SPARK Matrix™

Gestão de Segurança e Risco

SPARK Matrix™: Autenticação Baseada em Risco (RBA), 2021

Insights de mercado, avaliação competitiva e classificações de fornecedores

Julio 2021

Quadrant Knowledge Solutions

Índice

Visão geral executiva

Este serviço de pesquisa inclui uma análise detalhada da dinâmica de mercado de soluções de Autenticação Baseada em Risco (RBA) global, principais tendências, cenário de fornecedores e análise de posicionamento competitivo. O estudo fornece uma análise abrangente da concorrência e classificação dos principais fornecedores de RBA na forma da SPARK Matrix. Esta pesquisa fornece informações estratégicas para os fornecedores de tecnologia compreenderem melhor o mercado que suporta suas estratégias de crescimento e para que os usuários avaliem os recursos dos diferentes fornecedores, diferenciais competitivos e posição no mercado.

Principais resultados da pesquisa

A seguir estão os principais resultados da pesquisa:

Tendências de tecnologia

Os fornecedores de RBA continuam fortalecendo seu mecanismo de risco integrando-se amplamente com consórcios do setor ou provedores de detecção de riscos terceirizados. Os fornecedores estão continuamente aproveitando a inteligência artificial, aprendizado de máquina e análises avançadas para oferecer monitoramento e análise em tempo real de grandes entradas de dados, modelos de risco de ajuste fino para acomodar nova inteligência e determinação precisa de pontuações de risco para usuários e transações. Os fornecedores também estão garantindo um acesso seguro e contínuo usando várias técnicas de autenticação biométrica.

Principais tendências em impulsionadores de mercado:

- Os impulsionadores de mercado para o crescimento das soluções RBA incluem investimentos contínuos em projetos de transformação digital, levando ao aumento da disponibilidade online em vários setores, aumento do trabalho remoto, aumento do uso de dispositivos móveis e pessoais e aumento de fraudes online relacionadas à pandemia. Todos esses fatores estão impulsionando a necessidade de soluções de autenticação seguras que ofereçam uma experiência perfeita aos clientes.
- Impulsionada pela crescente demanda por soluções de autenticação adaptáveis, a maioria dos fornecedores líderes de IAM estão oferecendo o recurso e RBA, seja por meio de um mecanismo de risco interno ou pela integração com prestadores de serviços de risco terceirizados. Existem também muitos participantes de nicho que estão oferecendo experiência específica do setor, como para e-commerce.

- Com cenários de negócios interrompidos, aumento do trabalho remoto e aumento da atividade e fraudes online, um mecanismo de autenticação robusto é fundamental neste momento da pandemia da Covid-19. Postula-se que os investimentos críticos em soluções de RBA devem crescer, com as organizações se concentrando mais na segurança e na experiência do usuário contínua, sendo esta a nova estratégia de longo prazo para manter os clientes.

- A robusta proposta de valor da solução de RBA envolve o fornecimento de um mecanismo robusto de pontuação de risco, gerenciamento de regras, mecanismo de autenticação, autoatendimento dos usuários, gerenciamento de alertas e casos e visualização e relatórios. A transformação contínua da solução de RBA impulsionada por tecnologias avançadas está acarretando na adoção pelo mercado entre as grandes empresas.

Dinâmica e tendências de concorrência:

- Este estudo inclui a análise dos principais fornecedores, incluindo Accops, Appgate, Broadcom, CoffeeBean Technology, CyberArk, Duo Security (CISCO), ForgeRock, IBM, Kount, LexisNexis Risk Solution, Microsoft, Okta, OneLogin, OneSpan, Ping Identity, RSA, SecureAuth, Silverfort, Swivel Secure e TransUnion.

- IBM, Kount, Ping Identity, LexisNexis Risk Solution, Okta, Microsoft, Appgate e OneSpan são os de melhor desempenho no mercado de RBA global e se posicionaram como os principais líderes de tecnologia na análise da SPARK Matrix de 2021 para o mercado de RBA. A TransUnion se posicionou como líder emergente em tecnologia com sua proposta geral de valor tecnológico.

Visão geral do mercado e tendências tecnológicas

A Quadrant Knowledge Solutions define RBA como:

"A Autenticação Baseada em Risco (RBA), também conhecida como Autenticação Adaptativa, é uma forma de um poderoso processo de autenticação que utiliza um conjunto de regras para calcular pontuações de risco, considerando fatores abrangentes como endereço IP, navegador, localização física, função do usuário, comportamento, tipo de dispositivo, dia/hora, falhas de login consecutivas e outros fatores antes de conceder acesso. A solução de RBA oferece uma pontuação de risco agregada para cada login de usuário e impõe autenticação flexível com base nessas pontuações de risco".

