Identidade – Idtechs

Sua opinião é muito importante!

Sua opinião é muito importante para o Distrito. Por isso, queremos saber quais foram as suas impressões, críticas e sugestões sobre este relatório. Além disso, gostaríamos de saber quais outros estudos você gostaria que o Distrito Dataminer realizasse.

Quer falar com a gente? É só encaminhar um e-mail para: inside@distrito.me

Sumário

Para navegar pelos capítulos deste estudo, **clique nos botões na margem superior**. A qualquer momento, **clique no logo do Distrito no canto inferior direito para voltar a esta página.**

Metodologia

As startups delineadas no report foram selecionadas a partir de um trabalho minucioso de pesquisa e consulta ao banco de dados de startups proprietário do Distrito. Também foram realizadas consultas a bancos abertos e informações públicas do governo.

As startups foram examinadas individualmente para verificar adequação ao tema do report e aos critérios de seleção estabelecidos. São eles:

- **Ter a inovação no centro do negócio, seja na base tecnológica, no modelo de negócios ou na proposta de valor;**
- **Estar em atividade no momento da realização do estudo, medida pelo status do site e atividade em redes sociais;**
- **Desempenhar atividade diretamente relacionada ao setor estudado;**
- **Ter nacionalidade brasileira e operar atualmente no Brasil.**

O trabalho de definição das categorias foi baseado em análise da literatura relevante e das classificações utilizadas amplamente no mercado, no Brasil e no mundo.

A definição da categoria a que pertence cada startup foi feita por nossa equipe, e, quando uma startup opera em mais de uma categoria, a situamos na que interpretamos como sua atividade principal ou de maior visibilidade.

Também temos uma preocupação em incluir somente aquilo que consideramos startups—e, por mais que nosso critério para defini-las seja bastante amplo, excluímos alguns tipos de negócio que, embora muitas vezes se autodenominam startups, acabam fugindo do conceito. Isso inclui empresas que têm como característica principal serem:

- **Software Houses (desenvolvimento de software sob demanda);**
- **Consultorias;**
- **Agências de marketing, publicidade e design.**

Enfatizamos aqui que os números expostos podem sofrer alterações conforme a evolução da acurácia das informações e maior capacidade de interação com as próprias startups ao longo do tempo.

Entrevistados

Marcelo Bezerra
Executivo Sênior
Cisco

Tiago Alves
CEO
SimpleID

Lincoln Ando
Founder & CEO
IDwall

Cassio Sampaio
Vice Presidente de produto
Auth0

Rafael Medeiros
Líder em IAM
Open Consult

Introdução

Introdução

No Inside Cybertechs #5, procuramos destacar as startups que estão revolucionando com tecnologias em Identity and Access Management, fator primordial dentro de cibersegurança dentro das empresas.

Gestão de identidade e controle de acessos, principalmente aqueles que levam à sistemas, informações, aplicações e recursos de mais interesse dentro da organização precisam estar no centro das políticas de cybersecurity, pois são essenciais no controle de ataques cibernéticos. Além disso, com a quantidade de informações vazadas por criminosos diariamente, que foram obtidas por senhas fracas e acessos pouco seguros, o tema precisa estar no centro das discussões.

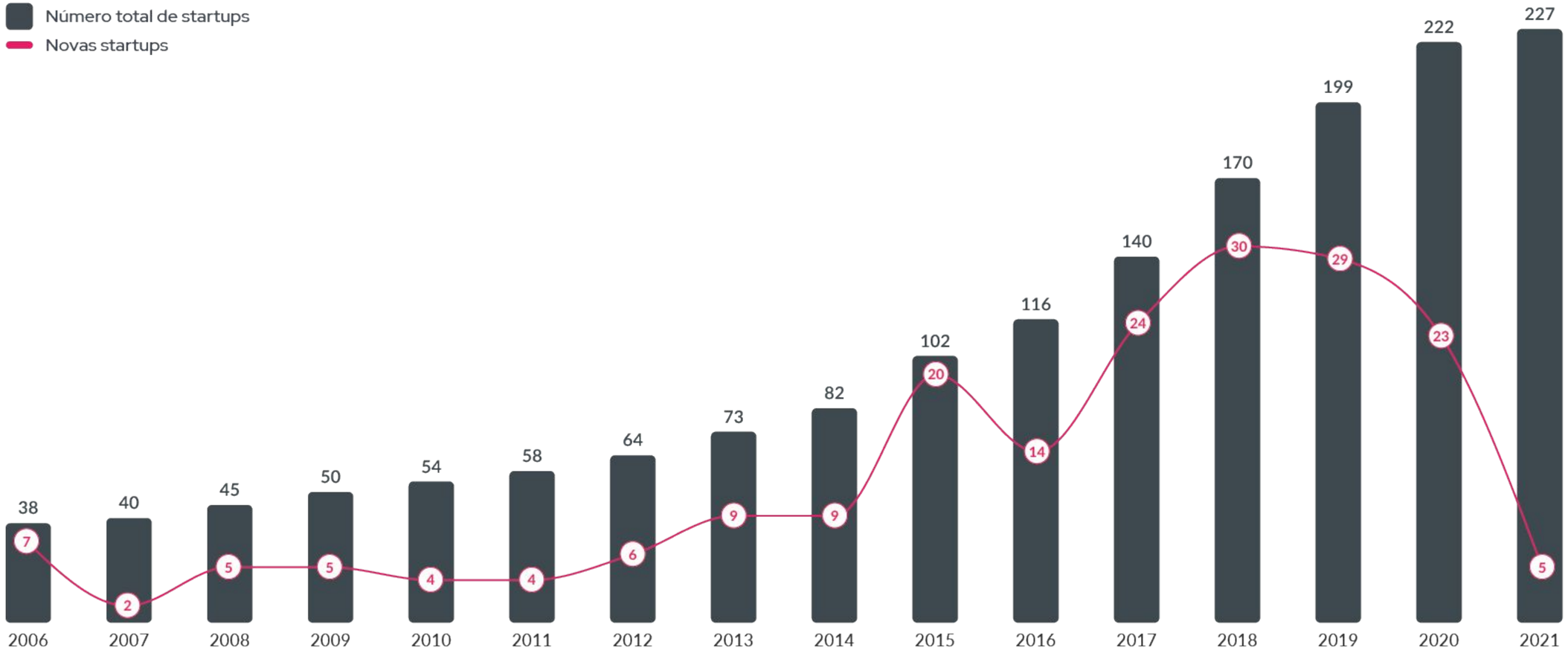
No Inside Cybertechs #3 foi destacado principalmente a importância de cuidar de informações sensíveis nas organizações e quais soluções de data protection estão revolucionando o mercado. Como complemento, as IDtechs são a primeira forma de impedir o acesso à esses dados.

Além de estatísticas nacionais e internacionais, no final do relatório, destacamos as principais tendências e tecnologias que estão se destacando no segmento, para que cada vez mais agentes do mercado se inspirem em criar e investir em novas soluções de IAM.

Agradecemos o apoio e o patrocínio da Cisco na confecção do report, que pretende alimentar cada vez mais conteúdos sobre cibersegurança, tema que se torna cada vez mais relevante dentro das corporações.

Boa leitura!

Evolução Cybertechs



Ecossistemas Cybertechs

Highlights

227
Startups

US$ 399M
Investimento recebido desde 2013

14
Categorias

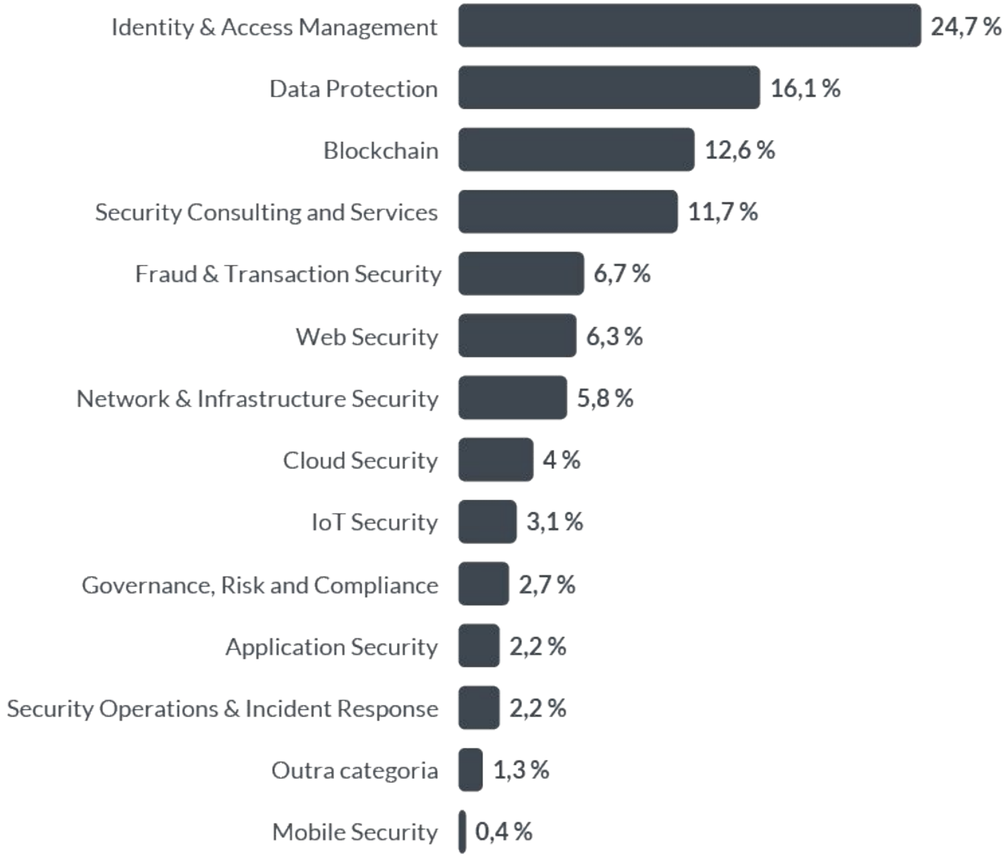
US$ 291M
Investimento recebido nos últimos 2 anos

7.200
Funcionários empregados

13
M&A's desde 2012

42
Startups com investimento recebido

Divisão Cybertechs por categoria



RADAR: CYBERTECHS

DISTRITO

Data protection

36ZERO · a2f · ADDERE SOLUTIONS · beAnalytic · CLAVIS · DADOS LEGAIS · dogma · ethquo · GLOBAL DATA BANK · guardSI · Intelivix · IT2SGROUP · leadcomm · LOGS360 · MODULO · NETTIME · sentnella · PHISHX · Privacy tools · PRIVALLY · riskex · SAFE WAY · senhasegura · SENSR. · Simply. · ST3TAILOR · FlashSafe

Cloud Security

ADTsys · BrasilCloud · DDMX · nuvic · RedeHost · CleanCloud

Mobile Security

BluePex

Security Consulting and Services

SOTO · CECyber · Collision · CROMISOFT · Deep.bbl · DESEC · ESTUARIO · HACK3R_RANGERS · IBLISS · iCybersec · INFOSAFE · INtroduce · SOLVIMM · nova8 · OPTRA SECURITY · REDBELT · RUSTCON · STRONG SECURITY · TEMPEST · Unbroken Cyber Security

