feedzai

Solution Guide

Digital Trust

feedzai

Conteúdo

Introdução 03
Prevenção de ataques de representação e manipulação 05
Como a confiança digital impede os ataques de representação 05
Como a confiança digital impede ataques de manipulação 06
Verificação Abrangente e Contínua do Usuário 07

Componentes de confiança digital 10
Colete 11
Dados biométricos comportamentais 12
Dados de Análise Comportamental 12
Dados de impressão digital do dispositivo 12
Dados de rede 12
Padrões de malware e ameaças Dados da Intel 12
Revelar 13
Prevenção de fraudes de representação e ataques de manipulação 14
Ataques de roubo de credenciais 14
Ataques Alimentados por credenciais roubadas 14
Ataques de manipulação 15
Responder 16

Operações de confiança digital 18
Biometria comportamental e o BionicID™ 19
Detecção de ator ruim de sessão única 20
Detecção de controle de conta amigável 21
Detecção biométrica comportamental de maus atores™ 22
Detecção de Malware 23
Banco de Dados de Impressões Digitais do Dispositivo 24
Detecção de emulador 24
Avaliação de rede 25
Detecção de bots 26

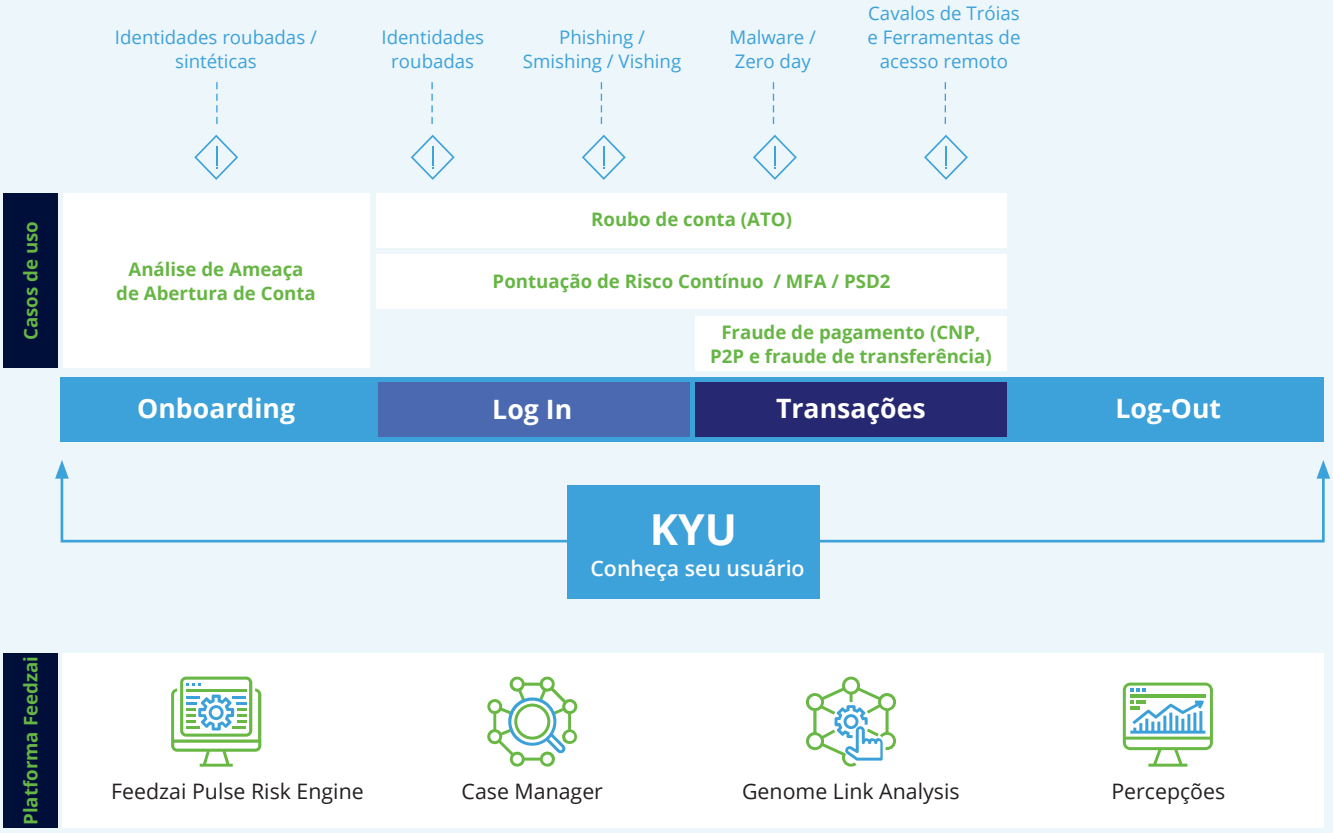
Casos de uso 27
Pontuação de risco contínua e em tempo real 27
Prevenção de roubo de conta (ATO) 28

Integração rápida e fácil 29
Visão geral da implantação 29

1. Introdução

O Digital Trust da Feedzai, é uma solução SaaS/baseada na nuvem que permite aos serviços financeiros e às empresas Fintech revelar e responder a ataques de representação e manipulação de identidade online desde o início de sessão até ao fim de sessão, em todas as interações do utilizador, tudo sem prejudicar o cliente experiência.

As Instituições Financeiras (IFs) usam o Digital Trust para pontuação de risco contínua que permite Autenticação de Cliente Forte (SCA) e PSD2 totalmente silenciosa e totalmente transparente. Também é usado para impedir o controle de conta (ATO).



A primeira linha de defesa que o Digital Trust oferece protege os usuários finais e clientes bancários contra ataques de malware e phishing destinados a roubar credenciais de usuários ou assumir sessões para cometer fraudes.