As soluções de RBA eliminam a fraude calculando o nível de risco para cada solicitação de acesso e, em seguida, decidindo o nível de autenticação necessário para cada login / transação. A RBA ajuda a aliviar vários tipos de fraudes, como apropriação fraudulenta de conta (ATO), fraude de pagamento, fraude móvel, phishing e ameaças cibernéticas, como ataques de botnet, impondo a autenticação de acordo com o nível de risco envolvido.

Antes da RBA, a autenticação estática era a técnica mais popular e amplamente usada até o momento. Como o nome sugere, as organizações usam o mesmo método de autenticação para todos os clientes e transações - através de nomes de usuário e senhas. Apesar de ainda ser usada predominantemente, a autenticação estática apresenta muitos desafios. Os usuários costumam escolher senhas simples, pois são fáceis de lembrar, aumentando assim o risco de fraude. Se escolherem uma senha complexa, será difícil memorizá-la e eles recorrerão a métodos não seguros, como anotá-la, tornando-a vulnerável a roubos. Ambos os cenários envolvem o uso de nomes de usuário e senhas frágeis, comumente usados e mal armazenados, o que facilita para os cibercriminosos invadirem e explorarem o sistema.

A eficácia dos sistemas de autenticação estática foi ainda mais desafiada por um aumento sem precedentes em ataques cibernéticos alimentados pela digitalização de empresas, trabalho remoto, aumento da atividade online e maior adoção de políticas BYOD/WYOD. Além disso, os avanços tecnológicos estão possibilitando que os cibercriminosos encontrem maneiras novas e inovadoras de lançar ataques fraudulentos complexos e de alto volume. Portanto, as organizações estão continuamente adotando tecnologias sofisticadas, como RBA, para que a segurança aprimorada funcione sem problemas nesses ambientes desafiadores.

As soluções de RBA oferecem um mecanismo de autenticação robusto para ajudar a determinar o nível de risco e a possibilidade de fraude. Ela adiciona uma camada

adicional de segurança antes de conceder acesso, avaliando o nível de risco. A avaliação de risco é baseada em vários fatores contextuais, como endereço IP, comportamento e função do usuário, detalhes do dispositivo e da rede, localização física, velocidade geográfica (distância física entre tentativas de login consecutivas), dia da semana, hora do dia, falhas de login consecutivas e assim por diante. Para tentativas de login com uma pontuação de alto risco, o usuário é solicitado a fornecer mais etapas de autenticação para confirmar e validar sua identidade. Além disso, se a pontuação de risco for baixa e o usuário estiver se comportando de maneira esperada, o sistema incluirá menos etapas durante a autenticação do usuário. As soluções de RBA normalmente usam autenticação multifator (MFA) para proteger a identidade de um indivíduo e deter os hackers. Em vez de simplesmente solicitar um nome de usuário e uma senha, a MFA exige um fator de verificação adicional, o que diminui a probabilidade de um ataque cibernético. Embora imponha autenticação rigorosa para usuários mal-intencionados e de alto risco, a RBA garante acesso simplificado para usuários confiáveis. Ao equilibrar a segurança e a experiência do usuário, a RBA está ganhando popularidade entre as organizações em uma série de setores.

A seguir estão os principais recursos de uma solução de RBA:

- **Mecanismo de pontuação de risco** - a pontuação de risco é o recurso mais importante das soluções de Autenticação Baseada em Risco (RBA). A pontuação de risco é o processo de avaliação do risco associado a cada solicitação de acesso, gerando uma pontuação de risco com base nos padrões comportamentais do usuário e fatores como dispositivo, localização, tempo de navegação, endereço IP, tipo de rede, hora do dia, atividade de login e outros. Assim, o mecanismo de pontuação de risco utiliza fatores contextuais relacionados a tentativas de acesso ou transações para estimar melhor o risco envolvido. Com base na pontuação de risco, o sistema decide o nível de autenticação necessário. Para transações ou solicitações de acesso com uma pontuação de risco alta, o sistema solicita etapas adicionais de autenticação ou pode bloquear o acesso. De forma oposta, uma pontuação de risco baixa indica usuários confiáveis e o sistema reduz o nível de autenticação para oferecer acesso contínuo a eles. Esse nível extra de segurança dificulta que hackers e fraudadores obtenham qualquer acesso não autorizado.