Fraud & Transaction Security

B2e Group · bigdatacorp. · BrScan · CQuantt · EXATO DIGITAL BETA · ZAIG · infodatos · konduto · legiti · MOST · Neoway · VIVALISTO · NeuroBanco · NEXTCODE · TRANSFERO SWISS AG

Network, Infrastructure Security

CONNECT · ISM · lumiun CLOUD MANAGED NETWORK · munio SECURITY · oktopus · ProFUSION embedded systems · StartLink · TI Safe · Virti · WEDOIT Working Together · Ztec

Security Operations & Incident Response

AXUR · gocache next-gen CDN

RADAR: CYBERTECHS

DISTRITO

Identity & Access Management

acert · AIKNOW · akiyama · Assine Online · autentique · AutoSeg · BeCloud · BRy Tecnologia · CH tecnologia · Formalizar e-signature · FULLFace · griaule big data biometrics · GrupoCloud · GRYFO · HDOBOX · contract · ID ESSENTIALS · idwall · MEERKAT · NATOSAFE · nexti · nTokens · DI TI · payface · qriar · QualiSign · PONTO · unike · UNISEC · VSOFT · welcome · COMBATE A FRAUDE · contraktor · CRED DEFENSE · D4S · FIVE VALIDATION · mavie · INOVACODE · JURIDOC · Let's Work · .ai · SHIELDER · SimpleID · SVATECH · T-SHIELD · UNICO

IoT Security

GAVB · LATOS · Ochain · TrackerThings · POLSEC · PREVISIOWN · ROBBIOT

Governance, Risk and Compliance

GAT InfoSec · NeuralMind · certo · REFINARIA DE DADOS

Application Security

Berghem · CONVISO · BugHunt

Blockchain

2LEDGER · 4D4 · amachains · bitshopp · BLOCKc · BlockNobre · BLOCO1 · bom valor · COSMOS · CRIPTONOMIA · EOSRIO · Go Blockchain · GoBlock · growthTech · InspireIP · ORIGINALMY · QUAN · rhizom · safe TRACE · health · GoLedger · HubChain

Web Security

apura · AuditSafe · CromiWAF · XLabs · SITE BLINDADO · Gatefy · UPX TECHNOLOGIES · XLabs

IAM – Identity and Access Management

Contexto e Panorama Nacional

Identidade no Centro: Uma política essencial em cibersegurança

Jay Gazlay, especialista em segurança da informação no departamento de segurança do governo dos Estados Unidos, diz: “Identidade é tudo agora. Podemos falar em defesas da rede, da importância de firewalls e segmentação da network, mas na realidade, identidade se tornou o ponto principal, e nós precisamos começar a repensar nossas estruturas com isso em mente”.

Gerir acessos a informações de bancos de dados com informações sensíveis, seja com senhas fortes recomendadas pelos sites ou com tecnologias que permitem entrar nas aplicações de biometria é fundamental para uma organização na prevenção de ataques cibernéticos e vazamentos de dados. De acordo com uma pesquisa realizada pelo Data Breach Incident Report, o número de brechas encontradas por criminosos cibernéticos relacionados a acessos/senhas fracas ficou entre 63% a 81%.

Uma política focada em identidade também inclui como prioridades data security, application security e network security, vistos como essenciais para uma boa política de segurança. Entretanto, uma política de identidade no centro significa englobar humanos e máquinas em cinco pilares principais:

Autenticação, autorização, acesso aos dados, auditoria e contabilidade

Essa abordagem foca em principalmente em centralizar a administração de funções, políticas, controles de acessos privilegiados em áreas distintas nas empresas.

Pensar em políticas relacionadas à Identity Centric Security é deixar de pensar cibersegurança reativamente, buscando solucionar problemas quando eles já são uma realidade. É necessário transformar o mindset das empresas para pensar em cibersegurança como uma prevenção, pois em uma realidade de aumento de serviços em nuvem, dispositivos conectados e de tecnologias de IA, **pensar em segurança de informação de forma remediadora não é o suficiente.**

Uma variedade de estudos relacionados ao aumento da preocupação com gestão de identidades foram listados pela ID Security Aliance, uma comunidade de colaboração dentro do mercado de IAM. Alguns destaques são:

- Cerca de 80% dos ataques cibernéticos em 2018 envolveram acessos privilegiados
- 65% das companhias tem mais de 1000 contas associadas que nunca foram usadas para nenhum login
- 70% dos ataques envolvem se mover lateralmente dentro da rede, e precisa de acessos diferentes para tal
- Na média, empresas compartilham informações sensíveis com aproximadamente 583 agentes terceiros.

IDtechs: o ecossistema de inovação em IAM

IDtechs são startups que visam garantir a identidade digital da população, com o intuito de facilitar as relações do dia a dia, garantir transparência e devolver o controle dos dados aos usuários detentores da sua própria identidade. Dentro de cibersegurança, a verificação de identidade é essencial na proteção de dados das empresas e na luta contra os ataques cibernéticos, que muitas vezes se aproveitam de senhas fracas ou acessos fáceis para implantar ameaças maliciosas nos sistemas das organizações.

As startups no setor utilizam diferentes tecnologias de Inteligência Artificial, biometria, Big Data e Machine Learning para tornar o processo de validação e identificação de identidade rápido e seguro. Entre os produtos oferecidos pelas IDtechs estão reconhecimento facial, admissão digital, assinaturas eletrônicas e outras processos semelhantes que facilitam as mais diversas experiências dentro das organizações.

Essas empresas estão cada vez mais se consolidando no Brasil, acompanhando um movimento de preocupação com políticas de cibersegurança em meio à crescente dos ataques cibernéticos, como exposto no Inside Cybertechs #4. Ademais, essas soluções estão adaptando as empresas às políticas de conformidade previstas na LGPD, que impulsiona cada vez mais investimentos em segurança digital no país (Inside Cybertechs #3).

As soluções das IDtechs estão sendo utilizadas de diversas formas, e em um mundo cada vez mais digital, verificar identidades de maneira remota é essencial para tornar as relações virtuais entre pessoas cada vez mais seguras.

Nesse contexto, o Brasil está cada vez mais atualizado no assunto, principalmente porque a pandemia trouxe novas necessidades dentro das organizações para tornar o ambiente virtual mais transparente. Em 13 de novembro de 2020, no decreto de Nº10.543, foi regulamentado que o uso de assinaturas eletrônicas possam ter a validade de um documento com assinatura física, movimento que acelerou a consolidação de mercado de grandes IDtechs que já estavam fortificadas no mercado.

Nos próximos anos, espera-que o ecossistema de startups que trabalham com Identity & Access Management esteja cada vez mais sólido e desenvolvido no Brasil.

Identity & Access Management dentro das empresas

Marcelo Bezerra
Executivo Sênior
Cisco

Para uma política completa de cibersegurança dentro das empresas, quão importante são as políticas de controle de identidade (Identity & Access Management) e de acessos privilegiados?

Tais políticas são essenciais para qualquer empresa, de todos os setores e tamanhos, já que tratam do acesso a dados confidenciais e/ou privativos da empresa e de clientes, sobretudo após a LGPD, assim como do acesso aos sistemas e aplicações críticas. Uma política de segurança sem esses dois itens é uma política incompleta. Ambas estão presentes nos padrões de boas práticas de segurança há mais de vinte anos, e já constava na BS7799, que mais tarde se converteu na ISO/IEC 17799 e posteriormente na ISO/IEC 27000.

O número de ataques cibernéticos já vinha em uma crescente nos últimos anos, mas se destacou na pandemia, principalmente com a ascensão e consolidação do home office. Como as empresas podem melhorar suas políticas de acesso a informações privilegiadas no trabalho remoto?

Os problemas de controle de identidade e acesso não vieram devido ao home office, e sim porque tanto políticas como controles de segurança não estavam bem implementados. O uso do home office acabou por mostrar a fraqueza dessa implementação, mas a pergunta é como as empresas podem melhorar de modo geral suas políticas de acesso. Dentre as várias medidas que podem ser adotadas, gostaria de ressaltar a implementação dos conceitos de Zero Trust.

O Zero Trust é o passo além do 2FA/MFA (segundo fator de autenticação / múltiplo fator de autenticação) que por sua vez é a evolução da autenticação simplificada por uma senha simples. Além de fortalecer a autenticação via MFA, o Zero Trust implementa a verificação contínua, ou permanente, de acesso. Nesse modelo o usuário deixa de ser apenas validado no momento da autenticação para ser validado a cada acesso. Entre os critérios de validação se incluem o perfil do computador usado e até seu comportamento.

A implementação do Zero Trust traz à tona a questão da autenticação centralizada, e hoje o ideal é a adoção do Single Sign-on, tecnologia bastante madura hoje. A novidade está em ampliá-la para incluir as aplicações corporativas baseadas em nuvem. A validação contínua resulta também na implementação de uma gestão mais ativa, com mais capacidade de detectar acessos suspeitos antes →

→ que os dados sejam efetivamente vazados, ou um sistema crítico acessado.

Por fim, outra tecnologia que está se tornando pilar de uma boa estratégia de segurança é a da microsegmentação, ou segmentação de rede baseada em software. Nela, usuários recebem seus acessos dinamicamente a partir de um perfil pré-estabelecido, implementado pelos próprios equipamentos de rede. Dessa forma, um usuário pode ter direitos de acesso diferentes quando acessando desde sua casa e de dentro do escritório. Tal tecnologia será ainda mais vital com o advento do trabalho híbrido.

Em média, empresas compartilham informações sensíveis com aproximadamente 583 agentes terceiros (2018 Third-Party Data Risk Study.) Como a Cisco, sendo uma das maiores empresas de cibersegurança do mundo, é capaz de gerir e proteger todos os acessos a dados privilegiados?

A Cisco é uma das maiores fornecedoras, e defensoras, da estratégia de Zero Trust e microsegmentação como técnicas de proteção dos acessos. Na verdade, a quantidade de compartilhamentos não importa muito. Basta um acesso desprotegido para que uma informação confidencial seja vazada. Foi dessa forma que empresas foram invadidas através de links com fornecedores, alguns deles sem nenhum acesso formal a dados sensíveis, como provedores de ar-condicionado.

Quais as principais tecnologias dentro de Identity & Access Management você gostaria de destacar?

Conforme comentado nas respostas anteriores, gostaria de destacar duas:

- Single Sign-On integrado com sistema Zero Trust e Federação quando necessário. A tecnologia de Federação faz com que a identidade dos usuários seja compartilhada entre diferentes sistemas de gestão de identidade e acesso. Todo o sistema deve estar expandido também para a nuvem.

- Microsegmentação no qual o acesso do usuário em rede, uma vez autenticado pelo método acima, é dinamicamente estabelecido de acordo com seu perfil e o perfil do computador em uso.

