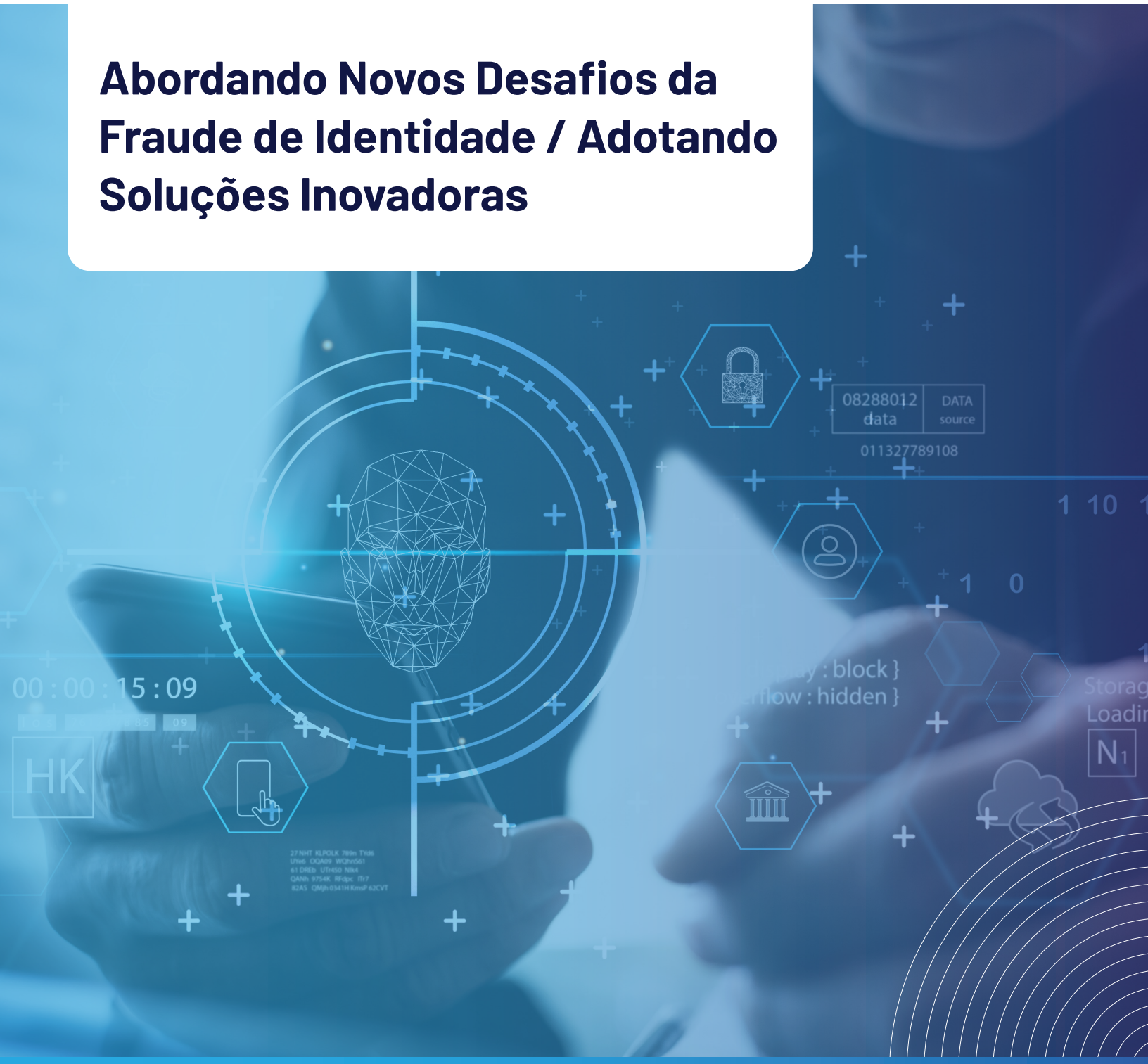
White Paper

Abordando Novos Desafios da Fraude de Identidade / Adotando Soluções Inovadoras



AWARE

781.687.0300 | sales@aware.com | www.aware.com

A Aware é uma das principais fornecedoras globais de produtos e soluções de software para identificação e autenticação biométrica. Eles são usados em uma variedade de aplicações, incluindo serviços financeiros, segurança empresarial, controle de fronteiras e aplicação da lei. A Aware é uma empresa de capital aberto (NASDAQ: AWRE) com sede em Burlington, Massachusetts.