Uma segunda linha de defesa mais profunda combina biometria comportamental do usuário (como você digita, desliza, segura e usa seu dispositivo para acessar um aplicativo móvel ou web protegido), análise comportamental (quando e o que você faz), dados do dispositivo e da rede e analisando esses dados usando modelos híbridos de Inteligência Artificial, incluindo Deep Learning para criar um **BionicID™** para cada usuário, no momento da inscrição. A partir desse ponto, o **BionicID™** é continuamente atualizado e analisado a cada interação para conhecer seu usuário **(KYU)** minuciosamente. O sistema examina a identidade do usuário realizando cada ação, permitindo que os usuários verificados prossigam enquanto bloqueiam os fraudadores.

Digital Trust proporciona a capacidade de realizar a defesa ativa e a defesa preventiva.

A maneira mais eficiente de proteger ativamente os usuários é interromper as perdas por fraude antes que elas ocorram. A segunda maneira mais eficiente é permitir que as equipes de fraude configurem processos automatizados que evitem ataques de personificação e bloqueiem atores mal-intencionados conhecidos – interrompendo a fraude e minimizando a carga de trabalho dos analistas de fraude. O Digital Trust inclui recursos de Defesa Ativa e Defesa Preemptiva que evitam automática e proativamente perdas por fraude, melhoram a eficiência operacional de fraude e evitam experiências negativas do cliente.

1.1. Prevenção de ataques de representação e manipulação

O Digital Trust combina biometria comportamental, análise comportamental, detecção avançada de malware e avaliação de rede e dispositivo com modelos híbridos de Inteligência artificial, incluindo Deep Learning, para criar e analisar continuamente o BionicID™, conhecer seu usuário (KYU), identificar agentes mal-intencionados e mitigar riscos independentemente do tipo de ataque.

Do login ao logout, em todas as interações, a solução tudo-em-um detecta de forma não intrusiva anomalias comportamentais e ambientais, protegendo os clientes contra ataques de falsificação de identidade e manipulação. Isso inclui trojans de acesso remoto, malware de dia zero, bots e ataques baseados em engenharia social.

Como a confiança digital impede os ataques de representação

Os **ataques de representação** começam com credenciais roubadas. O Digital Trust da Feedzai bloqueia ataques de personificação impedindo que ataques de malware ou phishing roubem as credenciais do usuário em primeiro lugar. A **Feedzai Active Defense** também permite que as instituições financeiras determinem as ações apropriadas quando ataques de malware ou phishing são detectados nos dispositivos dos usuários. Os usuários são imediatamente, automaticamente e frequentemente protegidos silenciosamente contra ameaças enquanto as equipes de fraude das instituições financeiras são alertadas automaticamente**.**

No mundo pós-violação de hoje, as credenciais roubadas estão prontamente disponíveis para os malfeitores usarem para se passar por usuários legítimos. Os ataques de credenciais roubadas exigem uma abordagem diferente para serem interrompidos, pois são executados por bots de preenchimento de credenciais e manualmente por humanos. Esses tipos de ataques são detectados e o controle de contas é impedido pela análise do **BionicID™**.

Como a confiança digital impede ataques de manipulação

Os ataques de manipulação utilizam software de acesso remoto, por meio de injeções de malware na Web ou sobreposições de aplicativo/tela, e enganam as vítimas para que executem um ataque RAT. Ambos os tipos de ataques são projetados para obter o controle do dispositivo da vítima.

Com mais frequência, os cibercriminosos buscam obter o controle da sessão bancária de um usuário. Essa forma de ataque é mais fácil de executar porque ignora a segurança tradicional da conta, permitindo que um malfeitor assuma temporariamente o controle da conta da vítima. A análise **Active Defense BionicID™** da Feedzai pode detectar e derrotar ambos os tipos de ataque de acesso remoto, impedindo tentativas de controle de sessão – protegendo os usuários e notificando as instituições financeiras.

O Feedzai analisa milhares de parâmetros de usuários, rede e sistema coletados durante cada interação ou operação online para proteger os usuários de ataques de personificação e manipulação. Esses dados são processados na nuvem usando modelos híbridos de inteligência artificial, incluindo Deep Learning para criar um BionicID™ para todos os usuários – sejam atores legítimos ou mal-intencionados – no momento da inscrição. O BionicID™ é continuamente atualizado e analisado a cada interação para calcular um risco holístico para cada cliente.

O BionicID™ é continuamente atualizado e analisado a cada interação para calcular uma pontuação de risco holística para cada cliente.

O sistema concede silenciosamente o acesso de usuários legítimos ou interrompe os malfeitores, dependendo do risco. As instituições financeiras têm acesso às pontuações de risco a todo momento, podendo configurar quando deve ser alertado e automatizar as ações cabíveis a serem tomadas.

Se um ataque de representação ou manipulação for detectado, as instituições financeiras recebem dois caminhos de resposta flexíveis. A primeira é proteger imediatamente os usuários no ponto de ataque. A segunda é alertar simultaneamente as equipes de fraude das instituições financeiras sobre o ataque e executar uma resposta de acompanhamento – desde enviar notificações ao usuário, intensificar a autenticação, encerrar uma sessão ou bloquear a conta – tudo para interromper a fraude antes que ela aconteça.

1.2. Verificação Abrangente e Contínua do Usuário

O principal objetivo das soluções de prevenção de fraudes têm sido tradicionalmente fazer a pergunta: “você é fraudador?” Mas abordar a prevenção de fraudes estritamente a partir do “você é fraudador?” abordagem não é uma estratégia abrangente para resolver um problema muito complexo.

User Types

Legítimos
Clientes que representam o maior percentual de usuários;

Ilegítimos
Maus atores que representam a menor porcentagem de usuários;

Indeterminado
Usuários que não podem ser facilmente classificados por serem novos proprietários de contas ou devido a uma mudança ambiental (suspeita ou não).

É por isso que a solução Digital Trust da Feedzai possui capacidades únicas de processamento biométrico que a distinguem de outras soluções ao responder à pergunta fundamental “você é realmente você?” Ambas as perguntas devem ser feitas e respondidas repetidamente, desde o login até o logout.