Identity & Access Management dentro das empresas

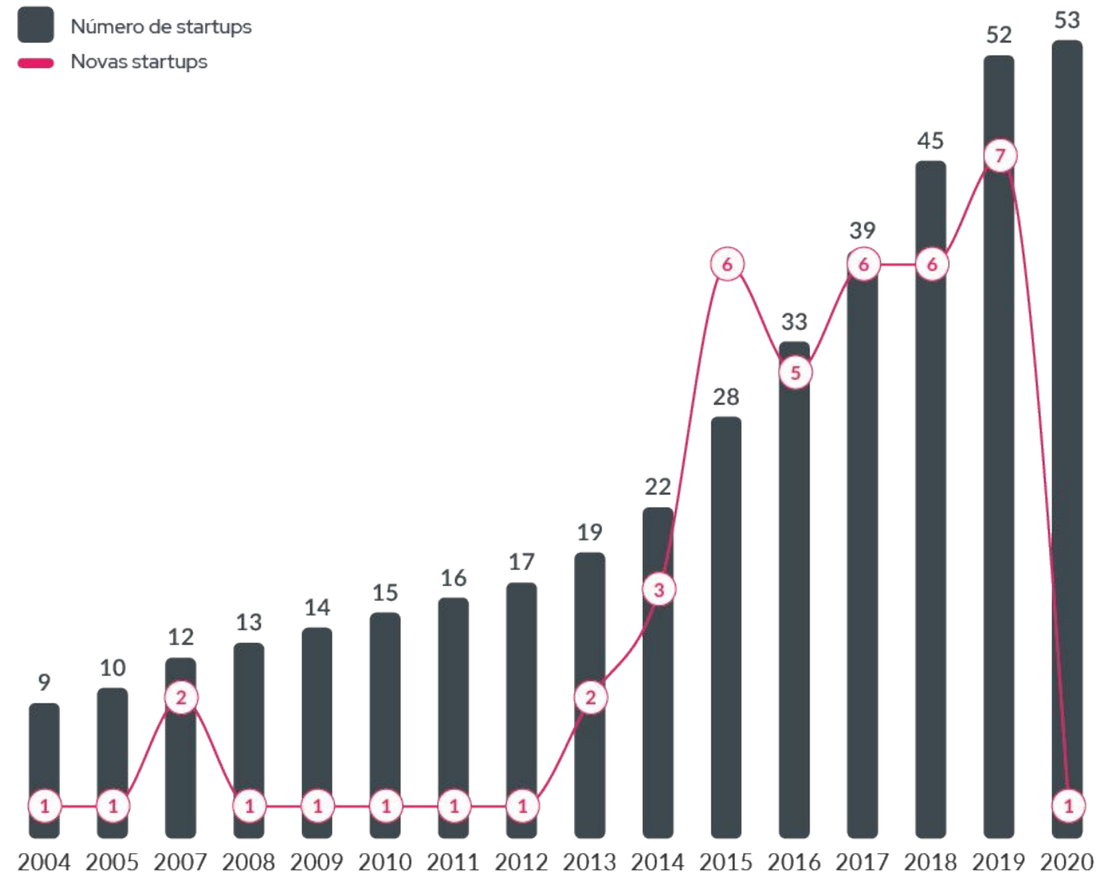
Marcelo Bezerra
Executivo Sênior
Cisco

Idtechs brasileiras se destacam dentro de cibersegurança

Representando atualmente 23% da base de Cibersegurança do Distrito, as IDtechs são a categoria de maior expressividade em números absolutos nas categorias avaliadas. É necessário destacar, entretanto, que a Unico (antiga acesso digital) e a IDwall são outliers que puxam muitos dos dados da categoria em volume aportado e quantidade de funcionários.

De todo modo, dentro de cibersegurança, o tema ganha cada vez mais relevância no país, e é esperado que sejam criadas cada vez mais soluções focadas em IAM para atender uma demanda de mercado muito presente.

2,2 mil
Funcionários

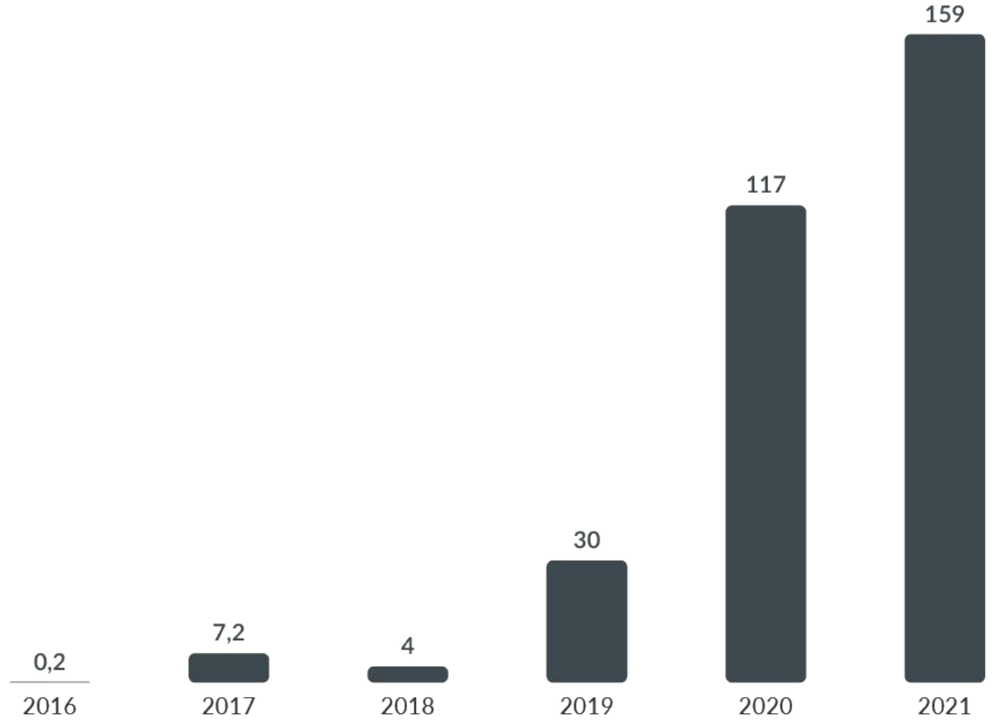


Investimentos em IDtechs

O investimento em IDtechs segue sendo liderado por grandes startups do segmento, contudo é interessante destacar que o grande volume aportado em 2021 mostra que empresas desenvolvidas no segmento estão sendo muito visadas pelo mercado, justamente pela necessidade das empresas de terem soluções de IAM.

24
Deals no total

Investimento em startups de IAM no Brasil (US$ Milhões)



SimpleID
IDENTIDADE CONFIRMADA!

Nome: SimpleID

Público: B2B

Ano de Fundação: 2015

Em todo o mundo, serviços de saúde têm buscado otimizar seus processos de cadastramento e controle acesso de pacientes. Em especial, operadoras de saúde dependem muito da eficiência e segurança dos mecanismos de controle de acesso, para garantir o bom atendimento aos seus beneficiários e eliminar fraudes.

A SimpleID cria ferramentas que confirmem a identidade das pessoas no setor de saúde. Da Validação de dados demográficos, passando pela identificação facial e análises de imagens odontológicas, a Idtech auxilia as empresas a atingirem melhores resultados.

A empresa destaca três produtos:

SimpleID API: Confirmação de identidade, agilização de processos com a API multibiométrica em nuvem que já identificou milhões de pessoas e evitou milhares de fraudes.

SimpleID Image Audit: Eliminação de fraudes de reutilização de imagens durante a solicitação de aprovação de procedimentos em operadoras de planos odontológicos

SimpleID Valida: Tornar o processo de onboarding de clientes dentro da empresa mais ágil e seguro, validando dados e prevenindo fraudes de identidade duplicada.

A empresa já conta com grandes clientes como a Unimed Maceió e o grupo Mil, já recebeu investimento e está mirando expansão em diversas regiões do país.

SimpleID: Controle de fraudes com biometria

Tiago Alves
CEO
SimpleID

A simpleID se diz apaixonada por criar ferramentas que confirmem a identidade das pessoas e que previnem fraudes de diferentes tipos, sempre com o uso do que existe de mais moderno em termos tecnológicos. Qual a importância da solução de vocês no mercado?

Nossa soluções ajudam empresas a reduzirem fraudes e a agilizarem processos. Com a digitalização cada vez maior de procedimentos que até pouco tempo atrás eram executados ou de forma presencial ou através da troca de materiais físicos (papéis assinados, documentos, etc), a confirmação da identidade se tornou essencial tanto para as empresas, que conseguem eliminar tentativas de fraudes de identidade, como para as pessoas, que passam a ter uma segurança que um indivíduo mal intencionado não irá se passar por ela para contratar um serviço, por exemplo.

Como exemplo, podemos citar a abertura de conta em banco que, até pouco tempo, exigia que a pessoa se deslocasse até uma agência, assinasse papéis e apresentasse inúmeros documentos. Hoje, em poucos minutos você abre uma conta no banco através do seu celular, apenas tirando uma foto do seu documento e uma selfie. E para que esse processo seja seguro é necessário que o banco realize ao menos 3 etapas relacionadas à confirmação da identidade: a primeira delas é garantir que a pessoa da selfie é a mesma pessoa que está fotografada no documento. A segunda é garantir que realmente existe uma pessoa real na frente da câmera no momento da selfie e não uma foto impressa, uma foto no celular ou até mesmo uma máscara de silicone 3D. E, por último, é garantir que essa pessoa não existe em sua base de clientes cadastrada com outro CPF, que é um dos possíveis tipos de fraudes de identidade no Brasil. Essas 3 etapas podem ser realizadas utilizando as tecnologias SimpleID.

Um outro exemplo que podemos citar é o caso de operadoras de saúde que, em sua maioria, vem migrando de um modelo em papel, no qual o paciente assinava uma guia toda vez que ia ao médico ou fazia um exame, para um modelo digital no qual o beneficiário do plano apenas apresenta sua carteirinha e a autorização é realizada de forma 100% digital. Com essa digitalização do processo, surgiu a preocupação de prevenção a fraudes, principalmente de empréstimo de benefício (o famoso empréstimo de carteirinha). Esse tipo de fraude, quando uma pessoa não segurada recebe atendimento, é responsável por uma porcentagem considerável das despesas das operadoras, o que acaba impactando nos preços dos planos. A SimpleID foi uma das primeiras empresas a levar o reconhecimento facial para esse mercado, que antes utilizava a impressão digital, que é uma tecnologia mais cara e com uma pior experiência do usuário. Com a nossa tecnologia, uma simples foto no momento da consulta elimina as fraudes, reduz os custos das operadoras →

→ de saúde e traz mais segurança para o médico e paciente.

Como vocês enxergam o aumento de soluções relacionadas a Identitity & Access Management no mercado? Esse movimento de fato indica que as empresas estão cada vez mais preocupadas com esses processos?

Qualquer empresa que possua processos no qual exista o risco de uma pessoa se passar por outra, deverá utilizar soluções relacionadas a Identity & Access Management. Aquelas empresas que não investirem na confirmação da identidade e na proteção do acesso aos seus serviços inevitavelmente irão ficar para trás. As empresas estão começando a mostrar uma maior preocupação com esses processos, mas ainda de forma embrionária, e acredito que veremos um crescimento acentuado nos próximos anos. Hoje o seu uso se limita a grandes empresas, processos específicos e utilização limitada da tecnologia.

O que nós vemos no mercado hoje é que muitas empresas ainda não acreditam que fraudes de identidade existem e, quando enxergam, não conseguem dimensionar o impacto financeiro em sua operação. E essa educação do mercado faz parte do nosso trabalho de mostrar o impacto das fraudes nos negócios e, entendermos junto com nossos clientes, como nossas soluções podem agregar valor e trazer retorno financeiro para as empresas.

Quais são as principais tecnologias dentro da confirmação de identidade que seriam interessantes destacar e que interessam à SimpleID?