O Desafio de Combater a Fraude de Identidade

Na era da ascensão das transações digitais, a fraude de identidade tornou-se uma ameaça persistente e crescente com consequências significativas para indivíduos, empresas e governos em todo o mundo. A proliferação de Informações Pessoais Identificáveis (PII) por meio das redes sociais e fontes públicas, combinada com o anonimato das interações online, capacitou as fraudes. Ao longo dos anos, o cenário da fraude de identidade continuou a evoluir, exigindo estratégias avançadas para combater este problema que chega a causar prejuízos de milhões de dólares todo ano. Embora abordagens tradicionais ainda possam ser relevantes, novas tecnologias e táticas estão moldando o futuro da prevenção da fraude de identidade.

Usando a Biometria para Prevenir Fraudes e Proteger Identidades

O roubo de identidade continua a ser a principal causa de fraudes com motivação de ganho financeiro. Com a proliferação das operações digitais e a facilidade das transações online moveis, organizações criminosas sofisticadas exploram as vulnerabilidades de sistema. Vazamentos de dados em larga escala continuam causando incidentes frequentes de roubo de identidade, muitos dos quais permanecem não detectados. O aumento da fraude de identidade sintética, em que identidades fictícias são meticulosamente construídas, apresenta um desafio significativo e em rápido crescimento.

Biometria: Uma Ferramenta Crucial na Luta Contra a Fraude de Identidade

A adoção da prova de vida ("liveness check") nas práticas de segurança convencionais acelerou nos últimos anos. A tecnologia de reconhecimento facial incorporada em aplicativos para smartphones tornou-se padrão para acesso seguro. Além disso, as capacidades de autenticação da prova de vida em sistemas operacionais abriram caminho para acesso seguro a plataformas externas usando reconhecimento facial, de voz e de íris. A prova de vida possui atributos únicos que constituem uma barreira eficaz contra a fraude, oferecendo uma camada adicional de segurança além dos métodos de autenticação tradicionais.

Além da Autenticação: O Crescente Papel da Biometria na Segurança Digital

Embora a autenticação biométrica em aparelhos pessoais tenha ganhado impulso como uma medida centrada no usuário, é necessário um enfoque mais abrangente para combater a fraude de identidade globalmente. Reconhecendo as limitações de depender apenas da autenticação baseada em dispositivos, os serviços de verificação e prova de vida utilizando a biometria baseados em nuvem surgem como uma via promissora. Essa mudança visa enfrentar os diversos desafios da fraude de identidade em vários cenários, os quais incluem o setor financeiro, agências governamentais e estabelecimentos comerciais.

AWARE

Saiba por que a Biometria tem papel Importante na Segurança Digital:

FRAUDE DE IDENTIDADE SINTÉTICA:
A prevalência de identidades sintéticas exige estratégias além da autenticação simples. A verificação biométrica e a prova de vida são importantes etapas no processo de camadas de segurança para evitar fraudes.

VERIFICAÇÃO DE IDENTIDADE:
A verificação biométrica confirma a identidade da pessoa que está se autenticando, não a autenticidade dos dados de identidade em si. Essa lacuna deixa espaço para estabelecer contas usando informações fraudulentas.

PENETRAÇÃO DE APARELHOS MÓVEIS:
O uso de smartphones permanece em crescimento, e uma parte substancial da população os utiliza regularmente. Soluções universais são necessárias para combater a fraude de identidade em diferentes devices e em todas as faixas demográficas.

PADRONIZAÇÃO E SEGURANÇA:
A autenticação em smartphones é limitada pela implementação do dispositivo, seu sistema operacional e os provedores de aplicativos. A padronização de arquitetura e interfaces é o objetivo das organizações, mas a funcionalidade e o desempenho biométrico não podem ser configurados universalmente nesses aparelhos. Além disso, essas limitações podem levar a problemas de segurança em aplicativos específicos.

Fundamentalmente, depender de senhas mais fortes não é suficiente para garantir a segurança. Arquitetura de segurança sólida, múltiplas camadas de proteção e a verificação de identidade confiável são necessárias para vários tipos de contas, aplicativos e ambientes.