A primeira e principal prioridade da Feedzai é permitir que clientes legítimos acessem suas contas e bloquear fraudadores ou mal-intencionados. O Feedzai faz isso com uma análise minuciosa do BionicID™ de cada usuário em cada interação. Isso permite que os institutos financeiros realmente executam o conheça seu usuário (KYU) e separem atores legítimos de ilegítimos. Um conceito aparentemente simples, mas desafiador devido à complexidade de um terceiro tipo de usuário: o usuário indeterminado.

Uma pequena porcentagem de usuários que são classificados como indeterminados E que se revelam fraudadores são, na verdade, responsáveis pela maior parte dos custos relacionados a fraudes de institutos financeiros. Esses incluem:

- **Custos relacionados ao tratamento de falsos negativos ou falsos positivos;**
- **Perdas reais de fraude por não impedir esses maus atores;**
- **Churn de clientes resultante de fraude ou atrito excessivo resultante da implementação de tecnologias onerosas de prevenção de fraudes.**

A identificação adequada de usuários indeterminados rapidamente, sem adicionar fricção desnecessária, é fundamental para reduzir as perdas por fraude, evitar investigações de fraude e impedir a perda de negócios devido a clientes insatisfeitos. Respondendo à pergunta simples - você é realmente você? – aumenta drasticamente a velocidade e precisão com que o Feedzai consegue reduzir o número de utilizadores classificados como indeterminados e avaliar se um utilizador é legítimo ou fraudador.

Respondendo à pergunta simples - você é realmente você? – aumenta drasticamente a velocidade e precisão com que o Feedzai consegue reduzir o número de utilizadores classificados como indeterminados.

A verificação do usuário é realizada usando várias etapas:

Passo 1

Primeiro, ele identifica e filtra rapidamente os **malfeitores** conhecidos usando dados, identificadores e técnicas de análise comumente usadas no setor. A partir daí, os usuários indeterminados podem ser examinados mais de perto para separar ainda mais os clientes legítimos dos malfeitores.

Passo 2

Em seguida, a **verificação de login** garante a continuidade dos dados do BionicID™ desde o último logout até o login atual, certificando-se de que nada mudou da interação anterior para a interação atual para confirmar que apenas bons usuários conhecidos têm acesso concedido. Essa fase de verificação pode detectar rapidamente ataques de representação, identificando anomalias de dispositivo e rede – indicadores de atividade claramente suspeitos. Após a verificação da rede e do dispositivo, os dados biométricos e comportamentais são analisados em relação aos dados BionicID™ anteriores. Essa análise mais detalhada pode verificar uma tentativa de aquisição de conta, especialmente em conjunto com um dispositivo inicial e verificação de rede.

Passo 3

A etapa final é a **verificação na sessão**. Depois que um usuário é identificado e o login é concedido, a próxima fase de validação começa. A partir daqui, cada interação sucessiva (verificar saldo, movimentar fundos, etc.) realizada pelo cliente “no momento” requer uma verificação BionicID™. A verificação contínua dos clientes durante a sessão é fundamental para evitar a manipulação na sessão ou um seqüestro de sessão. Essas formas de ataque são particularmente insidiosas, pois evitam a dificuldade de cometer uma invasão de conta. Em vez disso, um malfeitor sequestra uma sessão bancária, executa uma transação fraudulenta e desaparece sem deixar vestígios. Esses ataques de representação de ponto geralmente são executados usando malware RAT. Em alguns casos, os ataques são executados por pessoas mal-intencionadas usando aplicativos legítimos, mas comprometidos, para acessar o computador de um usuário chamado Remote Access Tools.

O BionicID™ de um usuário é examinado em cada ponto da sessão para garantir que o usuário inicialmente verificado e conectado seja a mesma pessoa que executa todas as transações. Este é um dos principais casos de uso em que verificar continuamente “você é realmente você?” não apenas evita o seqüestro de sessão, mas também minimiza bastante o atrito com o cliente. A necessidade de autenticação intensificada ou multifatorial durante a jornada do cliente é eliminada.

2. Componentes de Confiança Digital

O Digital Trust é composto por **três blocos funcionais**:

Colectar
Coleta de dados de cada interação na web e móvel;

Revealando
Análise BionicID™ contínua e avaliação de risco;

Respondendo
Capacidades defensivas ativas e preventivas.

2.1. Colectar

A coleta de dados é habilitada via JavaScript para web banking e um SDK para aplicativos bancários móveis. O sistema coleta continuamente milhares de parâmetros de dados para criar o contexto do usuário que é usado para estabelecer e verificar a impressão digital ou BionicID™ de um usuário. Essas fontes de dados e parâmetros incluem:

Dados biométricos comportamentais

- Toque/tecla
- Mouse
- Sensores espaciais móveis

Dados de Análise Comportamental

- Jornada do usuário
- Verificação de velocidade
- Data/hora das conexões
-

Dados de impressão digital do dispositivo

- Características do dispositivo móvel
- Características do computador
- Informações do sistema operacional
- Formulários
- Idiomas instalados/usados

Dados de Rede

- Endereço IP/domínio/ISP/ASN
- Tipo/velocidade de conexão
- geolocalização
- Wi-Fi SSID/BSSID

Padrões de malware e ameaças aos dados da Intel

Enquanto os dados sobre cada interação do usuário são coletados, feeds de dados de terceiros e inteligência de ameaças são usados para enriquecer o que se sabe sobre o usuário e determinar se há sinais óbvios de atividade fraudulenta que são imediatamente acionáveis. Este fluxo de dados paralelo inclui:

- Assinaturas de malware
- Phishing Site locations
- Identificadores fraudulentos que podem ser conectados de volta aos dispositivos
- Rede
  - Dispositivo
  - O email
  - Número de telemóvel
- Listas de ferramentas e aplicativos relacionados a comportamento fraudulento e conhecidos por serem comumente usados por pessoas mal-intencionadas.

