fraudulentos.

Cómo Funciona la Identificación de Dispositivos

Los portátiles, las computadoras de escritorio y los dispositivos inalámbricos están en perpetua evolución: los plugins son constantemente añadidos y eliminados, las fuentes son cambiadas y redimensionadas, los sistemas operativos son actualizados, y los usuarios cambian el contraste o brillo de sus pantallas y borran el caché para liberar espacio en disco. Todo lo anterior puede causar problemas con la identificación de dispositivos, ya que las especificaciones de un dispositivo en particular puede que no sean las mismas la próxima vez que sea utilizado para acceder a la plataforma online de una institución financiera. No obstante, nuestro algoritmo de autenticación de dispositivos se adapta ante estos cambios normales y conserva la capacidad para identificar dispositivos con precisión, mientras detecta efectivamente la aparición de dispositivos no antes vistos.

En el momento en que un usuario final se conecta al sitio web de una institución, un componente JavaScript previamente insertado en la página de inicio de sesión de dicho sitio recolecta las numerosas características del dispositivo y del navegador. Los datos reunidos son enviados a los servidores backend, los cuales analizan la información y realizan la identificación del dispositivo, incluso si el usuario se está conectando en modo "incognito".

El primer paso para analizar los datos es crear una ID de dispositivo cifrada (hashed) y ver si corresponde con otras IDs previamente usadas por el titular de la cuenta. De ser así, se considera que el dispositivo ha sido identificado exitosamente. El proceso, sin embargo, no se detiene ahí (lo cual es el caso en otras soluciones). De no encontrarse una correspondencia, el siguiente paso es un análisis completo de los datos contextuales para determinar si de hecho se trata del mismo dispositivo, solo que con ciertos cambios realizados por el usuario.



La solución también analiza otras 10 variables críticas que brindan una sólida comparación entre el actual estado del dispositivo y previas huellas digitales almacenadas en la base de datos. Cada una de estas variables cuenta con una lógica de comparación única. Por ejemplo, la forma en que los elementos canvas y las fuentes del navegador cambian es analizada de forma diferente. Cada variable tiene un peso o valor predeterminado basado en la probabilidad de que este valor sea manipulado. De esta forma, si se detecta un cambio en una variable con alta probabilidad de manipulación, dicho cambio (sin importar que tan grande sea) será considerado de poco peso, y no disminuirá el porcentaje general de similitud de forma significativa. Este proceso de pesaje se realiza a la par con el pesaje de configuración realizado por la institución (Easy Solutions ofrece esta opción a nuestros clientes). Las variables críticas de dispositivos son las siguientes:

- Fuentes
- Plugins
- Canvas
- Sistema Operativo
- Agentes de Usuario
- Tipos de MIME
- Colores de Estilo
- Resolución de Pantalla
- Idioma del Navegador
- Nombre del Navegador

Cómo Funciona la Identificación de Dispositivos

A cada una de las variables se le asigna un peso por defecto. Los valores por defecto parten de nuestras extensas pruebas y son aquellos con los cuales hemos logrado la tasa más baja de falsos positivos.

Nuestra solución es apoyada por las siguientes características:

- **Cookieless** – Limpiar las cookies no afecta la identificación de dispositivos. Además, esta función hace más seguro el proceso al no verse sujeto al posible robo de cookies.
- **Enfoque Heurístico** – La identificación de dispositivos opera al realizar una comparación inteligente entre el dispositivo actual y los perfiles (huellas digitales) almacenados en la base de datos.
- **Bajas Tasas de Colisión** – Cuando un dispositivo es confundido con otro similar se denomina "colisión". Este fenómeno es extremadamente bajo en nuestra solución.
- **"Lista Blanca" de Usuarios Finales** – Una vez autenticado, el usuario final puede elegir si desea añadir su dispositivo a la "Lista Blanca" de dispositivos registrados, u omitir este paso si el dispositivo usado es público o inseguro (p.ej. computadores de hotel o café internet, o si la conexión es realizada a través de redes Wi-Fi públicas).