Serviços Biométricos: Um Caminho em Direção à Acessibilidade em Diversas Indústrias

A Biometria como Serviço, fornece uma solução abrangente para prevenir a fraude em diversos aparelhos, inclusive os aparelhos móveis. Ela democratiza sua utilização em diferentes indústrias, reduzindo custos, fornecendo despesas previsíveis e incentivando a concorrência entre os provedores. Esses serviços atendem a diversas necessidades, suportam diversas modalidades biométricas, podem se hospedar na nuvem ou não, e estão transformando a indústria de verificação de identidade.

Fortalecendo a Integridade dos Dados por Meio da Verificação de Identidade Biométrica

A verificação de identidade biométrica protege a integridade dos dados ao verificar os dados de identidade durante a inscrição usando dados biométricos e comparando-os com registros existentes. Isso detecta cadastros ou onboardings duplicados e impede que fraudadores estabeleçam identidades falsas, estabelecendo confiança na autenticidade dos dados biométricos registrados e tornando-o uma medida preventiva eficaz contra a fraude de identidade.

Autenticação Baseada em Dispositivo vs. Servidor

Quando se trata de autenticação, é importante decidir se armazenar e comparar dados biométricos no dispositivo do usuário ou em um servidor central. O FIDO, que é centrado no dispositivo, realiza comparações no próprio dispositivo, reduzindo o risco de violações em massa. No entanto, aparelhos roubados podem representar riscos de fraude. Por outro lado, o modelo centralizado no servidor envolve o armazenamento de dados em um servidor de controle, o que pode gerar preocupações de segurança caso os dados biométricos sejam comprometidos. No entanto, falsificar dados biométricos é uma tarefa complexa, e com novas tecnologias e medidas contra a falsificação, é difícil para os fraudadores explorar violações de segurança biométrica.

Intensificando a Segurança Digital Contra Ameaças de Fraude.

Um banco líder na América Latina implementou a biometria para aprimorar suas medidas de segurança contra fraudes de identidade e para garantir uma experiência de autenticação de clientes segura e sem fricção. Ao adotar a biometria facial, eles evitam o investimento inicial em equipamentos de cadastramento biométrico, eliminando os riscos potenciais e os custos associados à manutenção e obsolescência tecnológica. Essa mudança estratégica está alinhada com o compromisso de proteger a identidade e as transações dos clientes.

A solução de biometria da Aware enfatiza a importância da verificação do usuário para estabelecer a autenticação à suas contas e transações. Isso garante que os dados biométricos coletados sejam de alta qualidade e estejam vinculados de forma segura às informações de identidade confiáveis, minimizando qualquer ambiguidade ou potenciais erros. O sistema suporta uma variedade de modalidades biométricas, incluindo impressões digitais, reconhecimento facial, íris e reconhecimento de voz, oferecendo flexibilidade e opções abrangentes de segurança.

Como a solução Aware resolveu um ataque de injeção em um banco líder na América Latina:

AUTENTICAÇÃO E VERIFICAÇÃO DE IDENTIDADE:

Ao procurar abrir uma conta para ter acesso a serviços bancários, os clientes são direcionados ao autenticador. Durante esse processo, os clientes fornecem provas de identidade de acordo com os requisitos do banco. As etapas da solução realizam a verificação de identidade e coletam os dados biométricos necessários. Esses dados são verificados e vinculados às informações de identidade dos clientes.

PESQUISA E VERIFICAÇÃO NO BANCO DE DADOS:

Os dados biométricos coletados são armazenados com segurança no servidor do banco. Quando uma cliente inicia uma nova solicitação de conta ou uma transação que requer autenticação biométrica, o sistema busca no banco de dados as inscrições existentes. Se surgirem conflitos ou inconsistências, é acionada uma investigação adicional. No entanto, se as informações coincidirem sem conflitos, a inscrição é atualizada e atribuída.

AUTENTICAÇÃO DE CLIENTES:

Os clientes podem se autenticar facilmente usando seu aparelho móvel, enviando seus dados biométricos pessoais. Se as informações de identidade dos clientes coincidirem, elas são recuperadas do sistema, garantindo uma identificação precisa e confiável.

OPÇÕES DE SEGURANÇA PERSONALIZÁVEIS:

O aplicativo oferece uma variedade de opções de personalização para se adaptar a diferentes requisitos dos clientes, benchmarks de desempenho, preferências de privacidade e necessidades de segurança. Essas opções incluem a seleção de modalidades biométricas específicas, a escolha de modalidades únicas ou múltiplas, e a decisão de armazenar dados biométricos no banco de nuvem privada ou no servidor.