2.2. Revelar

Em cada ponto da jornada do cliente, o Digital Trust Anomaly Detection & Classification Engine continuamente toma decisões e determina o risco atual associado ao BionicID™ de um cliente durante cada sessão do cliente e em cada ponto da jornada do cliente.

A análise selecionada é determinada pelo tipo de dados que está sendo examinado. Isso varia de anomalias simplistas (por exemplo, comparando com endereços IP comprometidos conhecidos) a anomalias muito complexas, por exemplo, determinando alterações nos dados biométricos de um usuário) entre o BionicID™ atual e o estado anterior verificado.

Nosso mecanismo de risco usa modelos por usuário, modelos baseados em população e modelos de maus atores, juntamente com técnicas híbrida

- Árvores de decisão
- Aprendizado de máquina supervisionado
- Aprendizado de máquina não supervisionado
- Aprendizado Profundo

Prevenção de fraudes de representação e ataques de manipulação

A solução Digital Trust da Feedzai foi concebida para detetar todas as tentativas online de aquisição de contas com base na identidade:

2.2.1. Ataques de roubo de credenciais

Ataques de malware

Trojan bankers que modificam as informações que o usuário vê ou códigos projetados para roubar credenciais para executar uma aquisição de conta posteriormente.

- O Digital Trust da Feedzai identifica malware previamente descoberto e classificado usando dados de ameaças de listas brancas e negras continuamente atualizados da indústria.
- O Digital Trust da Feedzai também é capaz de identificar padrões de malware não identificados anteriormente por meio de um processo chamado “lista cinza”. Esse processo encaminha as anomalias de código recém-descobertas para o sistema de classificação de malware da Digital Trust, onde são analisadas usando algoritmos de Deep Learning sob supervisão especializada.

Ataques de phishing

Geralmente entregues por e-mails de aparência convincente, projetados para direcionar os usuários a um site fraudulento e clonado, criado para roubar suas credenciais.

- A prevenção contra phishing detecta quando um cliente clica em um link de phishing para um site fraudulento e o redireciona para fora do site prejudicial.

2.2.2. Ataques Alimentados por Credenciais Roubadas

Representação do cliente

Um ataque direcionado contra uma conta de cliente utilizando credenciais roubadas. Os ataques de representação do cliente são detectados por:

- Análise de indicadores de maus atores, incluindo dados de rede, dados de dispositivos ou outros indicadores que são continuamente analisados e comparados com dados de ameaças coletados pelo Feedzai e feeds de dados de ameaças de terceiros.
- Análise BionicID™ para determinar anomalias comportamentais ou biométricas suspeitas.

Preenchimento de credenciais

Geralmente um ataque de base ampla, conduzido por bot, utilizando credenciais roubadas e usado em uma ampla variedade de contas, tentando tirar proveito da reutilização de e-mail/senha do usuário. Os ataques conduzidos por bots são detectados por:

- Análise de indicadores de ameaças, incluindo dados de rede, dados de dispositivos ou outros indicadores de ameaças que são continuamente analisados e comparados com dados de ameaças coletados pelo Feedzai e feeds de dados de ameaças de terceiros;
- Indicadores de ameaças comportamentais que identificam a capacidade de um bot de navegar rapidamente e carregar dados de credenciais mais rápido do que humanamente possível;
- Indicadores biométricos de ameaças para detectar bots que empregam modos sofisticados de operação “baixo e lento” para copiar melhor o comportamento humano.

2.2.3. Ataques de manipulação

O Digital Trust pode detectar a diferença entre cavalos de Tróia de acesso remoto e ferramentas de acesso remoto. Em conjunto com a Defesa Ativa da Digital Trust, pode mitigar proativamente esses ataques, desativando o RAT de ataque.

Trojans de acesso remoto

Um tipo específico de malware que permite que invasores assumam o controle de um vi computador do ctim durante uma sessão bancária.

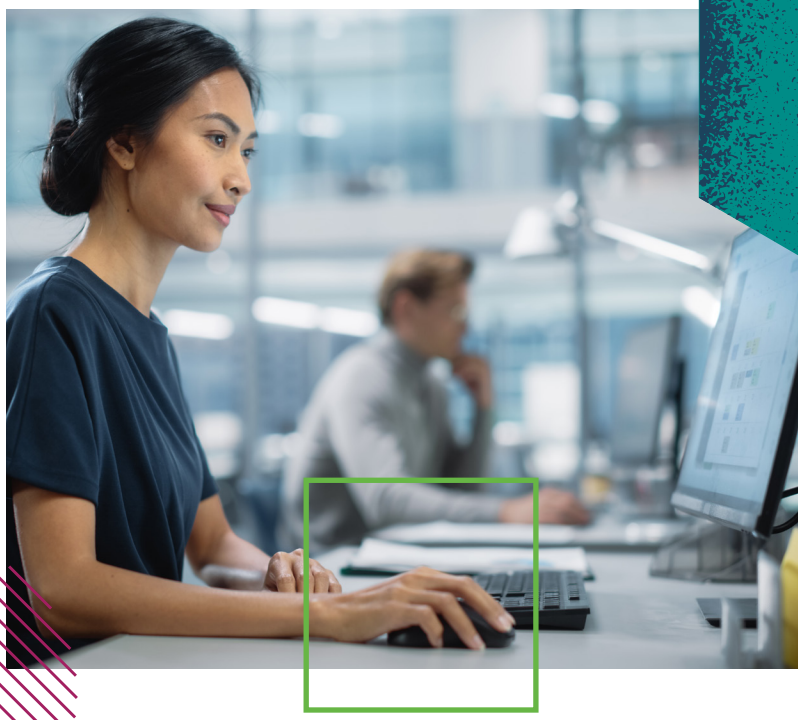
Ferramentas de acesso remoto

Aplicativos legítimos que podem ser mal utilizados por pessoas mal-intencionadas para assumir o controle total do computador de um usuário ou apenas de uma sessão.

2.3. Responder

Digital Trust Active Defense
Oferece um conjunto altamente flexível de recursos de resposta para impedir que um usuário seja manipulado para realizar uma ação que comprometa uma sessão ou exponha suas credenciais.