- **Gerenciamento de regras** - o gerenciamento de regras, também conhecido como gerenciamento de políticas, facilita o tipo de etapas que a solução de RBA deve executar. No gerenciamento de regras, a autenticação para cada um dos logins do cliente é fornecida com base nas pontuações de risco, que podem ser baixas, médias e altas. Algumas soluções de RBA possuem uma regra embutida na qual o software define certos limites ou intervalos. Muitos

clientes estão procurando um gerenciamento de regras personalizável, onde uma organização possa criar suas próprias regras dependendo de quanto risco pode assumir, dependendo dos clientes e das situações. Além disso, pode haver uma combinação de ambos, onde o software pode ter sua regra padrão junto com uma que pode ser personalizada de acordo com os requisitos.

- **Mecanismo de autenticação (MFA)** - A solução de Autenticação Baseada em Risco ou Autenticação Adaptativa oferece vários níveis de autenticação com base no nível de risco. Os fornecedores de soluções de RBA oferecem Autenticação Multifator (MFA). MFA é um método de autenticação que impõe duas ou mais etapas de verificação antes de conceder acesso a uma conta ou aplicativo. Ela fornece segurança adicional contra roubo de identidade, violação de dados, ataques cibernéticos, etc. A MFA envolve várias etapas de autenticação para verificar se o usuário é quem afirma ser. Para identificar o usuário, a MFA pode utilizar uma combinação de nome de usuário, senha, número PIN ou uma ID, token de hardware/software, autenticação de dois fatores (2FA), senha única (OTP), senha única baseada em tempo (TOTP), FIDO, autenticação biométrica ou mais. A autenticação biométrica, incluindo reconhecimento de impressão digital, reconhecimento facial, reconhecimento de voz, reconhecimento de íris, etc., está se tornando cada vez mais popular entre os fornecedores de RBA.

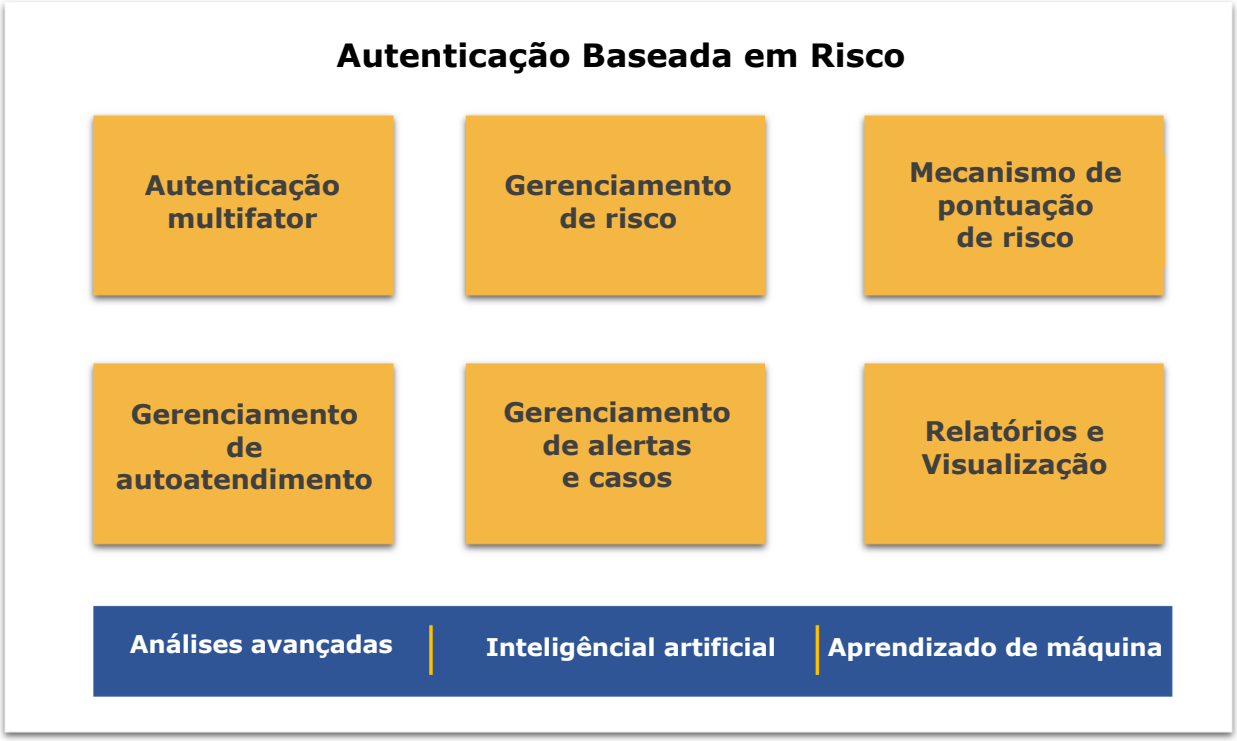
- **Gerenciamento de autoatendimento** - As soluções de RBA oferecem um recurso de autoatendimento que permite aos usuários executar várias ações, como recuperação de ID de usuário e senha, redefinição de senha e outras. O recurso permite que os usuários se cadastrem se forem novos na plataforma e gerenciem seus dispositivos de acordo com as políticas da empresa. Eles podem introduzir um novo dispositivo para autenticação ou remover o dispositivo existente e configurar dispositivos padrão. Os métodos de autenticação podem ser alterados. Por exemplo, os usuários podem decidir se desejam receber uma OTP por e-mail ou SMS.

