

## Entrust Datacard Device Reputation

Aproveita análises para melhorar a segurança e reduzir os problemas dos usuários

Com os negócios digitais em alta, usuários e clientes estão rapidamente passando a demandar experiências sem atritos, mas seguras. A atração e a retenção do cliente são essenciais para o sucesso da empresa e exigem que os usuários – como funcionários, clientes e consumidores – conduzam negócios em qualquer momento, em qualquer lugar, sem se preocuparem com atividades fraudulentas.

E, conforme as tecnologias de nuvem e dispositivos móveis aparecem, as organizações estão mudando a maneira de fazer negócios ao implementar processos internos mais eficientes, melhorando as experiências dos usuários e oferecendo novos produtos e serviços. A Entrust Datacard o equipa com as ferramentas para atender às demandas de transformação dos negócios digitais, com identidades confiáveis e autenticação de última geração como base.

O Device Reputation da Entrust Datacard permite que as organizações ofereçam aos seus usuários uma experiência transparente e segura, habilitando a autenticação por etapas apenas quando um dispositivo registrado do usuário representar um risco elevado.

### Reconheça, detecte e impeça fraudes no momento em que ocorrem

O Device Reputation da Entrust Datacard faz parte da nossa plataforma de última geração e usa a identificação de dispositivos, um contexto dinâmico de risco e análises de uma rede global de inteligência da melhor qualidade para transformar processos de autenticação estáticos com um fator único em soluções adaptáveis com fatores múltiplos. O Device Reputation reconhece e detecta comportamentos fraudulentos em todos os tipos de dispositivos da internet, incluindo computadores desktop, dispositivos móveis e tablets, mesmo antes do acesso, e é integrado a websites e aplicativos.

### O poder do três – autenticação de última geração

Identidades confiáveis com uma potente plataforma de autenticação são essenciais para o sucesso dos negócios digitais. As empresas não estão mais procurando por uma solução de um único fator, e estão buscando uma plataforma de autenticação de última geração que capacitará seus usuários enquanto lutam contra fraudes.

#### Amplitude, profundidade e flexibilidade

O Device Reputation e outros recursos de análise podem ser usados no mecanismo adaptável do IdentityGuard da Entrust e pareados com soluções de ampla gama e múltiplos fatores. Com mais de 17 métodos de autenticação – incluindo autenticação push para dispositivos móveis – uma grande escala de casos de utilização, recursos de autenticação adaptável e um portfólio abrangente de integrações, você pode atender às suas necessidades imediatas hoje e rapidamente se adaptar conforme seus negócios digitais se desenvolvem. Oferecemos a você a plataforma de autenticação de sua escolha para as demandas dos negócios digitais.

**+1-888-690-2424**

entrust@entrust.com  
entrust.com

 **@EntrustDatacard**

 **+entrust**

 **/EntrustVideo**

 **/EntrustSecurity**

#### Benefícios

- Proporcione ao usuário uma experiência transparente e sem atritos
- Impeça fraudes e violações em tempo real, antes do acesso
- Encontre padrões sutis com análises potentes para combater as fraudes de maneira mais efetiva
- Tome decisões baseadas em dados, com evidências detalhadas de fraude
- As análises profundas e a aprendizagem automática rapidamente se adaptam às novas tendências de fraude
- Evite que dispositivos anteriormente identificados como fraudulentos acessem sua rede e os aplicativos da empresa
- Obtenha informações de risco sobre o dispositivo antes do acesso



# Device Reputation da Entrust Datacard

Aproveita a análise de dispositivos para melhorar a segurança e reduzir os problemas dos usuários

## Device Analytics da Entrust Datacard

### Identifique padrões de fraude

Para o ajudar a separar de forma precisa os fraudadores dos usuários confiáveis, identifique comportamentos de risco do dispositivo, incluindo:

- Técnicas de evasão: Identifique transações fraudulentas que começam ao:
  - Redirecionar ou ocultar o uso ou local de um dispositivo por meio de servidores proxy e redes TOR
  - Simular artificialmente um dispositivo móvel e seu sistema operacional por meio de um aplicativo de computador desktop
- Anomalias do dispositivo: Inclui incompatibilidade de localização, alterações de fuso horário e endereço IP, muitos dispositivos por conta e limites de velocidade excedidos
- Localizações, IPs e ISPs de alto risco: Inclui localizações geográficas de alto risco ou protocolos de internet (Internet Protocol, IP) e provedores de serviço de internet (Internet Service Provider, ISP) sabidamente incorretos, ou localizações que violam sua política específica de negócios