Quando pensamos em confirmação de identidade na SimpleID, estamos sem dúvidas pensando em biometria. A SimpleID respira biometria desde o dia que nasceu. Entre as mais conhecidas, destacamos a facial, a de voz e a por impressão digital, que vem tendo a sua atuação cada vez mais limitada apenas ao setor público, especificamente na área da segurança pública. As tecnologias de biometria evoluíram muito nos últimos anos, com destaque para o reconhecimento facial que atingiu níveis de precisão que permitem sua utilização em diferentes situações e ambientes desafiadores, graças à evolução das técnicas de Machine Learning. Hoje, essa biometria é o foco principal da SimpleID mas, já temos planos para, no curto prazo, agregarmos a biometria por voz em nossa plataforma.

Um ponto que é importante destacar é que não está disponível na maioria das soluções que vemos no mercado é o anti-spoofing, também conhecido como liveness ou prova de vida. Apenas realizar o reconhecimento facial ou por voz não é suficiente. É fundamental garantir que a foto foi capturada ao vivo, com uma pessoa na frente da câmera e não se trata de uma tentativa de ataque como a apresentação de uma foto impressa, a foto do WhatsApp na tela do celular ou uma máscara 3D. Implantar reconhecimento facial sem esse tipo de validação reduz consideravelmente a eficácia do processo, pois os fraudadores tentam esse tipo de abordagem o tempo todo. Por isso, é fundamental que a solução de Identity & Access Management possua tecnologia de anti-spoofing e que essa tecnologia tenha o menor impacto possível na experiência do usuário.

Quais são os próximos passos da empresa para se consolidar cada vez mais no mercado?

O primeiro passo — e que não abrimos mão — é continuar caminhando próximo a nossos clientes, →

SimpleID: Controle de fraudes com biometria

Tiago Alves
CEO
SimpleID

→ entendendo suas necessidades e buscando uma relação de parceria.

Outro ponto fundamental é a busca por parcerias estratégicas com empresas que forneçam soluções para os mercados que desejamos atingir. Esse é o nosso grande foco no momento.

E no que diz respeito a produtos, vamos continuar a evolução constante da tecnologia, que é fundamental para estarmos sempre, senão à frente, mas com capacidade de responder rapidamente às demandas do mercado e, principalmente, aos novos tipos de fraudes de identidade que surgirem.

Nessa linha, atuamos em duas frentes. A primeira é a total adequação às leis, especificamente à LGPD, que desde o seu surgimento, impacta a forma como desenvolvemos o nosso produto. Hoje, a solução da SimpleID é totalmente aderente à LGPD, o que dá mais segurança aos nossos clientes.

Além disso, no curto prazo vamos adicionar um novo tipo de biometria em nossa plataforma, que é a biometria por voz. Com esse novo fator de autenticação esperamos confirmar a identidade em dois segmentos principais: call centers e chatbots.

SimpleID: Controle de fraudes com biometria

Tiago Alves
CEO
SimpleID

Nome: idwall

Público: B2B

Ano de Fundação: 2016

Funcionários: 290

Fundada em 2016 por Lincoln Ando e Raphael Melo, a idwall é uma regtech especializada em desenvolver soluções automatizadas de validação de identidade, facilitando o onboarding de usuários em organizações de diversos segmentos e auxiliando para que fiquem em conformidade com as legislações específicas de seus mercados.

A regtech foi criada com a missão de solucionar um grande desafio enfrentado pelas empresas brasileiras, vivenciado por Lincoln e Raphael em suas diversas experiências profissionais: a grande desconfiança existente no ambiente digital, causada por crimes como a fraude de identidade. No Brasil, essa infração é responsável pelo prejuízo de R$ 60 bilhões anualmente, colocando-o atrás apenas do México entre os países que mais sofrem com essa ocorrência.

Como consequência, a falta de confiança estagna novos negócios e impede consumidores de acessarem serviços essenciais remotamente, dificultando o dia a dia e impactando a economia de forma negativa.

Em 2016, a idwall passa pelo Angel Round e consegue levantar R$600 mil. Em 2017, em rodada capitaneada por investidoras como Monashees, Canary e 500 startups, arrecada R$ 2 milhões. O Series A vem em 2018, com uma rodada de R$ 9 milhões onde participaram empresas como Monashees, Canary, Fundação Estudar e Mercado Livre.

A idwall passa pelo Series B em 2019, em que levanta R$ 40 milhões e se torna a primeira empresa latino-americana investida pelo fundo de inteligência artificial da Qualcomm Ventures. A rodada também contou com os grupos ONEVC e Globo, além de Canary, Monashees e outros.

IDwall: Grandes IDtechs

Lincoln Ando
Founder & CEO
IDwall

A idwall é uma solução de onboarding digital com agilidade e segurança, que tem como missão construir relações de confiança através da tecnologia para que negócios possam ir cada vez mais longe. Qual a importância da solução de vocês no mercado?

A crescente digitalização do mercado fez todos os negócios olharem para dentro e ajustarem processos para conseguir atender ao cliente online. E a solução da idwall se tornou ainda mais relevante para empresas que querem construir relações comerciais com confiança. Validar a identidade de clientes e fornecedores de forma ágil e segura contribui para uma boa experiência do usuário, protege dados e processos da empresa e ainda permite ganhos de produtividade e escalabilidade do processo, de forma que os negócios possam se dedicar a outros pontos relevantes da operação.

Em um contexto em que as empresas estão cada vez mais se preocupando com a cibersegurança, a idwall e outras IDtechs estão se destacando no mercado. Como vocês avaliam a crescente procura por soluções relacionadas a verificação de identidade e como vocês estão se preparando para atender essa demanda?

O cenário certamente é muito positivo para as empresas do setor. Além do movimento de digitalização que ocorreu mundialmente, existem também questões do próprio cenário brasileiro, como o grande número de fraudes, desconfiança interpessoal, aumento no número de dados vazados, exigências legais e a complexidade documental do país. Com tudo isso, mais empresas passaram a adotar processos de validação de identidade e outros formatos de segurança digital, o que contribuiu para o crescimento do nosso mercado.

Vemos um cenário muito promissor e no qual podemos gerar bastante impacto ao ajudar as empresas a desburocratizar processos, realizar um cadastro seguro e com uma boa experiência para o usuário, além de auxiliar na inclusão de milhões de pessoas a serviços e oportunidades. Muitas empresas tiveram e ainda têm dificuldades na automação de processos de segurança, e estamos constantemente criando mais serviços e tecnologias que focam em melhorar essa automação, tornando o fluxo de cadastro, validação e aquisição de clientes, fornecedores e parceiros mais seguro e eficiente. Pensando nisso, ainda, recentemente lançamos o Professional Services, um serviço de consultoria da idwall em que nosso time de especialistas realiza um diagnóstico preciso e propõe medidas a serem tomadas para auxiliar as empresas a criarem um processo de acordo com suas estratégias e que atinja a excelência na avaliação de um usuário cada vez mais rigoroso e exigente. →

Quais os principais setores que a solução da idwall está presente? Existem algumas empresas que precisam mais da solução do que outras?

A idwall atende todo tipo de negócio que precisa validar ou obter informações sobre a identidade de usuários, empresas e fornecedores, mas os principais clientes que temos hoje são no mercado financeiro, varejo, marketplaces, transportes e logística. Nossas soluções podem ser utilizadas por empresas de diferentes segmentos que busquem garantir a segurança da informação e usuários, mas em geral os bancos e as empresas de transportes são os que mais fazem validações.

Quais as principais tecnologias presentes dentro das soluções idwall que vocês gostaria de destacar?

SDK: Com nosso SDK mobile, aprovar clientes sem comprometer a UX e a segurança se torna ainda mais simples para aplicativos. Nosso SDK conta com tecnologias de inteligência artificial e uma UX intuitiva que instrui o usuário a capturar corretamente a imagem. Após isso, fazemos a análise e o processamento da imagem recebida (documentos ou selfies).

OCR (optical character recognition) e validação de documentos: Utilizamos tecnologias como visão computacional, processamento de imagem e machine learning no nosso sistema de OCR , para extrair dados de fotos de documentos como RG, CPF ou CNH. Com isso, as empresas ganham mais agilidade em seus cadastros, já que não é necessário gastar tempo dos funcionários digitando os dados manualmente. O OCR também aumenta a eficiência do processo, já que erros de digitação são evitados.

Face Match e Liveness: A solução Face Match utiliza visão computacional, processamento de imagem e machine learning para realizar o reconhecimento facial e comparar se a foto capturada condiz com a foto de identificação no documento enviado. Para acrescentar ainda mais segurança a esse processo, acrescentamos a prova de vida ou Liveness durante a verificação, que pede que o usuário se posicione na câmera para verificar que está vivo. O SDK instrui o usuário a cumprir os parâmetros determinados, para garantir a qualidade da captura, e nossa tecnologia conta com algoritmos de visão computacional aplicados à imagens de rostos para fazer a prova de vida.

Background Check: Já nossa solução de Background Check utiliza os dados capturados do documento enviado pelos usuários para fazer buscas em diferentes bancos de dados. Assim, empresas podem verificar, por exemplo, se determinado CPF tem irregularidades na Justiça antes de permitir que o cadastro seja validado, ou garantir que um motorista tem permissão para dirigir motos ou caminhões, por exemplo. Além disso, nossa solução utiliza inteligência artificial para fazer a validação de dados desestruturados, mitigando riscos.

Qual é a visão de longo prazo da empresa? E quais os principais desafios que estão sendo enfrentados atualmente?

Estamos vivendo um grande momento de crescimento para empresas de tecnologia no Brasil, especialmente nos setores de finanças, logística e e-commerce, que geralmente têm um público muito grande e um tipo de gargalo específico. Isso gera uma forte competitividade no mercado, que faz com que o processo de cadastro se torne um ponto ainda mais importante de diferenciação e retenção de usuários. →

IDwall: Grandes IDtechs

Lincoln Ando
Founder & CEO
IDwall

Com o aumento nas mudanças regulatórias, é de extrema importância que as empresas acompanhem essas mudanças e possam adaptar rapidamente seus processos para atender às novas regras. É aí que surgem cada vez mais possibilidades de inovação para empresas como a idwall, que entende o contexto brasileiro e pode ajudar empresas estrangeiras, e até mesmo nacionais, a eleger as ferramentas necessárias para que as empresas cumpram seus objetivos e expandam suas operações com mais segurança e obedecendo às legislações e regulações de cada setor.

Recentemente passamos por uma rodada de Série C no valor de R$ 210 milhões. Com esse investimento queremos acelerar o crescimento da idwall investindo no lançamento de novos produtos, bem como na contratação e treinamento de mais profissionais. Há alguns meses tínhamos 150 funcionários, em novembro deste ano dobramos esse número e já estamos com 300. Nosso foco é continuar nos consolidando como a referência de mercado em soluções seguras de verificação de identidade para empresas e usuários, e por isso estamos investindo na expansão da equipe e dos serviços que oferecemos.

Além disso, com a rodada Série C, também pretendemos expandir nosso alcance B2C. Para o consumidor final, contamos com um aplicativo de identidade digital chamado MeuID, que permite ao usuário reunir e compartilhar todos os principais documentos em um só lugar de forma prática, acessível e segura.

IDwall: Grandes IDtechs

Lincoln Ando
Founder & CEO
IDwall

Nome: Unico

Público: B2B

Ano de Fundação: 2007

Funcionários: 501-1000

O grande propósito da Unico é facilitar a relação das empresas, ajudando as pessoas a provar com facilidade que elas são elas mesmas de fato e diminuir essa fricção entre empresas e pessoas.