- **Gerenciamento de alertas e casos** - As soluções de RBA oferecem um recurso de gerenciamento de alertas e casos que ajuda a gerenciar riscos e fraudes em tempo real. Os alertas ajudam a notificar e prevenir rapidamente tentativas de login de alto risco. A solução de RBA também fornece uma investigação de atividades suspeitas. Além disso, ao adotar a solução de RBA, os administradores podem ter uma visão holística dos ataques e, assim, projetar as políticas para proteger a empresa. Com a ajuda da RBA, o administrador e os usuários podem obter um alerta por e-mail/mensagem quando houver tentativa de acesso em um local diferente, dispositivo diferente ou em um momento incomum. O gerenciamento de casos da RBA

ajuda a analisar e marcar atividades como genuínas ou fraudulentas com base na investigação e, em seguida, as marcações são reinseridas no mecanismo de riscos para aumentar a precisão da pontuação de risco das atividades futuras.

- **Visualização e relatórios** - As soluções de RBA oferecem recursos de visualização, incluindo informações de rede, comportamento do usuário, informações do sistema e dados de aplicativos, para ajudar os usuários a navegar em grandes conjuntos de dados. Elas coletam e comparam dados de diferentes fontes e os colocam em uma única apresentação gráfica para facilitar a compreensão e a análise. As soluções de RBA utilizam várias técnicas de visualização, como gráficos, diagramas de pizza, etc., para analisar grandes quantidades de dados e detectar qualquer atividade peculiar. A capacidade de relatórios em uma solução de RBA se refere à geração de relatórios para obter uma visão holística relacionada aos perfis de risco, padrões de fraude, anomalias ativas, dispositivos com possíveis vírus, tendências, locais, endereços IP, etc. Esses relatórios são submetidos a auditorias internas pelas autoridades superiores, comumente conhecidos como relatórios internos, e também são usados para cumprimento de normas externas.

Figura: Principais componentes da solução de Autenticação Baseada em Risco



Fonte: Quadrant Knowledge Solutions

A crescente frequência e sofisticação do cenário de ameaças em evolução está impulsionando a demanda por soluções de Autenticação Baseadas em Risco

Nesta era digital, a maioria dos serviços, como compras, serviços bancários, transações, de socialização e assim por diante, são fornecidos pela Internet. As empresas estão passando por uma transformação digital com o objetivo de reduzir custos, aumentar a eficiência e a disponibilidade e aprimorar a experiência do cliente. No entanto, nesta jornada de transformação digital, as organizações estão enfrentando vários desafios relacionados à segurança.

Alguns dos desafios enfrentados pelas empresas modernas incluem a adoção da nuvem, um aumento em dispositivos BYOD/WYOD e IoT desprotegidos, aumento de ameaças cibernéticas e mecanismos de autenticação frágeis. As empresas modernas estão preferindo os serviços baseados em nuvem em vez do armazenamento local de dados e aplicativos, aumentando assim a probabilidade de acesso não autorizado. Além disso, o aumento da adoção de políticas como Traga seu próprio dispositivo (BYOD) e Use seu próprio dispositivo (WYOD) está permitindo que os usuários acessem informações/recursos por meio de uma variedade de dispositivos desprotegidos, incluindo notebooks, computadores, tablets, smartphones e dispositivos vestíveis, resultando em desafios de segurança de dados e rede para as empresas. E mais: os cibercriminosos estão usando técnicas cada vez mais sofisticadas para realizar ataques cibernéticos por meios como ransomware, phishing, roubo de identidade, controle de conta, ataques de botnet e muitos mais. Os hackers estão explorando as crescentes tendências de trabalho remoto e compras online. Em tais ambientes de alto risco, os métodos tradicionais de autenticação estática que dependem de senhas fracas e facilmente interceptáveis são insuficientes para fornecer uma segurança adequada.