A proteção ativa do cliente é executada em **três etapas simultâneas:**



Etapa 1
Proteção Imediata

Quando um ataque é detectado, o Cliente é redirecionado de forma imediata e transparente para a segurança;

Etapa 2
Automação de resposta

Varia desde notificar o cliente, intensificar a autenticação, encerrar a sessão (auto-logoff) ou bloquear a conta;

Etapa 3
FI Notification

Alerta as equipes de fraude do FI para tomar as providências necessárias.

O Digital Trust Active Defense detecta e responde a uma variedade de ameaças, incluindo:

Malware Blocker

Oferece uma capacidade de resposta altamente flexível para acompanhar as ameaças de malware mais recentes (com base no navegador).

- Valida o modelo de objeto de documento (DOM) do navegador e bloqueia códigos suspeitos de malware/injeção da Web.
- Identifica de forma inteligente códigos ruins para minimizar falsos positivos.
- Detecta e interrompe ataques de sobreposição de página do navegador projetados para redirecionar usuários para destinos fraudulentos/maliciosos.
- Responde automaticamente com sobreposições defensivas personalizáveis e notifica o FI para mitigar o ataque, configurando a autenticação avançada automatizada, o encerramento da sessão (logoff automático) ou o bloqueio da conta.

Bloqueador mRAT

Proteção RAT baseada em SDK que detecta e responde a um ataque de acesso remoto.

- Resposta automática com sobreposições defensivas personalizáveis para bloquear a visão do invasor sobre o aplicativo da vítima.
- Oferece proteção transparente sem interferir na interação do banco móvel do cliente.

Bloqueador de Phishing

Detecta quando um cliente clica em um link de phishing que o redireciona para um site clonado criado para roubar suas credenciais.

- Quando um redirecionamento de phishing é detectado, a navegação do cliente para o site fraudulento é automaticamente redirecionada de volta para uma página personalizável e legítima, mantendo-os protegidos do ataque de phishing.

Logoff automático

Uma das opções de resposta projetada para proteger os clientes de terem suas contas comprometidas.

- O logoff automático do navegador limpa os cookies bancários e encerra a sessão atual, exigindo que os clientes façam login novamente para estabelecer uma nova sessão limpa.
- Aplicativo móvel – o desligamento/logoff automático do aplicativo encerra a sessão do aplicativo móvel.

Digital Trust Pre-Emptive Defense

Fornece uma capacidade abrangente de prevenção de fraudes para descobrir agentes mal-intencionados, contas mulas e redes e impedi-los de cometer ataques fraudulentos a partir do ponto de descoberta.

3. Operações de Confiança Digital

A Digital Trust passa por várias etapas para detectar fraudes:

Biometria comportamental e o BionicID™
Usa todo o contexto para verificar identidades.

Detecção de agente inválido de sessão única
Identifica agentes nocivos conhecidos.

Detecção amigável de aquisição de conta
Trata anomalias detectadas quando amigos ou familiares estão ajudando proprietários de contas como de baixo risco e evita atrito devido a falsos positivos.

Banco de dados de impressões digitais do dispositivo
Facilita a detecção de controle de conta usando credenciais roubadas e agentes mal-intencionados usando seus dispositivos para abrir novas contas ou assumir contas existentes.

Detecção de malware
Pode proteger os usuários de forma silenciosa e transparente contra malware conhecido e de dia zero.

Detecção biométrica comportamental de maus atores™
Reconhece maus atores sofisticados, mesmo quando eles usam técnicas avançadas.

Detecção de emulador
Identifica a falsificação de dispositivos por bots e humanos.

Avaliação de rede
Detecta anomalias que indicam atividades suspeitas.

Detecção de bots
Identifica bots com base em falsificação de dispositivos, impressão digital de dispositivos, velocidade e outras anomalias do BionicID™.

3.1. Biometria comportamental e o BionicID™

A abordagem KYU exclusiva da Digital Trust responde à pergunta “você é realmente você?” usando um BionicID™. BionicID™ é uma impressão digital ou DNA digital que é exclusivo para cada usuário e é criado por meio da coleta e análise de milhares de informações não PII parâmetros relacionados ao contexto do usuário - o que eles usam para acessar um site ou aplicativo móvel protegido e como acessam esse aplicativo.

Muitas soluções de prevenção de fraudes “avançadas” usam biometria comportamental para identificar usuários com base em como eles digitam, movem o mouse, seguram um dispositivo móvel etc. Essas soluções normalmente comparam o usuário com um banco de dados básico de atores mal-intencionados, essencialmente fazendo a pergunta: “você parece um cara mau?” Embora esta seja uma abordagem eficaz em muitos casos, ela não fornece cobertura completa.

BionicID™ é uma impressão digital ou DNA digital que é criado por meio da coleta e análise de milhares de informações não PII parâmetros relacionados ao contexto do usuário.

Algumas soluções de detecção de fraude “avançadas” combinam biometria comportamental com impressão digital de dispositivos. Essas soluções geralmente geram falsos positivos estranhos resultantes da análise de dados de dispositivos de dispositivos compartilhados que são usados para acessar contas pertencentes ao mesmo FI. Nesse caso, um ou outro usuário pode não parecer exatamente um agente mal-intencionado, mas os indicadores comuns de impressão digital do dispositivo podem ser mal interpretados ou atribuídos de forma cruzada a um ou mais usuários, gerando falsos positivos.

O “você parece um cara mau?” O método de determinar usuários legítimos versus atores mal-intencionados também é extremamente limitante em cenários em que pessoas de dentro – pessoas que verificaram identidades e não fazem parte do universo maior de cibercriminosos – tentam acesso não autorizado a contas bancárias.

Os BionicIDs™ são baseados no contexto completo do usuário e construídos para reconhecer cada usuário. Eles se estabelecem rapidamente e podem começar a responder à pergunta “você é realmente você?” com precisão, em apenas duas a quatro interações.