Por ser focada em autenticação de identidade, a startup vem ganhando clientes em diversas áreas que permitem o login do usuário por meio de impressão digital ou reconhecimento facial, principalmente bancos, companhias aéreas e plataformas de ingresso online. Ao que tudo indica, a clientela da Unico deve se expandir ainda mais nos próximos anos, já que a previsão é que até 2023, todas as empresas com presença digital serão obrigadas a contratar serviços que ofertem maior segurança de acesso e login.

Como afirma Guilherme Cervieiri, VP Stategy & M&A na Unica na entrevista exclusiva no Inside VC de agosto: **"Atualmente, 5-10% das contratações de carteiras assinadas no Brasil passam por nós, pois permitimos que companhias contratem de uma forma confiável através de vias digitais. Nosso grande sonho é que a gente permita — até brincamos neste ponto — transformar você na moda! As calças e roupas não vão precisar ter mais bolsos. Tudo será realizado com a face, desde a abertura de contas digitais até o check-in em aviões."**

A Unico se tornou o primeiro **unicornio brasileiro** dentro da base de Cibersegurança no Distrito, em uma rodada liderada por Softbank e General Atlantic. Em processo de constante crescimento, a empresa pretende acelerar seu crescimento no Brasil e continuar auxiliando as empresas nas suas relações com pessoas e na redução de fraudes.

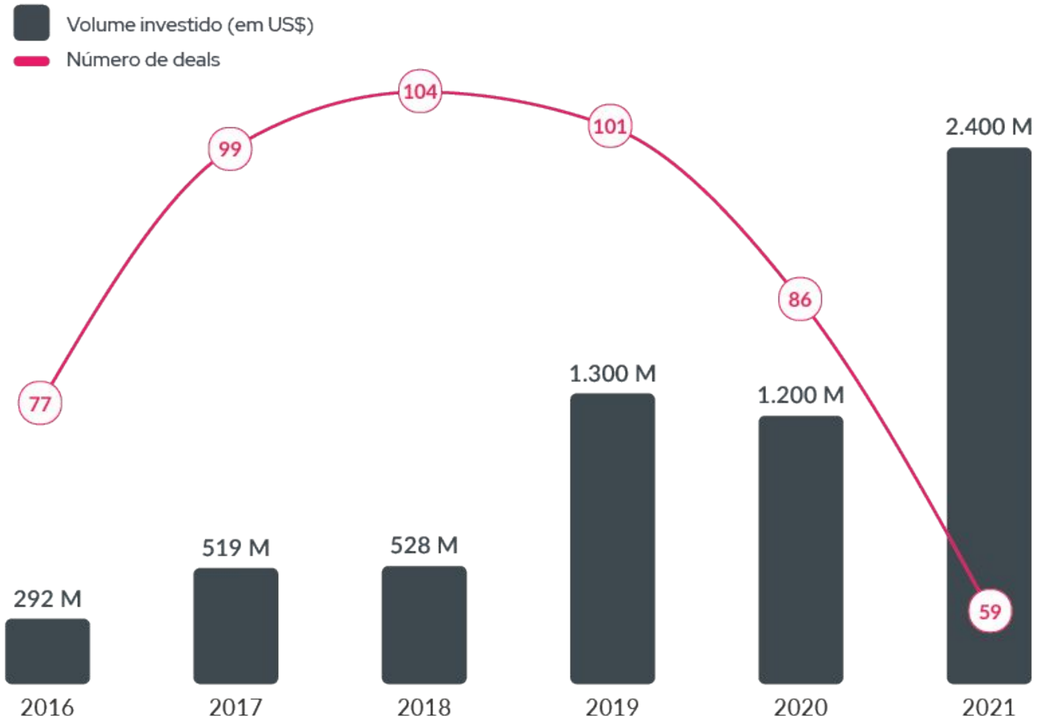
A entrevista com a Único completa você pode conferir clicando aqu e acessando a versão de agosto/2021 - Como os M&As estão mudando o mercado de tecnologia no Brasil

Investimentos em IAM

Panorama Internacional

Startups de IAM já receberam mais de US$ 9,4 bilhões em 765 rodadas de investimento

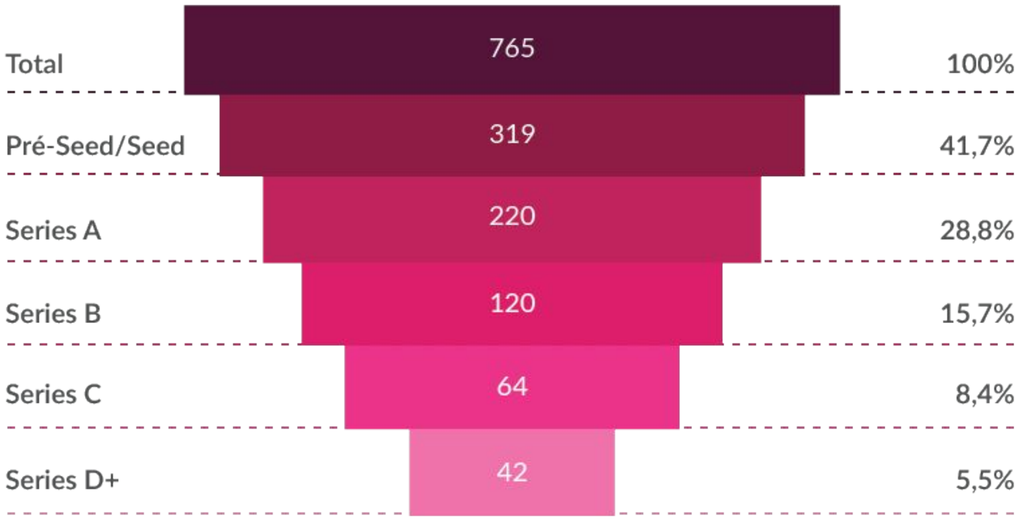
Investimento em startups de IAM



As startups de Identity Access Management tem chamado atenção dos investidores de Venture Capital, que tem aumentado suas apostas na categoria. Como vemos no gráfico ao lado, houve um grande aumento no volume de investimento entre os anos de 2018 e 2019. Em 2020 o valor sofreu uma pequena redução, muito provavelmente devido aos efeitos econômicos da pandemia do Covid-19.

Em 2021, mesmo antes do fim do ano, já foi dobrado o total investido em startups de IAM no ano passado, US$ 1,2 bilhões em 2020 e US$ 2,4 bilhões em 2021. Um dado interessante é a quantidade de rodadas de investimento que ocorreram entre os dois anos, 2021 teve 27 rodadas a menos e um montante duas vezes maior. Isso mostra o desenvolvimento das startups do setor, que estão captando valores maiores nas rodadas, tendo menos deals e volumes mais robustos para financiar suas operações.

Volume por estágio de aporte

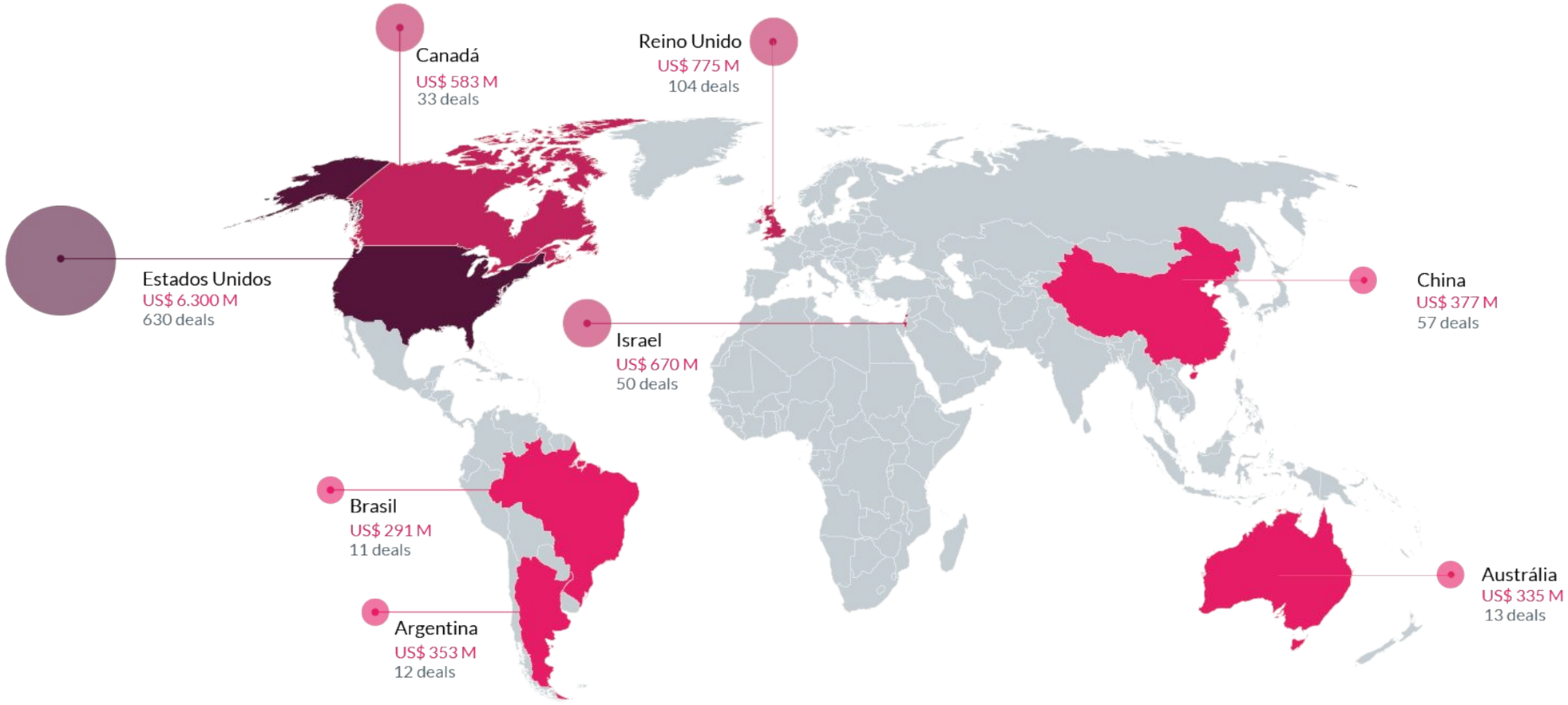


*N° Deals

A maioria dos investimentos em startups de IAM estão concentrados no Early Stage, 41,7% . Isso é um indicativo da pré-maturidade do setor, que ainda tem a grande maioria das startups em estágios de ideação e validação do modelo de negócio e produto.

Apesar de a maioria das startups estarem no Early Stage, já existem startups de Identity Access Management que atingiram o status de unicórnio, como é o caso da brasileira Unico, que captou US$ 121,3 milhões em rodada Série C e contou com grandes investidores: General Atlantic e Softbank.