Portanto, as organizações estão adotando cada vez mais as soluções de Autenticação Baseada em Risco (RBA), também conhecidas como soluções de Autenticação Adaptativa. Elas ajudam as empresas a superar esses desafios garantindo uma segurança robusta e oferecendo uma experiência perfeita para o cliente. A Autenticação Baseada em Risco usa como base um conjunto de regras que englobam vários fatores contextuais para calcular o risco associado a qualquer usuário ou transação. Com base na pontuação de risco atribuída, ela determina o nível de autenticação necessário. As soluções de RBA oferecem autenticação multifator (MFA) adaptável, que impõe etapas de autenticação rigorosas para usuários com pontuação de risco alta e autenticação menos rigorosa para oferecer uma experiência sem complicações aos usuários confiáveis com pontuação de risco baixa. Assim, as soluções de RBA oferecem um mecanismo de autenticação perfeito para organizações que buscam atingir o equilíbrio certo entre alta segurança e experiência de usuário aprimorada.

As soluções de RBA estão continuamente se transformando, impulsionadas por análises avançadas, IA, AM e biometria comportamental

Para lidar com o problema de sofisticação e volume crescentes de ataques cibernéticos, os fornecedores estão aprimorando suas soluções de RBA integrando tecnologias emergentes como IA, AM, análises avançadas e biometria. As soluções de RBA usam inteligência artificial (IA) e aprendizado de máquina (AM) para permitir o monitoramento e análise em tempo real de grandes conjuntos de dados. Com as tecnologias de IA e AM, as soluções de RBA podem monitorar com eficiência o comportamento de um usuário para fornecer uma precisão com relação aos padrões de perfil e login. Elas rastreiam qualquer anomalia na localização do dispositivo, endereço IP, hora de login e rede. Impulsionado por AM, o mecanismo de risco é calibrado para acomodar qualquer nova inteligência ou percepção. As soluções de RBA usam análises avançadas para determinar com precisão a pontuação de risco de qualquer usuário ou tentativa de login, de modo que os usuários de risco sejam solicitados com autenticação mais rígida, enquanto os usuários confiáveis recebem uma experiência de login sem complicações. Além disso, a maioria dos fornecedores de RBA também está optando pela autenticação biométrica, pois ela garante segurança definitiva por ser exclusiva para cada usuário, não poder ser roubada ou adulterada e por oferecer facilidade de uso. Como a autenticação biométrica garante a identificação e verificação precisas de um indivíduo, ela está se mostrando crítica para a prevenção de fraudes online. Assim, as soluções de RBA estão aproveitando a IA, AM, análises avançadas e biometria para garantir segurança robusta e experiência aprimorada do cliente.

Como o setor bancário e financeiro tem sido o principal alvo dos cibercriminosos, os bancos e instituições financeiras foram os primeiros a adotar as soluções de RBA. Além do setor bancário, outros setores como de varejo, jogos, saúde e aviação também estão adotando cada vez mais a transformação digital. O setor de e-commerce está testemunhando um boom impulsionado pela pandemia da COVID-19 em curso. Portanto, os fornecedores de e-commerce estão exigindo cada vez mais mecanismos de autenticação robustos, como a RBA, que oferecem proteção contra fraudes online como phishing, controle de conta, estorno, fraude amigável e muito mais, garantindo uma experiência ininterrupta para o cliente. Os jogos online são outro segmento sempre no radar dos hackers, já que é um setor lucrativo em termos monetários. A RBA não só garante o acesso seguro a contas online como também remove o risco de anonimato ao oferecer autenticação biométrica. Como a saúde é outro vetor primordial para ataques de phishing e malware, as organizações de saúde estão usando sistemas de RBA para proteger as informações confidenciais dos pacientes, como dados pessoais, seguros, dados bancários, registros médicos, etc. As soluções de RBA também estão sendo utilizadas no ramo de aviação, que lida com um vasto volume de dados pessoais de clientes.

Indo além, devido à pandemia da COVID-19, a maioria da força de trabalho global tem trabalhado de maneira remota. Com a necessidade de garantir o acesso remoto seguro, as organizações estão adotando soluções de RBA para verificar se os usuários que acessam os dados e recursos da empresa são funcionários e clientes genuínos. Com sua capacidade de equilibrar segurança e experiência do cliente, a demanda por soluções de RBA aumentará em todos os setores.