BionicIDs™

responde à pergunta “você é realmente você?” em apenas duas a quatro interações.

Os BionicIDs™ são baseados no contexto completo do usuário e construídos para reconhecer cada usuário.

3.2. Detecção de ator ruim de sessão única

O sistema começa a capturar dados biométricos, comportamentais, de dispositivos e de rede para estabelecer “você é realmente você?” e crie a linha de base BionicID™ inicial assim que encontrar um novo usuário. A análise inicial compara o BionicID™ do novo usuário com os BionicIDs™ de criminosos conhecidos e verifica um banco de dados de dispositivos e redes vinculados a atividades fraudulentas conhecidas. Os dados do BionicID™ de criminosos ajudam a identificar os criminosos que trabalham dentro de um sistema bancário on-line e que podem estar tentando criar uma nova conta de mula.

A Digital Trust também verifica outros identificadores suspeitos, como os aplicativos descobertos em uso pelo novo usuário que são usados apenas por criminosos, ou endereços de e-mail ou números de celular vinculados a atividades fraudulentas para descobrir outros criminosos.

3.3. Detecção amigável de aquisição de conta

Existem muitas situações em que vemos um amigo ou familiar ajudando um cliente com sua conta bancária online. Na maioria dos casos, isso não é fraude. Vimos claramente esse pico de caso de uso nos primeiros meses da pandemia, quando o uso de serviços bancários online aumentou. Numa época em que o banco presencial não era possível, os clientes novos ou pouco frequentes do banco on-line costumavam ser ajudados por amigos ou familiares de confiança.

O BionicID™ reconhece quando alguém que não seja o usuário real está acessando uma conta e usa todo o contexto para determinar se o risco de fraude é baixo. Em vez de gerar falsos positivos ou bloquear o acesso e perturbar o cliente, o sistema permite que atividades de baixo risco prossigam sem interrupções. As soluções que dependem exclusivamente da comparação dos comportamentos do usuário com os de pessoas mal-intencionadas não funcionam tão bem em circunstâncias semelhantes. Essas soluções não emitem um alerta sobre possível fraude ou são muito agressivas e geram um falso positivo.

3.4. Detecção biométrica comportamental de maus atores™

Atores mal-intencionados que fazem pouco para esconder suas identidades, usam bots de preenchimento de credenciais de força bruta ou têm centenas de contas e dispositivos comprometidos conectados a seus computadores não são difíceis de detectar. Por outro lado, os maus atores que são melhores em seu ofício, assim como os criminosos no mundo físico, são mais difíceis de detectar e parar.

Agentes mal-intencionados sofisticados que são mais cuidadosos, usam hardware e redes limpas junto com humanos nunca vistos como proxies. Esses maus atores não serão detectados por soluções que se concentrem na pergunta "você parece um mau ator?" abordagem que simplesmente compara indicadores biométricos, de dispositivos e de rede com aqueles em seu banco de dados de agentes mal-intencionados.

Por outro lado, com a capacidade de criar o BionicID™ e atingir 99% de precisão rapidamente, a capacidade de verificar continuamente "você é realmente você?", reconhecer anomalias e realizar análises refinadas de atividades suspeitas, o Feedzai está em um posição muito melhor para detectar criminosos sofisticados e suas tentativas de manipulação e representação mais avançadas.

A capacidade de verificar continuamente "você é realmente você?", reconhecer anomalias e realizar análises refinadas de atividades suspeitas.

3.5. Detecção de malware

O malware bancário projetado para roubar credenciais ou controlar sessões bancárias é um crime de oportunidade com pagamentos substanciais e muito pouco risco. O código de malware é constantemente modificado, criptografado, redirecionado e combinado com outras técnicas para executar campanhas de fraude complexas. Mesmo os esquemas de autenticação de dois fatores (2FA) estão sendo contornados com malware da geração atual. Com redes criminosas bem financiadas e organizadas constantemente inovando, perdas financeiras significativas ocorrem entre o momento em que uma nova variante de malware é lançada e o momento em que pode ser identificada e interrompida por provedores de soluções antivírus.

O Digital Trust Malware Anomaly Detection & Classification Engine pode identificar malware previamente descoberto e classificado por meio do uso de listas continuamente atualizadas do setor de dados de ameaças de lista negra e branca. A lista branca é projetada para identificar o código suspeito como “seguro”, não representando nenhuma ameaça para os clientes, e as assinaturas de código da lista negra são usadas para identificar malware previamente identificado como “inseguro”. Em ambos os casos, a identificação é altamente precisa, resultando em nenhum falso positivo ou falso negativo.

O Digital Trust Malware Anomaly Detection & Classification Engine também é capaz de identificar malwares de dia zero mais perigosos – códigos maliciosos e padrões de malware que ainda não foram identificados – por meio de um conceito chamado lista cinza. Esse processo encaminha as anomalias de código recém-descobertas para o Mecanismo de classificação de malware da Digital Trust, onde são analisadas usando algoritmos de aprendizado profundo sob a supervisão de um especialista. Esse processo resulta na classificação das amostras como sem risco ou com risco confirmado.

Uma vez classificado como arriscado, na próxima vez que esse malware de dia zero for detectado, os recursos de defesa ativa do Digital Trust protegerão o usuário de forma transparente e proativa, desativando o ataque. Além disso, o sistema responderá de acordo com regras pré-configuradas com ações que vão desde autenticação por etapas, encerramento da sessão e bloqueio da conta até notificação ao usuário e geração de um alerta.

3.6. Banco de dados de impressões digitais do dispositivo

A impressão digital do dispositivo é uma maneira de combinar certos atributos de um dispositivo – como seu sistema operacional, o tipo e a versão do navegador da Web usado, a configuração de idioma do navegador e o endereço IP do dispositivo, etc. – para identificá-lo como único.

O BionicID™ inclui a impressão digital exclusiva do dispositivo do usuário e o Feedzai usa esses dados para determinar se a impressão digital do dispositivo de um usuário é consistente ou mudou por algum motivo desconhecido, exigindo um exame mais granular.

