Entrust Datacard™

+1-888-690-2424

entrust@entrust.com

entrust.com

@EntrustDatacard

+entrust

/EntrustVideo

/EntrustSecurity

Entrust Datacard Reputación del dispositivo

Aproveche el análisis para mejorar la seguridad y minimizar los problemas para el usuario

Con el negocio digital en aumento, las exigencias de los usuarios evolucionan rápidamente por disfrutar de experiencias seguras y sin complicaciones. La atracción y la retención de clientes son fundamentales para el éxito empresarial, y requieren que los usuarios, como los empleados, los clientes y los consumidores, hagan negocios en cualquier momento y en cualquier lugar sin la preocupación por las actividades fraudulentas.

Además, a medida que surgen las tecnologías móviles y en la nube, las organizaciones cambian la forma de hacer negocios e implementan procesos internos más eficientes, lo que mejora las experiencias del usuario y ofrece nuevos productos y servicios. Entrust Datacard le proporciona las herramientas para satisfacer las demandas de la transformación comercial digital con procesos de identificación confiables y autenticación de última generación.

La reputación del dispositivo de Entrust Datacard les permite a las organizaciones proporcionar a sus usuarios una experiencia transparente y segura al permitir una autenticación intensificada solo si el dispositivo registrado de un usuario se considera un riesgo.

Beneficios

- Proporciona una experiencia de usuario transparente y sin complicaciones
- Evita el fraude y el abuso en tiempo real, antes de iniciar sesión
- Encuentra patrones sutiles con poderosos análisis para combatir el fraude de la manera más efectiva
- Toma decisiones basadas en los datos con evidencia detallada del fraude
- El análisis profundo y el aprendizaje automático se adaptan rápidamente a los tipos de fraude cambiantes
- Evita que los dispositivos anteriores marcados como fraudulentos accedan a la red y a la aplicación de la empresa
- Recopila información de riesgo sobre el dispositivo antes de iniciar sesión

Reconozca, detecte y detenga el fraude en seco

La reputación del dispositivo de Entrust Datacard es parte de nuestra plataforma de última generación y utiliza la mejor identificación de dispositivos, el contexto de riesgo dinámico y el análisis de una red de inteligencia mundial para transformar los procesos de autenticación estáticos de un factor en soluciones flexibles de múltiples factores. La reputación del dispositivo reconoce y detecta el comportamiento fraudulento en todos los tipos de dispositivos de Internet, incluidos los de escritorio, dispositivos móviles y tabletas, incluso antes de iniciar sesión, y se integra con sitios web y aplicaciones.

El poder de tres: autenticación de última generación

Una identificación confiable y una plataforma poderosa de autenticación son esenciales para el éxito del negocio digital. Las empresas ya no buscan una solución centralizada, sino que ahora buscan una plataforma de autenticación de última generación que les permita a los usuarios luchar contra el fraude.

Amplitud, profundidad y flexibilidad

La reputación del dispositivo y otras fuentes de información se pueden usar en el motor flexible de Entrust IdentityGuard, y se combinan con soluciones de múltiples factores de amplia variedad. Con más de 17 métodos de autenticación, incluida la autenticación automática móvil, una amplia variedad de casos de uso, capacidades de autenticación flexibles y una cartera completa de integraciones, puede abordar las necesidades inmediatas actuales y adaptarse rápidamente a medida que el negocio digital evoluciona. Le proporcionamos la plataforma de autenticación preferida para las exigencias del negocio digital.

Reputación del dispositivo de Entrust Datacard

Aproveche el conocimiento del dispositivo para mejorar la seguridad y minimizar los problemas del usuario

Análisis del dispositivo de Entrust Datacard

Identificar patrones de fraude

Para ayudarlo a diferenciar con precisión a los estafadores de los usuarios de confianza, identifica conductas de dispositivos riesgosas que incluyen:

- Técnicas de evasión: Identificar transacciones fraudulentas originadas por lo siguiente:
  - La redirección u ocultamiento del uso o la ubicación de un dispositivo a través de redes TOR y servidores proxy
  - Simulación artificial de un dispositivo móvil y su sistema operativo a través de una aplicación de escritorio
- Anomalías del dispositivo: Incluye incompatibilidades de la ubicación, cambio de la zona horaria y dirección de IP, demasiados dispositivos por cuenta y límites de velocidad excedidos
- Ubicaciones de alto riesgo, IP y proveedor de servicios de Internet (ISP): Incluye ubicaciones geográficas de alto riesgo, IP o ISP malignos, o ubicaciones que violan una política comercial específica