Cenário competitivo e análise

A Quadrant Knowledge Solutions conduziu uma análise aprofundada dos fornecedores de Autenticação Baseada em Risco, avaliando seus produtos, presença no mercado e proposta de valor para o cliente. A avaliação é baseada em pesquisas primárias com entrevistas de especialistas, análise de casos de uso e análise interna da Quadrant do mercado em geral. Este estudo inclui uma análise dos principais fornecedores, including Accops, Appgate, Broadcom, CyberArk, CoffeeBean Technology, Duo Security (Cisco), ForgeRock, IBM, Kount, LexisNexis Risk Solutions, Ping Identity, Microsoft, OneLogin, OneSpan, Okta, RSA, Silverfort, SecureAuth, Swivel Secure e TransUnion.

IBM, Ping Identity, Kount, LexisNexis Risk Solutions, Okta, Microsoft, Appgate e OneSpan são os líderes de desempenho e tecnologia no mercado global de RBA. Essas empresas fornecem uma plataforma de tecnologia de autenticação baseada em risco sofisticada e abrangente para lidar com uma variedade de casos de uso de RBA.

A **IBM Security** oferece uma solução de RBA integrada com recursos funcionais de ponta a ponta, fornecendo autenticação robusta, gerenciamento de risco e gerenciamento de acesso baseado em nuvem. A solução de RBA da IBM é incorporada ao consórcio de inteligência de risco, mecanismo de risco em identidade digital e integração baseada em API para autenticação de risco contínua e aprimorada.

A solução de RBA da **Kount** é movida por tecnologia patenteada baseada em IA, com relatórios detalhados, inteligência abrangente, oferecendo proteção perfeita contra fraudes de pagamento. A Kount incorpora uma ferramenta de análise biométrica passiva que monitora padrões de comportamento para fornecer proteção aprimorada contra bots, detecção de risco precisa para usuários e proteção de dados contra logins maliciosos.

A **Ping Identity** é uma fornecedora líder de IAM com um mecanismo de risco interno robusto e políticas de autenticação configuráveis. Ela usa modelos UEBA e AM com IA para analisar preditores de risco em tempo real e garantir um login sem problemas. O gerenciamento de risco da empresa com serviços terceirizados pode ser bem integrado em sua plataforma para lidar com vários casos de uso de RBA e MFA.

A **LexisNexis® Risk Solutions** é bem conhecida no mercado por seus fortes recursos de RBA em toda a jornada do cliente para lidar com fraudes e, ao mesmo tempo, oferecer uma experiência ininterrupta ao cliente. A recente adição do recurso de biometria comportamental da empresa ajuda na tomada de decisões

aprimorada sobre fraude com recursos de autenticação robustos. A **Okta** com o Auth0 oferece plataformas para gerenciar uma gama mais ampla de soluções de autenticação baseada em risco. A plataforma está equipada com recursos de AM, gerenciamento de acesso por API para segurança aprimorada e funcionalidade de geração de relatórios. A **Microsoft** continua aprimorando suas soluções de autenticação baseada em risco inteligentes com tecnologia de AM e automação para login de usuário seguro e sem complicações.

A **Appgate** é reconhecida por seus recursos de RBA que são orientados por um AM poderoso e regras robustas para fornecer autenticação contínua. A **OneSpan** é reconhecida por sua solução de análise de risco que aproveita o poder da IA e AM para detecção de ameaças e tomada de decisões informadas para prevenção de fraudes. A solução incorpora uma plataforma preparada para o futuro com integração perfeita de tecnologia de terceiros. A **TransUnion** aprimorou significativamente seus recursos de tecnologia e continua se concentrando nos módulos de RBA. A empresa continua aproveitando o aprendizado de máquina para prever resultados de transações digitais, independentemente do cliente ou dispositivo ser conhecido ou desconhecido.

A **RSA** continua desfrutando de seu forte conhecimento sobre domínios para oferecer uma plataforma abrangente de detecção de fraudes que aproveite a MFA baseada em risco para proteção aprimorada. O recurso de autenticação baseada em risco da RSA é acoplado à análise com AM robusta de vários indicadores de risco, juntamente com controles de política refinados. A **CyberArk** está entre os fornecedores líderes que oferecem recursos de solução de RBA da próxima geração com um mecanismo de análise comportamental do usuário orientado por IA que cria percepções aprofundadas em tempo real. A **Broadcom** fornece funcionalidades de RBA aprimoradas com recursos OOTB. A plataforma da **ForgeRock** é explorada por IA avançada para orquestrar jornadas de risco e realizar um modelo de segurança Zero Trust ou CARTA e fornecer um processo de autenticação baseada em risco abrangente. A **OneLogin** aproveita a tecnologia de pontuação de risco por IA com uma solução adaptativa e aprimorada para proteção contra ameaças e ataques sofisticados com base em credenciais, oferecendo SSO sem atrito. A **Duo Security** (Cisco) oferece uma solução poderosa equipada com recursos robustos de MFA. A solução se integra a qualquer aplicativo para proteger usuários e dispositivos.