Por exemplo, é fácil detectar esses tipos de tentativas de controle de conta se credenciais roubadas forem usadas para acessar uma conta de um navegador ou aplicativo móvel com uma impressão digital do dispositivo diferente da do usuário legítimo.

Da mesma forma, os BionicID™s dos malfeitores também incluem suas impressões digitais exclusivas do dispositivo. Quando esses malfeitores usam seus dispositivos para tentar abrir uma nova conta ou assumir uma conta existente, é fácil para a Feedzai descobrir e impedir essas tentativas.

3.7. Detecção de emulador

Um emulador é um simulador de dispositivo móvel virtual. Essencialmente, é um software capaz de executar um ou vários ambientes móveis em um PC ou computador Linux. Os emuladores são flexíveis, fáceis de configurar e podem ser executados em ambientes virtuais – todos os motivos que os tornam atraentes para os cibercriminosos. Eles ajudam os malfeitores a evitar sistemas de detecção emulando ou falsificando os sensores do dispositivo e contornando a verificação anterior de impressões digitais do dispositivo.

O Digital Trust Anomaly Detection & Classification Engine detecta anomalias de dispositivo e rede que são indicadores claros de falsificação de dispositivo baseada em emulador, como ataques de bot de preenchimento de credenciais de força bruta ou ataques iniciados manualmente.

O Feedzai também detecta atividades suspeitas de dispositivos analisando os perfis BionicID™. qualquer tentativa para duplicar BionicIDs™ por proxies automatizados ou humanos (que são virtualmente impossíveis) é rapidamente detectado, analisado e avaliado como de alto risco para que a equipe de fraude possa investigar e tomar as medidas apropriadas.

3.8. Avaliação de rede

Os dados de rede coletados incluem todos os elementos de infraestrutura usados para acessar o banco online. O BionicID™ inclui os dados de rede do usuário e o Feedzai usa esses dados para determinar se a infraestrutura de rede de um usuário é consistente ou mudou por algum motivo desconhecido e requer um exame mais profundo. Os dados de rede BionicID™ incluem:

- Dados de infraestrutura de rede
- Endereço IP e ISP
- Padrões de mobilidade do usuário
- Geolocalizações

Os dados da rede são enriquecidos com informações de ameaças da Feedzai e de terceiro

- Geolocalização perigosa
- Infraestruturas de rede conhecidas usadas para fraude
- Mascaramento de conexão
- Aplicativos móveis maliciosos

O Digital Trust Anomaly Detection & Classification Engine analisa dados de infraestrutura em cada interação. Ele pode identificar como, quando e onde cada usuário está acessando um serviço para descobrir anomalias relacionadas a sessões originadas em um local incomum, se o usuário é um viajante frequente ou com que rapidez um usuário se desloca de um local para outro – e se tal o movimento é mesmo possível

3.9. Detecção de bots

O Digital Trust detecta bots de várias maneiras:

- As técnicas de detecção mais simples incluem detecção de emulador e impressão digital do dispositivo.
- O próximo nível de detecção é baseado na análise da velocidade com que as credenciais são inseridas no formulário/página de login. Ataques de bot não sofisticados inserem informações significativamente mais rápido do que os humanos e são facilmente detectados.
- Ataques de bot mais avançados são baseados em tentativas baixas e lentas de imitar o comportamento humano, como movimentos não lineares do mouse e digitação, mas também não têm chance de sucesso devido a anomalias detectadas durante a análise do BionicID™.

Assim que um ataque de bot é detectado, a equipe de fraude é imediatamente notificada e pode tomar as medidas apropriadas.

4. Casos de uso

O Digital Trust é usado por IFs em vários casos de uso:

Pontuação contínua de risco

SCA e PSD2 completamente silenciosos e totalmente transparentes.

Prevenção de aquisição de conta (ATO).

4.1. Pontuação de risco contínua e em tempo real

A abordagem KYU da Digital Trust analisa o risco de cada interação do usuário, examinando continuamente os BionicIDs™ do usuário em busca de anomalias, pontuando o risco com base em modelos por usuário, modelos baseados na população e modelos de maus atores, além de garantir que os dispositivos do usuário não sejam infectados por malware e que as sessões do usuário não foram invadidas.

Essa verificação contínua do usuário e análise de risco em tempo real permitem que os BANCOS cumpram uma série de regulamentações, incluindo autenticação forte do cliente (SCA), PSD2, prevenção de fraude CNP, verificação 3D-Secure e conformidade AML, melhorando a eficiência da abertura de novas contas e Sistemas de monitoramento de transações.