Investimento por país em IAM



Principais investidores e deals

	INVESTIDOR	PAÍS	INVESTIMENTOS NA CATEGORIA
1	**Plug & Play Tech Center**	EUA	37
2	**Y Combinator**	EUA	12
3	**Techstars**	EUA	12
4	**500 startups**	EUA	11
5	**Startupbootcamp**	UK	11

Analisando o perfil dos cinco principais investidores de startups de IAM, vemos um padrão de serem aceleradoras ou incubadoras, reforçando a tese apresentada na página 29, de que a há pré-maturidade desta categoria dentro do ecossistema de inovação, uma vez que os grandes investidores buscam startups mais maduras. Já as aceleradoras e incubadoras procuram startups em estágio muito inicial, normalmente em idealização ou MVP, para investirem e acelerarem com programas de aceleração e desenvolvimento, ajudando a montar o business model e estruturar os primeiros passos da startup.

A forte presença de investidores de Early Stage indica uma tendência de crescimento para a categoria de IAM para os próximos anos, quandos as startups que atualmente estão em fase inicial poderão comprovar suas teses e avançaram para estágios de desenvolvimento mais avançados

A cibersegurança começa na sua caixa de login

Cassio Sampaio
Vice Presidente de Produto
Auth0

As empresas muitas vezes afirmam ter foco no cliente, se esforçando para oferecer as tecnologias que seus usuários exigem. No entanto, as descobertas de uma pesquisa recente da Auth0 global sugerem que as organizações em todo o mundo continuam errando o alvo quando se trata de fornecer aos usuários a experiência de login que desejam. O estudo da Auth0, conduzido pela YouGov, de fevereiro a agosto de 2021, pesquisou mais de 17.000 tomadores de decisão de marketing/TI e consumidores em 12 países, e descobriu que as expectativas dos consumidores para suas experiências de login não correspondem à realidade.

Na Argentina, Brasil e México, os destaques de aproximadamente 1.000 consumidores e 200 tomadores de decisão de TI/Marketing pesquisados são especialmente reveladores: 84% dos consumidores latino-americanos abandonaram totalmente uma tentativa de compra ou registro devido a uma experiência de login complicada - 87% no Brasil, em comparação com México (85%) e Argentina (80%). Outro achado interessante é que os consumidores latinos (61%) se disseram mais propensos a se inscrever em um aplicativo/serviço online se ele oferecesse logins sociais, em comparação com 42% na região da Ásia-Pacífico, 31% na Europa, África e Oriente Médio (31%), e EUA, com 38%. No entanto, apenas 41% dE mais: embora os tomadores de decisão de TI/Marketing da América Latina sejam os mais propensos a dizer que oferecem social logins, as empresas em toda a América Latina estão aquém das expectativas do consumidor para todas as tecnologias de login.as empresas latino-americanas oferecem essa alternativa.

Os números mostram que há uma lacuna clara entre as expectativas dos consumidores e das empresas. Na América Latina, as pessoas estão buscando tecnologias de login modernas, como SSO, logins sociais e biometria para maior comodidade, segurança e privacidade, mas a maioria das empresas argentinas, brasileiras e mexicanas ainda não atendem às expectativas dos consumidores locais. A primeira impressão do seu negócio começa no login, e se o seu processo for frustrante e não acompanhar as demandas dos consumidores, eles podem migrar para outros negócios.

De outro lado, a confiança nas senhas como meio principal de autenticação, combinada com a tendência dos usuários de reutilizar senhas em aplicativos, apresenta uma série de problemas de segurança, experiência do usuário e custos. De acordo com um Relatório de investigações de violação de dados de 2021 da Verizon, as senhas comprometidas são responsáveis por 84% das violações. A autenticação sem senha atenua esses desafios e oferece maior →

→ segurança e confiança para aplicativos, dispositivos e provedores de serviços; experiências de login mais rápidas e suaves para seus usuários finais; e economia de custos ao eliminar a necessidade de suporte ao gerenciamento de senhas.

No cenário atual, pós-pandemia, com mais pessoas trabalhando no modelo remoto, os cibercriminosos quadruplicaram a quantidade de ataques cibernéticos, e o impacto para as organizações e seus usuários de um único ataque bem-sucedido está crescendo a cada ano. Dados do FBI de 2020 mostram que em 2017, quase 197 milhões de registros foram expostos devido a violações de dados nos Estados Unidos. Em 2020, esse número cresceu para 37 bilhões, embora o número geral de violações de dados tenha diminuído. E a IBM relata que os custos dos ataques em países como os Estados Unidos estão crescendo: o custo médio de uma violação de dados passou de US$ 7,91 milhões para US$ 8,64 milhões entre 2018 e 2020.

Muitos dos métodos que os cibercriminosos usam para violar as organizações dependem de erro humano. Até mesmo os funcionários mais espertos podem se tornar sua maior fraqueza se clicarem em um link malicioso sem perceber. No entanto, outros ataques cibernéticos exploram lacunas em seus esforços de segurança de dados para obter acesso a dados confidenciais.

Mesmo com a orientação contínua sobre a criação adequada de senhas e avisos repetidos contra a reutilização de senhas, os consumidores anseiam por conveniência e continuam a usar o caminho mais fácil para acessar seus apps.

Os dados do cliente podem ser o maior ativo da sua empresa - a menos que caiam nas mãos erradas. Para que possamos avançar, temos que olhar para as ferramentas e estratégias de gerenciamento de identidade e acesso do cliente (CIAM, na sigla em inglês para Customer Identity Access Management) é a forma como as empresas fornecem aos usuários finais acesso às suas propriedades digitais, bem como controlam, coletam, analisam e armazenam com segurança os dados desses usuários.

Uma solução de CIAM robusta tem recursos de segurança para proteger contra fraudes, hacks e uso indevido de dados em várias frentes. Nos últimos anos, a caixa de login se tornou a linha de frente para afastar invasores. Os hackers usam ataques de autenticação quebrada para roubar ou adivinhar as credenciais do usuário e se passar por usuários legítimos na caixa de login.

Uma das formas mais prejudiciais de ataques de autenticação quebrada é o enchimento de credenciais, no qual os hackers usam senhas roubadas em uma violação para invadir outros sites. Esse método funciona devido à tendência das pessoas de reutilizar senhas. Atualmente, bilhões de senhas roubadas são transmitidas pela dark web. Só os ataques de enchimento de credenciais custam às empresas uma média de US$ 4 milhões por ano, de acordo com um estudo de 2019 do Ponemon Institute.

A maneira como conseguimos melhorar nossa força contra os ataques nos permitirá nos livrar de cargas pesadas que prejudicam nosso desempenho com os usuários. A pesquisa da Auth0 reflete exatamente isso: o mais desestimulante é o preenchimento de longos formulários de acesso ou cadastro, a criação de uma senha que atenda a determinados requisitos e o compartilhamento de informações privadas. São as principais questões que hoje desencorajam o uso de aplicativos e sites de todos os tipos. Isso leva ao fato de que a esmagadora maioria dos consumidores →

A cibersegurança começa na sua caixa de login

Cassio Sampaio
Vice Presidente de produto
Auth0

→ reutiliza senhas para mais de uma conta, uma das más práticas que levam a mais violações de identidade em todos os processos.

Em um panorama no qual cada vez mais aplicativos têm migrado para a nuvem e se expandido mundialmente, as organizações dependem de seus serviços de identidade para proteger e gerenciar o acesso para seus usuários, aplicativos e dados mais críticos. Podemos dizer que o futuro caminha para o login sem senha, especialmente por conta de duas forças principais - segurança e conveniência.

Auth0 se posiciona como uma plataforma de autenticação e autorização adaptativa. Qual a importância da solução para o mercado?

Auth0 Identity Platform, uma unidade de produto da Okta, tem uma abordagem moderna para identidade e permite que as organizações forneçam acesso seguro a qualquer aplicativo, para qualquer usuário. É uma plataforma altamente personalizável, simples e flexível conforme a necessidade das equipes de desenvolvimento, e protege bilhões de transações de login todos os meses.

A importância hoje é essencial devido à enorme transformação digital que está ocorrendo e, nesse sentido, a plataforma do Auth0 oferece conveniência, privacidade e segurança para que os clientes possam se concentrar na inovação e no core business.

Quais são os próximos passos da empresa para se consolidar ainda mais no mercado?

O ponto principal é que está claro que o papel da identidade no mundo evoluiu e temos que lidar com essa mudança. Juntos, Okta e Auth0 estão reimaginando a função da identidade na estratégia de tecnologia de cada organização. Nuvem, dispositivos móveis e BYOD (Traga seu próprio dispositivo) transformaram a dinâmica do mundo digital na última década. Ao mesmo tempo, a TI está trabalhando para acompanhar todas essas mudanças, e os desenvolvedores devem ser capazes de se concentrar na criação de mais aplicativos rapidamente e sem sacrificar a segurança e a experiência do usuário. A identidade é o perímetro e está no cerne de cada escolha e transformação de tecnologia. As experiências digitais estão conectando mais empresas, clientes e funcionários do que nunca. Entendemos essa necessidade de conexão.

A cibersegurança começa na sua caixa de login

Cassio Sampaio
Vice Presidente de produto
Auth0

Nome: Duo Security

Público: B2B/ B2G

Ano de Fundação: 2009

Funcionários: 251-500

Adquirida em 2018 pela Cisco, a Duo é uma startup sediada nos EUA focada em autenticação em dois fatores de diferentes formas. A tecnologia permite garantir o acesso privilegiado por meio dessa autenticação em aplicativos mobile, ligações, mensagens de texto, tokens, sendo os aplicativos o maior foco de demanda.

As soluções da Duo estão em diferentes áreas da cibersegurança, como cloud security, endpoint security e mobile security, mas o foco maior da companhia está na autenticação em dois fatores. As soluções são divididas em diferentes setores da indústria, destacando educacional, financeiro, saúde, legal, varejo e tecnologia. Além disso, a empresa também fornece soluções para governos.

A missão da empresa é fornecer acessos seguros ao redor do mundo, ganhar a confiança das empresas para embarcarem em uma jornada zero-trust com confiança em seus serviços diversos de autenticação. Além disso, a empresa já atua e produz conteúdo com as principais trends dentro de Identity & Access Management, como em sua produção do Ebook: Passowrdless: The Future of Authentication (Sem senha: o futuro da autenticação).

A empresa, em seu relatório “The 2021 Duo Trusted Access Report” destaca que em toda a sua base de clientes realiza cerca de 800 milhões de autenticações todos os meses, em mais de 36 milhões de dispositivos e já realizou mais de 400.000 autenticações únicas.

Atualmente, a empresa atende mais de 5.000 empresas ao redor do mundo, com clientes como Facebook, Paramount Pictures, Toyota, Yelp e Etsy.

okta

Local
São Francisco, USA

Ano de Fundação
2009

Público
B2B

Investimento Recebido
US$ 228,5 milhões

Investidores
Andreessen Horowitz, Sequoia Capital, Altimeter Capital, Janus Capital Group, Glynn Capital Management, Webb Investment Network, Khosla Ventures, Greylock, SV Angles

Sobre

A Okta é uma das empresas líderes em controle de acesso, oferecendo soluções de acesso segura para outras organizações, sendo uma IDaaS. Ela trabalha tanto com o soluções para o cliente final, quanto para o controle de acesso interno de seus contratantes.

Ela oferece desde soluções finais como sing-on únicos e autenticação multifator, até produtos como gateway de acesso, API de gestão de acesso e integrações B2B.

A startup possui mais de 7.000 integrações pré-construídas para aplicativos e provedores de infraestrutura e possui mais de 13 mil clientes. Entre eles destacam-se nomes como Siemens, Slack, Nasdaq e a Major League de Baseball dos Estados Unidos.