A **SecureAuth**, com seus recursos poderosos, continua alavancando análises orientadas por IA integradas com configurações granulares, SSO e relatórios detalhados com envolvimento do usuário sem problemas. A **CoffeeBean Technology** oferece soluções robustas de autenticação baseada em risco para garantir recursos aprimorados de autenticação adaptativa. A empresa planeja continuar aprimorando sua integração com os novos protocolos FIDO. A **Accops**

tem grande experiência no espaço de RBA para detecção de SSO, inclui logs de auditoria detalhados para maior eficácia no desempenho de sua autenticação multifator. A **Swivel Secure** oferece plataformas de RBA robustas que suportam uma ampla gama de requisitos arquitetônicos que envolvem uma vasta opção de fatores de autenticação. Eles estão posicionados entre os desafiantes emergentes. A plataforma da **Silverfort** é bem conhecida por seu mecanismo de risco orientado por IA e recursos aprimorados de autenticação adaptativa e ela está posicionada como aspirante.

Principais fatores competitivos e diferenciais tecnológicos

A maioria dos fornecedores líeders de Autenticação Baseada em Risco (RBA) pode fornecer recursos de RBA prontos para uso, boa experiência do cliente, integração perfeita, um mecanismo de pontuação de risco robusto, gerenciamento de regras, mecanismo de autenticação (MFA), autoatendimento do usuário, gerenciamento de alertas e casos, visualização e relatórios. Porém, a flexibilidade de implementação e dos mecanismos de autenticação pode variar de acordo com as ofertas de diferentes fornecedores. Impulsionados pela concorrência cada vez maior, os fornecedores estão cada vez mais procurando melhorar seus recursos de tecnologia e proposta de valor geral para se manterem competitivos. Alguns dos principais fatores competitivos e diferenciais para a avaliação dos fornecedores de RBA são os seguintes:

- **A sofisticação dos recursos de tecnologia**: o volume, a sofisticação e as complexidades crescentes em fraudes online estão elevando consistentemente a exposição ao risco das instituições financeiras e das empresas. Nos últimos anos, organizações globais em diversas regiões geográficas observaram um aumento nos ataques fraudulentos, incluindo fraudes de identidade, fraudes de pagamento, violações de segurança cibernética e outros, levando à necessidade de uma solução de RBA robusta. Os impostores estão cada vez mais usando ferramentas de ponta para lançar ataques sofisticados e complexos. Uma solução de RBA poderosa, escalonável e avançada é necessária para verificar as crescentes ameaças de fraude e o aumento na sofisticação de tais ameaças, bem como para gerenciar os desafios de padrões de fraude e dinâmica de ataque cibernético em constante mudança. Assim, os usuários devem avaliar uma solução de RBA que ofereça recursos abrangentes, incluindo o gerenciamento de grandes conjuntos de dados, um mecanismo baseado em risco, recursos de autenticação avançados como MFA e autenticação biométrica, detecção e interdição de fraude em tempo real, gerenciamento de alertas e casos, visualização e relatórios e gerenciamento de regras. Além disso, a proposta de valor do fornecedor para o cliente pode diferir em termos de facilidade de implementação, facilidade de uso, relação custo-benefício, suporte para uma ampla gama de casos de uso baseados em risco e fraude, serviço de suporte global e outros. A maioria dos fornecedores está oferecendo essas funcionalidades e continua investindo fortemente em aprimorar ainda mais suas plataformas com IA, AM, protocolos de autenticação mais recentes e análises baseadas em risco. Uma solução de RBA avançada pode fornecer uma experiência superior ao cliente e detectar atividades de login mal-intencionadas em tempo real.

- **Visão tecnológica e roteiro**: o uso de tecnologia sofisticada por hackers está permitindo um aumento nos crimes cibernéticos, como invasões de conta (ATO), logins maliciosos, fraudes de pagamento, ataques de botnet, ataques direcionados sofisticados, fraude de fidelidade e outros. Portanto, é imperativo que os usuários escolham o parceiro de tecnologia apropriado de acordo com seus casos de uso específicos, tendências de fraude em evolução e seu roteiro de transformação digital. Os fornecedores de RBA estão constantemente aprimorando e inovando sua proposta de valor de tecnologia em termos de fornecimento de uma solução de autenticação baseada em risco holística com integração de dados abrangente, verificação e validação de cliente, mecanismo de risco sofisticado impulsionado por análises avançadas, IA e AM, desenvolvimento de modelo personalizado, robusta investigação e gerenciamento de casos, ferramentas de visualização avançada, incorporação de fluxos de trabalho e automação de processos, entre outros. Os fornecedores também estão se concentrando em oferecer uma experiência digital excepcional aos clientes por meio de um processo de RBA contínuo. As organizações devem avaliar cuidadosamente os recursos de tecnologia existentes do fornecedor, juntamente com sua visão tecnológica e roteiro para melhorar a satisfação geral e a experiência de propriedade do cliente em direção ao sucesso a longo prazo.