### Análises avançadas

Nossos recursos avançados de detecção e prevenção estendem sua proteção aos padrões de fraude que mais o preocupam. Por exemplo, o Device Reputation pode informá-lo:

- Se um determinado dispositivo foi usado para acessar múltiplas contas em um determinado período de tempo
- Quantos dispositivos foram usados para acessar uma única conta
- Se o dispositivo tem um histórico de tipos específicos de atividade fraudulenta
- Quando o dispositivo estiver conectado a outros dispositivos ou contas associados a fraudes
- Se o dispositivo violou políticas específicas que você definiu, como geolocalização, violação de chat, limites de gastos ou fraude

Todas essas informações são reunidas e analisadas em milissegundos antes de o dispositivo acessar a sua rede

## Principais recursos

**ID do dispositivo e registro:** Confirma a identidade do usuário ao fazer a correspondência das impressões digitais do dispositivo com um alto grau de precisão, e ao parear explicitamente as identidades dos dispositivos sabidamente corretos com a conta do usuário.

**Tolerância de alteração no dispositivo:** Sistemas de autenticação mais fracos instalados no dispositivo são vencidos pelo desvio natural causado por atualizações, novos aplicativos ou mesmo novas fontes. E a tecnologia de correspondências parciais leva em consideração as alterações esperadas no dispositivo para minimizar respostas “negativas” desnecessárias e criar limites de “risco aceitável”.

**Revele conexões ocultas:** Compreender de que forma um dispositivo está conectado a uma atividade sabidamente incorreta, ou outros usuários permitirão que você automaticamente aplique confirmações de autenticação por etapas, se os limites de risco forem excedidos.

**Detecção de evasão:** O proxy piercing detecta servidores proxy que são frequentemente usados por fraudadores e golpistas, ao mesmo tempo que aproveita as técnicas avançadas para desmascarar redes TOR, redes privadas virtuais (Virtual Private Network, VPN), máquinas virtuais (Virtual Machines, VM) de dispositivos móveis, emuladores ou outras atividades de anonimato.

**Plataforma global de inteligência de dispositivos:** Feedback analítico do dispositivo em tempo real de milhares de contas e dispositivos suspeitos imediatamente identificados por analistas de risco.

**Precisão “PII-less”:** A tecnologia de reconhecimento usa centenas de atributos de dispositivos e suas orientações únicas entre si para identificar instantaneamente um dispositivo, sem a necessidade de informações pessoais de identificação do usuário.

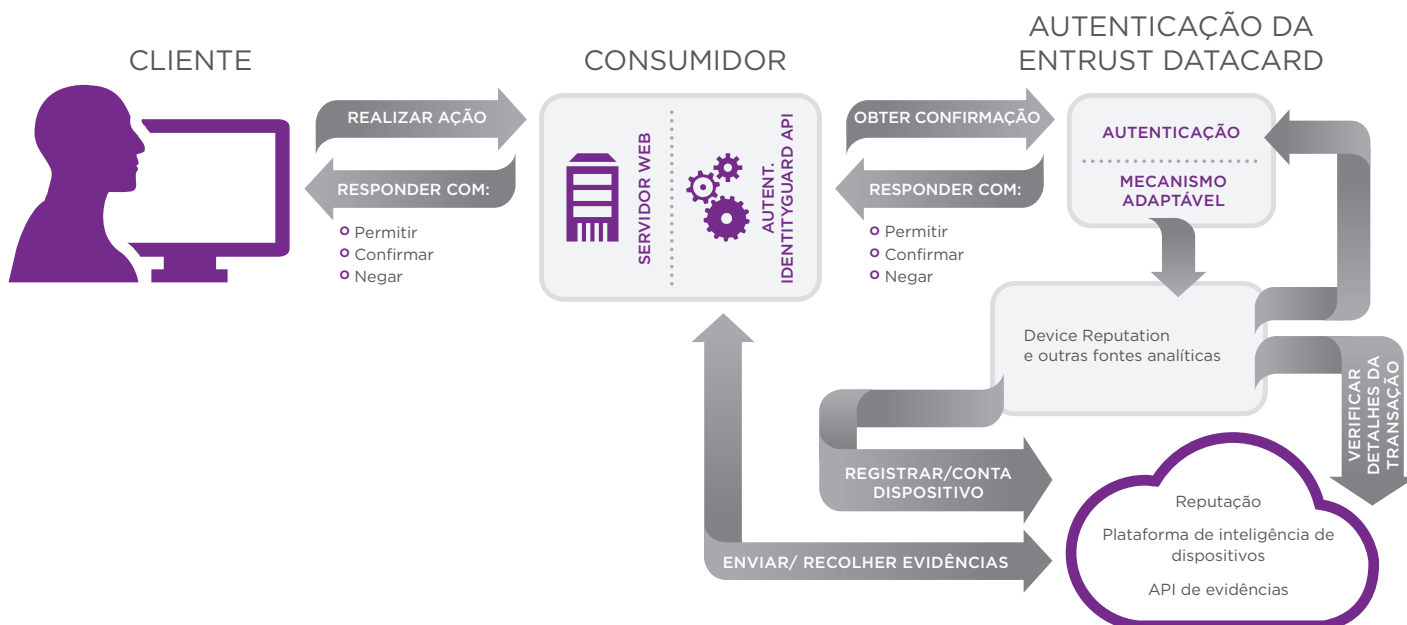
## Como a Entrust Datacard aplica o Device Reputation