A Okta foi considerada como líder no Quadrante Mágico da Gartner, na categoria Gerenciamento de Acesso, tendo a maior pontuação entre todas as empresas no critério “Habilidade de execução”.

Entre 2009 e 2015 a empresa captou mais de 228 milhões de dólares em investimentos e em 2017 realizou seu IPO, na Nasdaq.

PingIdentity.

Local
Denver, EUA

Ano de Fundação
2002

Público
B2B

Investimento Recebido
US$ 128,3M

Investidores
General Catalyst, Threshold, Sapphire, Kohlberg Kravis Roberts, Triangle Peak Partners, Volition Capital, TenEleven Ventures, Appian Ventures, W Capital Partners, DFJ Element, Silicon Valley Bank, Avista Partners, Fidelity Ventures, I-Vent.

Sobre

A Ping Identity é uma empresa que oferece soluções de identificação inteligente, ajudando empresas a realizarem sua transformação digital através do acesso a aplicativos em nuvem, aplicações móveis, SaaS e aplicações locais.

Ela oferece meios de autenticação multifator, logon único, gerenciamento de acesso, segurança de API inteligente, recursos de governança e dados. Sua plataforma cloud registra, verifica, autentifica, autoriza e monitora os acessos do cliente final, ou do time interno de seus clientes.

Através de seus produtos, a empresa consegue entregar soluções para reforçar arquiteturas Zero Trust, gerar acessos passwordless, mitigar riscos de fraude e entregar eficiência em M&A’s.

60% dos membros da Fortune 100 são seus clientes, contando com 13 dos 15 maiores bancos dos EUA, sete das nove maiores companhias de saúde globais e cinco dos sete maiores varejistas norte americanos. A empresa realizou seu IPO na NYSE em 2019, e aparece no Quadrante Mágico da Gartner ao lado da Okta.

IDnow.

Local
Munique, Alemanha

Ano de Fundação
2014

Público
B2B

Investimento Recebido
US$ 40 milhões

Investidores
Corsair Capital, Plug and Play, Seventure Partners, 10x Group, Giesecke+Devrient, BayBG Venture Capital,

Sobre

A IDnow é uma startup de Verificação de Identidade as a Service, que oferece serviços para empresas que necessitam de alta segurança para seus clientes.

A startup usa IA para checar todos os pontos de segurança e consegue identificar identidades forjadas, reconhecendo mais de 7 bilhões de pessoas em 193 países ao redor do mundo, tudo isso em tempo real.

Entre sua gama de produtos estão os de auto identificação por IA, identificação por vídeo, por transferência bancária e por NFC, para casos como de cartão de crédito, uma vez que a startup possui muitos clientes do setor financeiro.

Sua plataforma abrange desde nichos tradicionais como o próprio setor financeiro, seguros, turismo e telecomunicações, até novos modelos digitais, tal como crypto, mobilidade, games e e-sports.

A IDnow possui mais de 350 clientes, entre eles Bank of Scotland, BNP Paribas, Commerzbank, além de startups como Fidor, N26, Smava e Wefox.

onelogin

Local
São Francisco, EUA

Ano de Fundação
2009

Público
B2B

Adquirida por
One Identity

Sobre

A OneLogin é uma startup focada em soluções de identificação e acesso para empresas de diversos mercados. Ela oferece serviços desde serviços mais simples como autenticação em uma etapa e multifator, até produtos mais robustos como, vigilância em tempo real através de IA e ML, verificação especificamente desenvolvida para tablets e celulares, e integrações com sistemas de terceiros.

A startup alega que, com o seu sistema, operações de on e offboard podem se tornar 9x mais rápidas, integrando dados de diversas fontes, além das suas proprietárias.

Hoje, a OneLogin possui mais de 5,5 mil clientes, entre eles estão nomes como Airbus, Evernote, BIC e AAA. Como destaque, a empresa se posiciona no Quadrante Mágico da Gartner como líder, na categoria gerenciamento de acesso, ao lado de Microsoft e Okta.

A startup foi adquirida recentemente, em outubro de 2021, pela One Identity. Antes da fusão ela já havia levantado mais de 175 milhões de dólares através de fundos de investimento.

Tendências

Reconhecimento facial cresce

O **mercado de reconhecimento facial tem a expectativa de chegar em 2022 a US$ 9,6 Bilhões**, o que registraria um **crescimento médio anual de 21,3% entre 2016-2022**. O mercado engloba tecnologias 2D, 3D e facial analytics, porém, as soluções 3D aparecem como maior destaque. Tecnologias de gestão de acessos e identidade, dentro de cibersegurança, correspondem a maior parte do mercado, tanto no âmbito público quanto no privado. Nos últimos anos, tecnologias de reconhecimento facial ganharam força no varejo, principalmente focado em marketing e publicidade.

A pandemia causada pela COVID-19 teve um impacto positivo no mercado, principalmente pelo aumento da preocupação das medidas sanitárias, que levou às empresas a buscarem soluções de gestão de identidade que não envolvesse contato. Ademais, com o aumento dos investimentos direcionados a cibersegurança, as soluções do segmento também se beneficiaram.

Atualmente as maiores dificuldades das empresas do setor são o alto custo de implementação dessas soluções e a falta de acuracidade em diversos casos distintos. Entretanto, com os avanços nas tecnologias e com o crescimento do mercado, essas dificuldades tendem a naturalmente serem perpassadas.

Destaques em IAM - Duo Security

A DUO Security realizou um estudo com seus clientes e constatou algumas destaques interessantes que podem signifcar futuras tendências no mercado de IAM, entre junho de 2020 e maio de 2021, para entender também os impactos da pandemia. Alguns destaques são:

- **Aumento de 5x nas opções de acesso sem senha;**
- **Aumento de 12% de acessos com biometria nos celulares registrados;**
- **Autenticação em 2 fatores ganhou mais destaque, com o produto DUO do segmento sendo mais procurado em 39% em comparação ao período analisado;**
- **Autenticação em aplicativos de nuvem aumentou de 13% para 15%.**

Podemos inferir uma tendência no aumento da utilização de soluções “Passwordless”, ou seja, que não necessitam de senhas ou códigos que precisam ser lembrados, anotados ou armazenados para que sejam utilizados posteriormente. Destacamos isso na próxima página.

Mundo sem senha – Futuro da autenticação

A origem de senhas para acessos no mundo digital é datada do meio dos anos 60, no MIT (Massachusetts Institute of Technology), durante a criação de um sistema de compartilhamento de informações. A tecnologia permitiu acessos simultâneos ao mesmo ambiente virtual, e o acesso personalizado foi introduzido para controlar o tempo que os usuários tinham acesso ao sistema.

O modelo de um acesso único, de um fator único e autenticação, não é mais compatível com a realidade atual. Em 2019, uma pessoa anônima conseguiu ter acesso e liberar publicamente mais de 2,2 bilhões de usuários e senhas em fóruns de hackers, o que ficou conhecido como o maior vazamento de dados já datado.

Avanços em fatores secundários de autenticação sendo amplamente oferecidos no dia a dia das pessoas, tecnologias de biometria, smartphones e reconhecimentos faciais levam os desenvolvedores de tecnologia IAM pensarem em uma questão:

Se as senhas são o elo mais fraco de autenticação em múltiplos fatores, por que ter elas de qualquer forma?

A lógica do mercado é clara, e mostra a necessidade que as empresas vão precisar prestar atenção. **Até 2022**,de acordo com o Gartner Market Guide for User Athentication, **60% das grandes empresas e empresas globais e 90% das empresas médias vão implementar métodos de autenticação que não necessitam de senha, em 50% dos casos.**

Soluções sem senha (No inglês, Passwordless) provém um fator único, forte e confiável de autenticação para conseguir a segurança dos usuários. Como resultado, as empresas que implementam soluções de IAM que não utilizam acessos com senha tem como benefícios:

- **Melhor experiência do usuário**

Aumento de produtividade e noção de segurança entre os usuários do serviço, que não se preocupam com logins e senhas e já estão assegurados de seu acesso privilegiado.

- **Redução dos custos e tempo em TI**

Não existem necessidades dentro do time de TI de resolver problemas dentro das organizações relacionadas à acessos específicos.

- **Postura mais forte de cibersegurança**

Soluções Passwordless trazem confiança, segurança contra ameaças e vulnerabilidades sempre exploradas por criminosos e **eliminam o risco do fator humano nos aspectos envolvendo IAM dentro das organizações.**

Idtechs e meios de pagamento

Dados ligados ao sistema financeiro necessitam de extremo cuidado nas questões de segurança. Historicamente, ao mesmo tempo que as técnicas de fraude melhoraram a sua eficiência para roubar esses dados, empresas tradicionais e startups se movimentaram para promover cada vez mais segurança e agem para tornar os pagamentos mais seguros. Uma das técnicas utilizadas é a adição de camadas de segurança, principalmente nas transações. Além disso, a identificação de que quem está acessando a conta bancária é essencial para manter a segurança dessas instituições, e é nessa frente que as Idtechs tem foco de atuação.

Embora tenha acontecido um enorme avanço na proteção das transações presenciais, como a adição do chip nos cartões de crédito e débito que vão nas maquinas de cartão de crédito, o foco principal dos hackers se volta para os meios digitais. Os mais populares são o e-commerce, que evoluiu muito com a pandemia, e links de mensagens no celular. Por este motivo, surgiram iniciativas como as certificações de segurança incluindo a Payment Card Industry - Data Security Standard (PCI-DSS), que promove mais segurança nas compras em meios eletrônicos. Apesar da adoção dessas práticas por empresas do setor financeiro, essas ações ainda não são obrigatórias por lei, apesar de já estar na pauta de órgãos reguladores. Esse fator pode representar um driver de crescimento para startups atuantes nesse setor.

Os pagamentos instantâneos têm sido um desafio atual na promoção de segurança, tanto que recentemente o Banco Central criou novas regras para o Pix. Dentre as medidas estão o limite de R$ 1000,00 de transferência entre as 20 horas da noite e 6 horas da manhã com o objetivo de evitar roubos e fraudes nesse período. Antes, com a demora de transferência de um saldo de uma conta para a outra permitia o titular da própria conta a identificação de uma movimentação anormal a tempo de comunicar a instituição para interromper a transação, por isso soluções que identifiquem a veracidade do recebimento e envio das partes tendem a ganhar força.

Ademais, as criptomoedas estão começando a ser aceitas como meios de pagamento em determinados locais e situações, mas a cautela em adotar uma solução mais massificada dessa solução se relaciona com o exposto acima de pagamentos instantâneos e a falta de confiança das instituições reguladoras já que, pelo menos no caso do Bitcoin, eles não possuem controle sobre a moeda e mesmo com a blockchain por trás ainda terem maneiras de golpes serem elaborados sobre as moedas digitais.