Nuestra identificación de dispositivos no es solo efectiva a la hora de distinguir entre dispositivos registrados o visitantes nuevos (y potencialmente peligrosos) basándose en los navegadores web. Nuestra solución también cuenta con una versión para plataformas móviles donde los SDKs (Kits de Desarrollo de Software, por su sigla en inglés) pueden ser insertados en la aplicación móvil nativa de la institución. De esta forma, los usuarios pueden disfrutar del mismo nivel de autenticación segura y sin fricción al iniciar sesión en la aplicación móvil bancaria.

La tolerancia del motor de correspondencias puede ser ajustada, permitiendo así que sea más estricta o flexible al determinar coincidencias de dispositivos. Esto les permite a las instituciones configurar el sistema de acuerdo a su entorno y asegurar que los niveles apropiados de cambios en los dispositivos sean medidos con precisión.

Múltiple Identificación Dinámica de Dispositivos – Identifique todos los dispositivos de los usuarios, incluyendo aquellos actualizados o utilizados en modo de navegación "incógnita".

Identificación de Dispositivos: Integración Rápida y Sin Dolor

Adicionalmente, el peso e importancia de cada variable pueden ser modificados. Estos valores son pre-configurados con base en los resultados de nuestras propias investigaciones para permitir que la solución entre en funcionamiento tan pronto sea instalada. Esta inmediata disponibilidad funciona en un rango global de entornos y dispositivos. Sin embargo, los valores pueden ser configurados de acuerdo a sus necesidades específicas.

Este enfoque dinámico aplicado a la autenticación de dispositivos de usuario le brinda al departamento IT de su organización toda la libertad para lograr el perfecto equilibrio entre acceso exclusivo para coincidencias exactas o acceso estándar para todo dispositivo. De ser muy flexible, se corre el riesgo de otorgar el acceso a los cibercriminales, y de ser muy estricto, los usuarios posiblemente tendrán que registrar su dispositivo cada vez que quieran acceder a la plataforma online o aplicación móvil, lo cual llevará a la erosión de la experiencia de uso, no muy diferente a la erosión causada por sistemas tradicionales de autenticación de usuarios.

Es importante recordar que la ventaja más grande que la autenticación de dispositivos posee sobre otros tipos de autenticación es su habilidad para suministrar una protección fuerte casi invisible al usuario final. Una agradable experiencia de uso es casi tan importante como el nivel de seguridad, quizás incluso más importante. Un cliente feliz es un cliente leal, pero un cliente frustrado es uno que muy probablemente esté pensando en cambiar de institución.

Sobre Easy Solutions

Easy Solutions® es un proveedor líder de seguridad digital enfocado en la detección y prevención total del fraude electrónico a través de todos los dispositivos, canales y servicios en la nube. Nuestra línea de productos abarca desde protección contra amenazas digitales y navegación segura, hasta autenticación multifactorial y detección de anomalías transaccionales, ofreciendo así un único destino para la más completa protección anti-fraude.

Las actividades online de más de 100 millones de usuarios en 385 importantes compañías financieras, firmas de seguridad, cadenas de retail, aerolíneas y otras entidades alrededor del mundo están protegidas por la plataforma de Protección Total contra Fraude® de Easy Solutions

Easy Solutions es orgulloso miembro de importantes organizaciones de banca y seguridad como APWG (Anti-Phishing Working Group), y FIDO (Fast IDentity Online), y nuestra suite Digital Threat Protection es avalada por la Asociación de Banqueros Americanos (ABA).

Para mayor información, visítenos en http://www.easysol.net o síganos en Twitter en @goeasysol

EASYSOLUTIONS®
TOTAL FRAUD PROTECTION

w w w . e a s y s o l . n e t s a l e s @ e a s y s o l . n e t