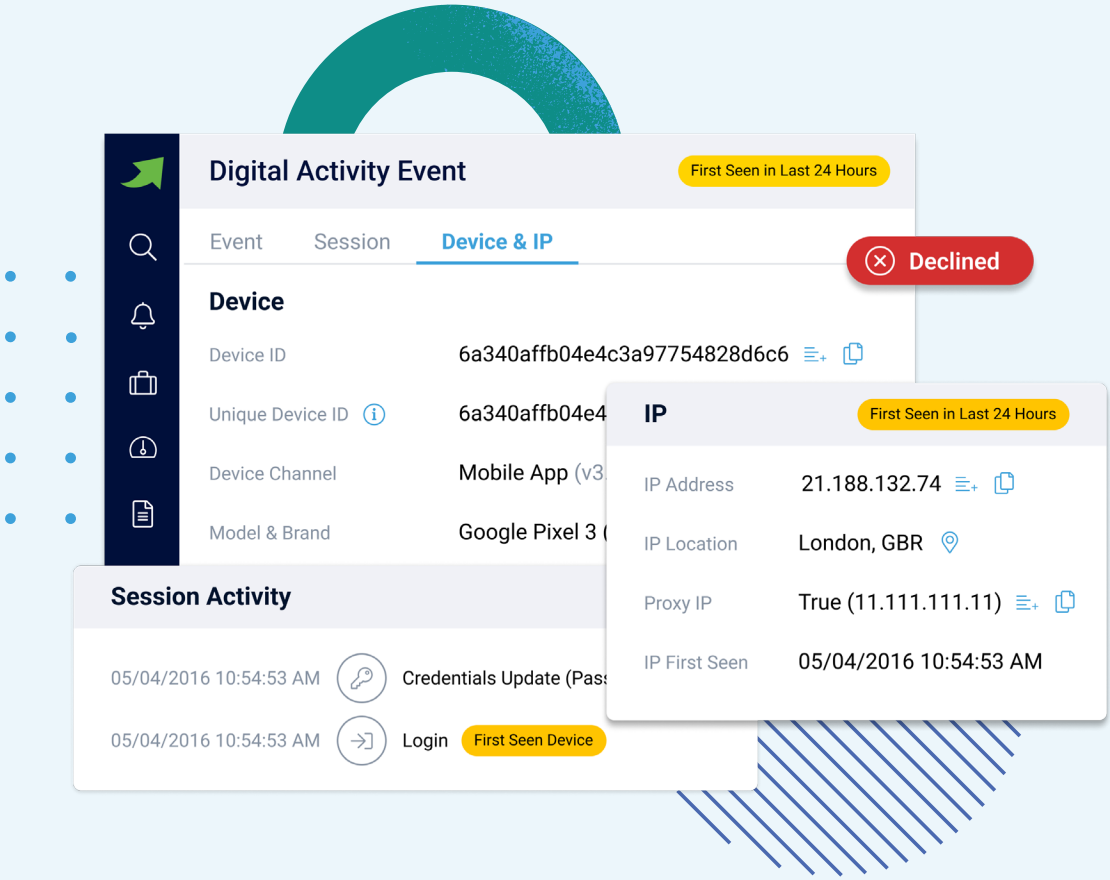
Caso essa análise revele anomalias do BionicID™, a Digital Trust imediatamente toma ações pré-determinadas de acompanhamento. Por exemplo, se o malware comprometeu o dispositivo de um usuário, o aplicativo móvel ou a página da Web pode fornecer a primeira linha de defesa e impedir o ataque.

A verificação dos usuários em cada interação reduz os falsos positivos e o atrito do usuário, protegendo instantaneamente contra problemas como sessões invadidas e minimizando a necessidade de autenticação avançada. A verificação contínua de usuários e dispositivos do Feedzai é completamente silenciosa e totalmente transparente.

4.2. Prevenção de controle de conta (ATO)

O Digital Trust determina instantaneamente se uma conta foi invadida respondendo a uma pergunta simples - “você é realmente você?” Sabemos quem é um usuário porque começamos a fazer a impressão digital dele no momento em que ele faz login em um site, capturando instantaneamente dados biométricos básicos, comportamento, dispositivo e rede. O Feedzai então compara silenciosa e continuamente o ator que controla a sessão com o perfil básico do usuário para garantir que um usuário legítimo ainda esteja no comando.

Em contraste, outras soluções perguntam: “você é um mau ator?” Responder a essa pergunta exige vasculhar bancos de dados contendo milhões de pessoas mal-intencionadas em busca de uma correspondência. Esse processo de identificação pode levar várias sessões, deixando os novos usuários em uma área cinzenta onde não são classificados como bons ou ruins. São os malfeitores não identificados nesta área cinzenta os responsáveis pela maior parte das fraudes e custos relacionados.



5. Integração rápida e fácil

5.1. Visão geral da implantação

O Digital Trust foi projetado para implantação de SaaS rápida e escalável. Aqui estão alguns pontos-chave para manter em mente:

Integração do cliente

- O Digital Trust não tem agente nem atrito. Não requer a instalação de agentes locais ou software nos dispositivos dos clientes do banco. Os clientes simplesmente acessam o banco com seu navegador habitual ou aplicativo móvel do banco. O Digital Trust é altamente compatível com navegadores da Web, sistemas operacionais e plataformas de hardware disponíveis comercialmente. O suporte móvel está disponível para dispositivos com sistema operacional iOS e Android.
- A coleta de dados no cliente é fácil e integrada e requer apenas a inclusão do código JavaScript no portal da web do FI e a integração de um SDK móvel leve no aplicativo móvel do FI.

Implantação em Nuvem

- O Digital Trust opera na nuvem e não é necessária nenhuma instalação ou atualização de qualquer hardware ou software no datacenter do FI.
- O Digital Trust é complementar e apenas enriquece outras plataformas de segurança proprietárias ou de terceiros ou hubs de fraude que o FI já possa ter.
- Se a IF ou banco decidir atualizar ou adicionar novos recursos, nenhuma alteração em sua infraestrutura é necessária e nenhuma modificação no código da web ou no aplicativo móvel é necessária.
- A integração requer uma ligação segura (VPN, HTTPS) entre o centro de dados do FI e a cloud da Feedzai.

Integração de API de back-end

- A Digital Trust usa uma API REST ou Web Sockets para enviar e receber eventos, alarmes e pontuações de risco. A integração requer uma ligação segura (VPN, HTTPS) entre o centro de dados do FI e a cloud da Feedzai.

feedzai

RiskOps

Transforme sua gestão de riscos.

A Inteligência artificial da Feedzai mantém-se à frente da fraude emergente e do crime financeiro e mitiga até os esquemas mais fraudulentos para que os bancos, emissores, adquirentes e comerciantes possam concentrar-se no crescimento. Entregamos resultados explicáveis e acionáveis com o comprovado valor de proteger milhões de clientes em todo o mundo.

Mas não somos apenas a melhor tecnologia. A parceria com a Feedzai significa as instituições recebem as melhores práticas que ajudam a criar experiências excepcionais para os clientes, ao mesmo tempo em que previnem e detectam crimes financeiros.

Abertura de conta | Prevenção à Lavagem de Dinheiro | Fraude Transacional

Agende uma demonstração

feedzai.com/pt-br **info@feedzai.com** **sales@feedzai.com**