Adicionar uma segurança em camadas para reduzir o envolvimento do usuário proporciona uma experiência perfeita e transparente e apenas recorre à autenticação de múltiplos fatores quando necessário – dando às organizações o equilíbrio certo entre segurança e funcionalidade.



Com base na configuração de Análise baseada em riscos, nossa solução oferece uma recomendação, como a seguinte:

- **Permitir:** dispositivo é confiável, e a política diz que isso basta
- **Confirmar:** dispositivo pode estar sob análise, e a política identifica que outro fator para autenticação é necessário
- **Negar:** dispositivo foi identificado como não confiável, e a autenticação é recusada de imediato



# Device Reputation da Entrust Datacard

Aproveita a análise de dispositivos para melhorar a segurança e reduzir os problemas dos usuários

## Casos de utilização para empresas e instituições financeiras

### Transações bancárias



**Nova criação de conta:** Ofereça de maneira segura novos serviços ao comprovar a integridade do dispositivo do seu cliente, quando ele cria uma conta on-line ou por meio dos dispositivos móveis dele.

**Transações bancárias on-line e por dispositivos móveis:** Possibilite que os seus usuários acessem informações da conta com uma experiência perfeita e transparente e que apenas habilite a autenticação por etapas quando o risco é elevado.

**Verificação de transações:** A verificação de transações sem necessidade de conexão ajuda a acabar com os ataques de fraude avançados ao adicionar uma camada de segurança e avaliar a integridade do dispositivo.

### Funcionário



**Pré- Checagem do tipo “traga o seu próprio dispositivo” (Bring Your Own Device, BYOD):** Garanta a integridade do dispositivo do seu novo funcionário antes de emitir acesso às informações, ferramentas e recurso da empresa.

**Pré- Checagem da identidade do dispositivo móvel:** Garanta que o dispositivo do usuário não esteja associado a nenhuma atividade fraudulenta antes de uma identidade confiável ser providenciada para o dispositivo.

**Agilize o acesso do usuário:** Reduza a quantidade de vezes que o usuário precisa autenticar, ao sobrepor as análises do dispositivo para identificar situações de baixo risco.

- Aplicativos de nuvem e instalados no servidor do usuário
- Portais dos parceiros e clientes

### Sobre a Entrust Datacard

Consumidores, cidadãos e trabalhadores esperam ter, cada vez mais, experiências em qualquer lugar, em qualquer momento – seja ao fazer compras, cruzar fronteiras, ou acessar serviços de governo eletrônico ou redes corporativas. A Entrust Datacard oferece as tecnologias de identidade confiável e de transações seguras que tornam essas experiências confiáveis e seguras. As soluções vão desde o mundo físico dos cartões de banco, passaportes e documentos de identidade ao campo digital da autenticação, dos certificados e da comunicação segura. Com mais de 2.000 colaboradores da Entrust Datacard no mundo, e uma rede de fortes parceiros globais, a empresa atende a clientes em 150 países.

Para mais informações sobre os produtos e serviços da Entrust Datacard, ligue para **+1-888-690-2424**, envie um e-mail para [entrust@entrustdatacard.com](mailto:entrust@entrustdatacard.com) ou visite [www.entrustdatacard.com](http://www.entrustdatacard.com).

### Sede

Entrust Datacard  
1187 Park Place  
Shakopee, MN 55379  
EUA