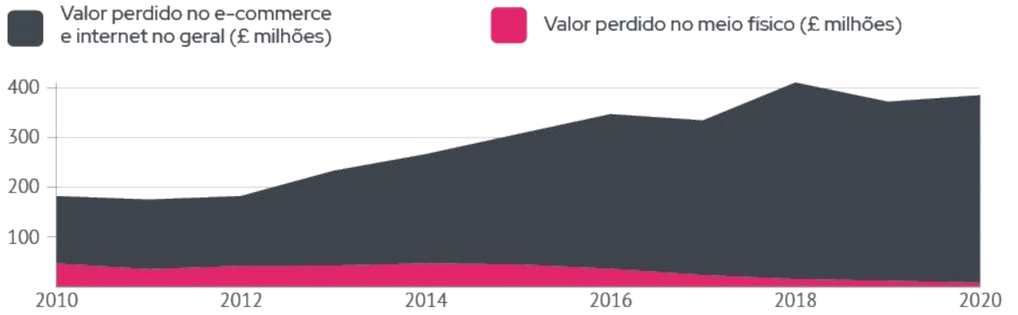
Idtechs no cenário de meios de pagamento

As Idtechs podem atuar em diversas frentes para proteger as contas bancárias, os invasores têm através dos meios eletrônicos praticado uma série de golpes, dentre os mais conhecidos e praticados estão o phishing e smishing os quais roubam as informações do titular das contas, nesse cenário as Idtechs se mostram essenciais.

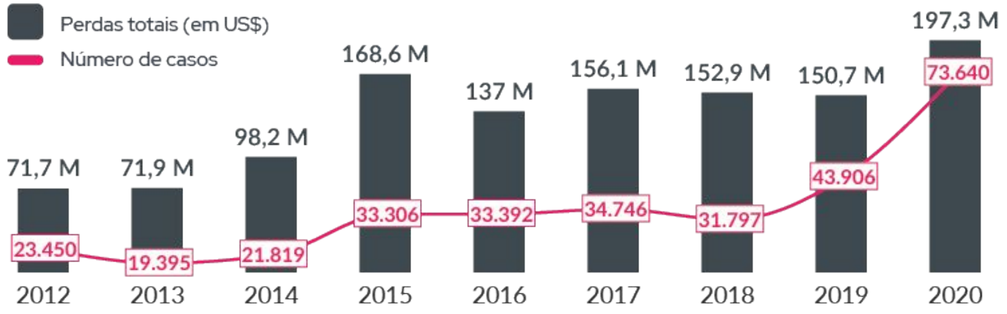
Nos gráficos ao lado podemos notar através de dados do Reino Unido que os golpistas têm migrado cada vez mais para os meios digitais, dado a maior rigidez para conseguir aplicar golpes através de dispositivos físicos. Assim como no Brasil, o Reino Unido adotou a tecnologia do chip e por este motivo incentivou a queda de casos e valores roubados com transações que tinham conexão com o presencial, mas os meios online demonstraram vulnerabilidade para pessoas maliciosas que têm aproveitado brechas para aplicar mais golpes e em tickets mais altos.

Instituições financeiras devem movimentar recursos para impedir perdas e serem mais seguras para os usuários o que mostra uma oportunidade de investimento e atuação para as Idtechs em parceria com o setor financeiro.

Valores perdidos em milhões de libras em golpes, fraudes e falsificações aplicados em cartões no Reino Unido



Valores perdidos por transferências feitas após invasão de contas bancárias no Reino Unido através do remote banking e número de casos desses incidentes



© UK FINANCE FRAUD - THE FACTS 2020 E 2021

payface

Nome: Payface

Público: B2B

Ano de Fundação: 2018

Categoria: Identity & Access Management, Meios de Pagamento, Pagamentos

A Payface é uma empresa que oferece a vendedores de varejo físico uma opção de pagamento via reconhecimento facial. O objetivo da startup é tornar todo o processo de compra mais leve, fácil, seguro e natural.

Atualmente, a solução da Payface está presente em estabelecimentos parceiros de São Paulo e Florianópolis e está no processo de expansão para novas localidades.

A empresa conta com o apoio da Fundação de Amparo a Pesquisa e Inovação no Estado de Santa Catarina (FINESC) e da FINEP. A empresa é certificada com dentro das necessidades de compliance com a certificação PCI-DSS.

O mercado é extremamente promissor, em um contexto de aceitabilidade de pagamentos online durante a pandemia, a transformação no varejo físico também é evidente.

Próximos anos em IAM

Rafael Medeiros
Líder em IAM
Open Consult

Rafael, com toda a sua experiência em IAM, quais são alguns fatores de evolução na tecnologia nos últimos anos que você gostaria de destacar?

Flexibilização das implementações, direcionamento para a nuvem e risco. As soluções de IAM foram, desde sua concepção e, limitadas pela tecnologia da época, monolíticas, rígidas e pouco flexíveis em relação às suas implementações. Ambientes muito complexos e críticos sempre foram um problema para a sustentação, atualização e manutenção da saúde do ecossistema como um todo, enrijecendo até mesmo novas implementações, o que deveria ser uma coisa mais corriqueira. Com o passar dos anos, a compreensão da criticidade da área e, naturalmente, os investimentos envolvidos nas tecnologias, permitiram uma melhora na flexibilização dos ambientes e uma redução drástica da complexidade das implementações, tornando-as mais localizadas, mais simples, menos arriscadas e com menor impacto para o usuário final. A abordagem cloud-first contribuiu (e ainda contribui muito) para alavancar essa redução da complexidade.Embora um ecossistema de IAM naturalmente exija uma interconectividade muito grande com aplicações locais, bancos de dados, diretórios, webservices e aplicações SaaS, ambientes completamente em nuvem são sempre a primeira opção.

Porém, nem sempre são a melhor opção, geralmente direcionando as implementações para um ecossistema híbrido, flexível e funcional.

A consideração cada vez maior do risco para as avaliações de acessos também foi uma contribuição técnica muito grande para o estado atual da tecnologia. Gerenciar as identidades e seus acessos não quer dizer remover acessos arriscados e impossibilitar os colaboradores de trabalhar, mas sim ter segurança e tomar decisões bem-informadas. Acessos elevados, por exemplo, passam por uma série de análises automatizadas que concedem uma pontuação de risco para aquela identidade, o que pode disparar uma anomalia, exigindo multi-fator, aprovações adicionais, ou até uma política específica de certificação e revisão daquele acesso. Tudo de maneira automatizada e inteligente.

Como as tecnologias de IAM brasileiras se comparam ao panorama internacional? Tem alguma empresa brasileira que atua no ramo que você gostaria de destacar?

Infelizmente as tecnologias brasileiras ainda não tem a exposição ao mercado e o tempo de desenvolvimento de produto necessários para a competição com grandes empresas desse ramo. Mas a necessidade do mercado atual gera essa demanda, e isso com certeza é fomentado entre as startups e os investidores que olham para o Brasil com um certo brilho nos olhos. Algumas empresas inovadoras atuam em desenvolvimento in-house para sua própria necessidade, como é o caso da Zup Innovation e seu Live Pass, que cuida de seus processos de autenticação. Outro bom exemplo é a Único, que se identifica como uma IDtech, tendo IAM como core do seu negócio. O mercado é promissor e há muito espaço para crescimento!

O que você espera em termos de tecnologia para IAM nos próximos 10 anos? Quais setores vão ser mais beneficiados?

A transformação é agora, e o caminho para o conceito de IAM 3.0 já está pavimentado. O que falta é, de fato, implementar! A tecnologia evoluiu e se flexibilizou, e a onda de trabalho remoto levou os olhares dispersos para a segurança da identidade, ecoando termos como identity-first security ou identity-centric security. O que eu espero é ver cada vez mais implementações funcionais dos conceitos de IAM 3.0, com inteligência artificial e avaliações de risco, gerenciamento de acessos baseados em políticas imediatas, revisões e certificações automatizadas, análise de anomalias e ações corretivas, concedendo acessos de forma segura para quem de fato precisa, e impedindo de maneira efetiva cenários de access-creep e fraudes de identidade.

Imagino que essas implementações beneficiem muito os setores bancários e as fintechs, onde a redução da superfície de ataque é essencial, assim como a redução do escopo de auditorias, automatizando e facilitando os processos sem perder a qualidade e a integridade das informações.

Próximos anos

Rafael Medeiros
Líder em IAM
Open Consult

Cybertechs

Glossário de categorias

Categorias

NETWORK & INFRASTRUCTURE SECURITY
Companhias que apliquem processos de proteção da infraestrutura de rede, instalando medidas preventivas para negar acesso não autorizado, modificações, exclusões e roubo de recursos e dados. Essas medidas de segurança podem incluir controle de acesso, segurança de aplicativos , firewalls, redes virtuais privadas (VPN), análise comportamental, sistemas de prevenção de intrusão e segurança sem fio. Se relaciona com a camada física de transmissão e conexão. Também englobamos soluções de endpoint e messaging security nesta categoria.

WEB SECURITY
Medidas e protocolos de proteção que empresas utilizam para proteger suas organizações de cyber criminosos e ameaças que usam a web como canal. Se relaciona com a camada não física de segurança, o que engloba internet e segurança de sites.

APPLICATION SECURITY
Medidas de segurança que impedem roubo/sequestro de dados e códigos dentro de dentro de aplicativos e plataformas.

DATA PROTECTION
Data protection engloba empresas responsáveis pela proteção de informações sensíveis à empresa (Banco de Dados, Informações de Corporações) e enquadram às corporações na LGPD.

MOBILE SECURITY
Empresas que atuam com produtos e serviços voltados a garantir a segurança do device (dispositivo móvel), IoS, Android. Via de regra, são companhias que visam a proteção contra ameaças associadas à conexões wireless.

SECURITY OPERATIONS & INCIDENT RESPONSE
Empresas que desenvolvem soluções estruturadas para responder a vazamentos de dados ou ciberataques. A solução visa minimizar os impactos de ataques cibernéticos já realizados, possibilitando um controle da situação com o menor tempo e custo.

IOT SECURITY
Empresas que atuam com segurança relacionada a internet das coisas, aparelhos e networks que estão conectados entre si.

IDENTITY & ACCESS MANAGEMENT
Empresas que desenvolvem soluções que garantem a veracidade das informações e identidades de todas as partes envolvidas em um processo. Aqui se encontram empresas de Identidade as a Service, que capturam, armazenam e asseguram a veracidade do usuário, e companhias de assinatura digital, que trazem inovação e segurança para todo o ciclo de documentos.

Categorias

BLOCKCHAIN
Blockchain as a Service (BaaS) são empresas que possibilitam o desenvolvimento de produtos digitais com a tecnologia blockchain, instalando, hospedando e/ou mantendo redes desse tipo em nome de outras organizações.

FRAUD & TRANSACTION SECURITY
Empresas que aplicam tecnologias de análise de dados para gerar avaliações e insights sobre clientes, permitindo mapear riscos, analisar a conformidade com leis e regulamentações e se prevenir contra perdas, desvio, fraude e ataques cibernéticos.

CLOUD SECURITY
Cloud Secutiry refere-se às startups que atuam com políticas, tecnologias, aplicativos e outros mecanismos de controle utilizados para proteger IP virtualizado, dados, aplicativos, serviços e a infraestrutura associada de computação em nuvem.

SECURITY CONSULTING & SERVICES
Security Consulting and Services refere-se a startups que prestam serviços para testar ou aprimorar serviços de cibersegurança. Um exemplo aqui são empresas que atuam com simulações de ataques cibernéticos como forma de identificar possíveis falhas nos sistemas.

GOVERNANCE, RISK AND COMPLIANCE
Soluções GRC (Governança, Risco e Cokmpliance) são compostas por ferramentas que abrangem a gestão de riscos, governança corporativa e práticas de auditoria e controle, com o objetivo de garantir a conformidade com leis, regulamentos, frameworks e padrões de boas práticas.

Corporates members

APOIO