EXPERIÊNCIA PERFEITA DO USUÁRIO:

A espinha dorsal da solução é uma plataforma de gerenciamento que coordena a segurança e os fluxos de trabalho com uma experiência de cliente sem problemas.

O banco líder na América Latina fortaleceu sua infraestrutura de segurança contra fraudes, e acessos não autorizados ao integrar a solução Aware. Isso não apenas aumenta a confiança dos clientes por meio de uma verificação de identidade precisa, mas também fornece a flexibilidade para se adaptar às necessidades de segurança em constante mudança e aos avanços tecnológicos, garantindo uma experiência bancária resiliente e sem problemas para seus clientes, ao mesmo tempo que prioriza a inovação e a segurança.

Olhando para o Futuro: O Futuro da Biometria na Prevenção do Fraude de Identidade

Conforme navegamos pelo complexo cenário da fraude de identidade, fica claro que a biometria surgiu como uma arma fundamental na luta contra essa ameaça onipresente. Os avanços na prevenção da fraude representam passos cruciais em direção a um ecossistema digital mais seguro e resistente. No entanto, a jornada não termina aqui; em vez disso, continua a evoluir à medida que a tecnologia, as táticas de fraude e as expectativas dos clientes passam por transformações.

O caminho da biometria na prevenção da fraude de identidade está repleto de oportunidades e desafios. Conforme olhamos para o futuro, várias considerações-chave surgem:

INOVAÇÃO CONTÍNUA:

O campo da biometria está longe de ser estático. Inovações continuarão a redefinir o que é possível. Desde a fusão biométrica multimodal até a análise comportamental impulsionada por inteligência artificial, a próxima onda de tecnologias promete soluções ainda mais precisas, adaptáveis e amigáveis aos clientes.

PANORAMA DE AMEAÇAS EM EVOLUÇÃO:

Os fraudadores também se adaptarão. À medida que os sistemas biométricos se tornarem mais sofisticados, também aumentarão as tentativas de violá-los. Devemos antecipar a evolução dos vetores de ataque e manter-nos à frente, melhorando não apenas a força de nossas defesas, mas também a profundidade de nossa vigilância.

PRIVACIDADE E PREOCUPAÇÕES ÉTICAS:

Com a crescente dependência de dados biométricos, a privacidade e a ética permanecerão na vanguarda. Encontrar o equilíbrio entre segurança, a experiência do cliente e a privacidade de dados exigirá diálogos contínuos e considerações cuidadosas para garantir que as soluções biométricas continuem sendo eficazes e respeitosas à privacidade pessoal.

EXPERIÊNCIA DO CLIENTE E PADRONIZAÇÃO:

A adoção da biometria em diversas indústrias e plataformas exige maior satisfação na experiencia do usuário e práticas padronizadas. Esforços colaborativos serão fundamentais para estabelecer estruturas coesas que melhorem a segurança e reduzam a fricção dos clientes.

PRÓXIMA GERAÇÃO DE APARELHOS DE FÁCIL UTILIZAÇÃO PARA OS CLIENTES:

O sucesso dos sistemas biométricos depende da aceitação e da educação dos clientes. Capacitar os clientes a entender as nuances da tecnologia biométrica, seus benefícios e limitações potenciais fomentará uma base de clientes mais informada e cooperativa.

REGULAMENTAÇÃO E GOVERNANÇA:

Órgãos reguladores em todo o mundo estão lidando com as implicações da tecnologia biométrica. Conforme essas estruturas amadurecem, elas fornecerão diretrizes essenciais para que as organizações garantam o uso ético, a proteção de dados e o cumprimento das mudanças legais em constante evolução.

Finalmente, enquanto continuamos a enfrentar os desafios da fraude de identidade e a abraçar soluções inovadoras, o papel da biometria será fundamental. Ela tem o potencial de revolucionar a forma como autenticamos, verificamos e interagimos no mundo digital. Embora não possamos prever todos os caminhos e curvas, uma coisa está clara: o caminho a seguir envolve tecnologia segura, adaptabilidade e um compromisso firme com a segurança das identidades dos clientes, empresas e governos em todo o mundo.

AWARE

781.687.0300 | sales@aware.com | www.aware.com