Análisis avanzado

Nuestras capacidades avanzadas de prevención y detección de fraude extienden la protección a los patrones de fraude que más le preocupan. Por ejemplo, la reputación del dispositivo puede informarle:

- Si se ha utilizado un dispositivo en particular para acceder a varias cuentas dentro de un período de tiempo en particular
- Cuando muchos dispositivos se han utilizado para acceder a una sola cuenta
- Si el dispositivo tiene un historial de tipos específicos de actividad fraudulenta
- Cuando el dispositivo está vinculado a otros dispositivos o cuentas asociadas con el fraude
- Si el dispositivo ha violado políticas específicas que usted ha determinado, como la ubicación geográfica, el comportamiento abusivo por chat y los límites de gastos o engaños

Toda esta información se recopila y se analiza en milisegundos antes de que el dispositivo inicie sesión en la red

Características principales

Identificación y registro del dispositivo: Confirma la identidad del usuario mediante la coincidencia de las huellas digitales del dispositivo con un alto grado de precisión y empareja de forma explícita la identificación del dispositivo benigno con la cuenta del usuario.

Tolerancia del cambio del dispositivo: Los sistemas de autenticación basados en dispositivos más débiles son superados por la tendencia natural provocada por actualizaciones, aplicaciones nuevas o incluso fuentes nuevas. Y la tecnología de coincidencias parciales tiene en cuenta los cambios esperados del dispositivo para minimizar las respuestas "negativas" innecesarias y crear límites de "riesgo aceptable".

Revelar conexiones ocultas: Comprender cómo un dispositivo se vincula con una actividad maligna o con otros usuarios le permitirá ejecutar de forma automática los desafíos de autenticación intensificada si se exceden los límites de riesgo.

Detección de evasión: El localizador de proxy (proxy piercing) detecta servidores proxy que a menudo son utilizados por estafadores y timadores, y aprovecha técnicas avanzadas para desenmascarar las redes TOR, VPN, máquinas virtuales móviles, emuladores u otras actividades anónimas.

Plataforma mundial de inteligencia del dispositivo: La información analítica de dispositivos en tiempo real de miles de analistas de riesgo señalan las cuentas y dispositivos sospechosos de forma inmediata.

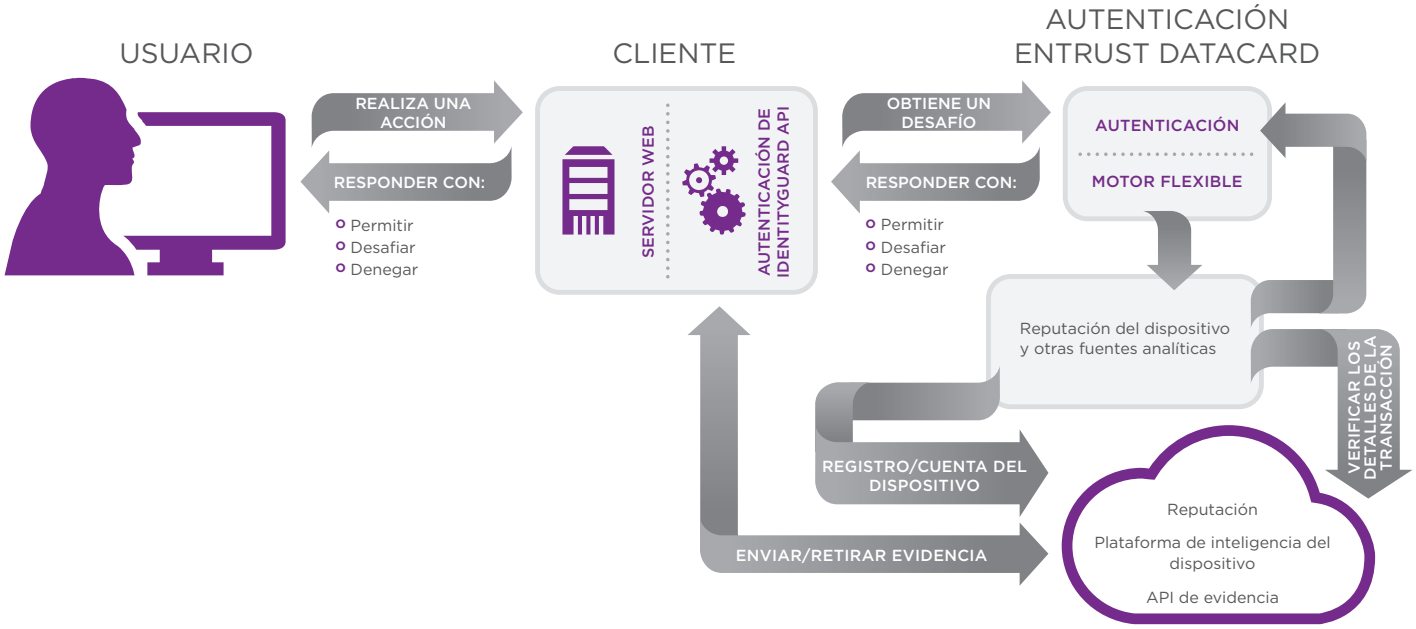
Precisión sin información de identificación personal: La tecnología de reconocimiento utiliza cientos de características del dispositivo y la orientación única entre sí para identificar de forma inmediata un dispositivo sin la necesidad de la información de identificación personal del usuario.

Cómo Entrust Datacard implementa la reputación del dispositivo

Agregar seguridad en niveles para reducir la participación del usuario proporciona una experiencia impecable y transparente, y solo depende de la autenticación de múltiples factores cuando es necesario, lo que les brinda a las organizaciones el equilibrio adecuado entre seguridad y funcionalidad.

Según la configuración del análisis basado en riesgos, la solución proporciona una recomendación como la siguiente:

- **Permitir:** el dispositivo es seguro y la política expresa que eso es todo lo que se requiere
- **Desafío:** el dispositivo puede estar bajo revisión y la política identifica que se requiere otro factor para la autenticación
- **Denegar:** el dispositivo se marca como inseguro y la autenticación se rechaza de inmediato



Reputación del dispositivo de Entrust Datacard

Aproveche el conocimiento del dispositivo para mejorar la seguridad y minimizar los problemas del usuario

Casos de uso para instituciones financieras y empresas

Banca

Nueva creación de cuenta: Ofrezca servicios nuevos de forma segura mediante la verificación de la identidad de la integridad del dispositivo del cliente cuando crean de forma digital una cuenta en línea o a través del dispositivo móvil.

Banca en línea y móvil: Permita que los usuarios accedan a la información de la cuenta con una experiencia impecable y transparente, y solo habilite la autenticación intensificada cuando el riesgo sea elevado.

Verificación de transacciones: La verificación de las transacciones fuera de banda ayuda a evitar ataques fraudulentos avanzados agregando niveles de seguridad y evaluando la integridad del dispositivo.

Empleados

Verificación previa de dispositivos personales: Asegura la integridad de los dispositivos de los empleados nuevos antes de permitir el acceso a la información, las herramientas y los recursos de la empresa.

Verificación previa de la identificación móvil: Se asegura de que el dispositivo del usuario no se haya asociado con ninguna actividad fraudulenta antes de proporcionar identificación segura al dispositivo.

Agilizar el acceso del usuario: Reduce la cantidad de veces que un usuario necesita autenticarse mediante el análisis del dispositivo en niveles para identificar casos de bajo riesgo.

- Aplicaciones en los servidores y en la nube
- Portales de socios y clientes

Acerca de Entrust Datacard
Los consumidores, los ciudadanos y los empleados esperan cada vez más experiencias en cualquier lugar y en cualquier momento, ya sea cuando hacen compras, cruzan fronteras, acceden a servicios electrónicos del gobierno o ingresan a redes empresariales. Entrust Datacard ofrece tecnologías de identificación confiable y de transacciones seguras que hacen que esas experiencias sean seguras y de confianza. Las soluciones varían entre el mundo físico de las tarjetas financieras, los pasaportes y las tarjetas de identificación hasta el campo digital de la autenticación, los certificados y las comunicaciones seguras. Con más de 2000 colegas de Entrust Datacard en todo el mundo y una red de importantes socios mundiales, la empresa brinda servicios a clientes en 150 países en todo el mundo.

Para obtener más información acerca de los productos y servicios de Entrust, llame al **+1-888-690-2424**, envíe un correo electrónico a **entrust@entrust.com** o visite el sitio web **www.entrust.com**.

Oficina central
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
Estados Unidos

Entrust Datacard™

xxxxx/0217