- **Experiência e conhecimento sobre domínios do fornecedor**: instituições financeiras e empresas devem conduzir uma avaliação abrangente de várias soluções de RBA e fornecedores antes de tomar uma decisão final. As organizações devem avaliar a experiência e o conhecimento sobre domínios dos fornecedores para entender seus problemas de negócios exclusivos, casos de uso e requisitos específicos do setor. Os usuários devem buscar facilidade de uso, abrangência da oferta, flexibilidade do software para se adaptar às constantes mudanças do mercado e requisitos regulatórios, minimizando o custo total de propriedade e transparência. As empresas devem buscar soluções que garantam uma ferramenta de análise de risco unificada e eficaz que forneça rapidamente as informações apropriadas e vitais para a tomada de decisões corretas. Os usuários devem estar atentos a soluções integradas que ofereçam cobertura abrangente com uma visão contínua e holística dos clientes e das contas associadas, bem como os fatores de risco. As instituições financeiras devem procurar soluções de RBA que suportem várias formas de IA e modelos de detecção baseados em regras e devem ter potencial para integração de dados de terceiros. Os usuários também devem procurar uma solução com um histórico de implementações em grande escala bem-sucedidas e analisar cuidadosamente os estudos de caso existentes dessas implementações. Isso

deve formar a base para preparar as melhores práticas para implantemeções de uma plataforma de RBA.

- **IA, AM e análises avançadas**: inteligência artificial, aprendizado de máquina e análises avançadas são tecnologias emergentes no espaço de RBA. Impulsionada por IA, AM e análises avançadas, uma solução de RBA fornece uma análise aprimorada de enormes conjuntos de dados, aumentando assim a eficiência da solução. Desenvolvida com essas tecnologias emergentes, uma solução de RBA oferece monitoramento contínuo e detecção de anomalias em tempo real. Além disso, a solução ajuda a detectar um hábito ou desvio do usuário que possa precisar de mais autenticação. As análises avançadas fornecem detecção de risco precisa para todos os usuários em cada sessão de login. Os fornecedores estão cada vez mais usando técnicas de análise avançada, como análise preditiva, análise de big data, análise de redes sociais, análise de comportamento do usuário, análise de gráfico, PNL, modelos de classificação de risco e outras para superar os desafios no domínio de RBA e maximizar a eficiência e eficácia gerais de sua solução. Modelos robustos de classificação de risco do cliente impulsionados por IA oferecem pontuações de risco em tempo real com base em vários fatores, e seus recursos aprimorados de detecção podem atravessar jurisdições e empresas.

- **Integração e interoperabilidade**: integração e interoperabilidade contínuas com as tecnologias existentes dos fornecedores estão entre os fatores cruciais que afetam a implementação da tecnologia e a experiência de propriedade. A solução de RBA deve oferecer integração e interoperabilidade contínuas com várias soluções de análise de fraude, consórcio do setor, sinais de risco de terceiros, soluções IAM e aplicativos de segurança móvel para garantir uma operação sem problemas, troca de informações e flexibilidade de implementação. A solução também deve oferecer suporte à integração com soluções terceirizadas de conformidade de dispositivos, soluções SIEM e prestadores de serviços de pagamento e gateways. Os usuários devem avaliar a capacidade dos fornecedores de fornecer integração imediata com as melhores tecnologias e integração personalizada com vários produtos corporativos e de detecção de fraude. Além disso, os usuários devem avaliar a plataforma de RBA em termos de capacidade de ofertar amplitude e profundidade de integração específicas para suas ferramentas e infraestrutura existentes.

SPARK Matrix™: avaliação e classificação de desempenho estratégico

A SPARK Matrix da Quadrant Knowledge Solutions fornece uma síntese do posicionamento de mercado dos principais participantes. A SPARK Matrix fornece uma representação visual dos participantes do mercado e percepções estratégicas sobre como cada fornecedor se classifica em relação aos seus concorrentes, em relação a vários parâmetros de desempenho com base na categoria de excelência em tecnologia e impacto no cliente. A Análise do cenário competitivo da Quadrant é um guia de planejamento útil para tomadas de decisões estratégicas, tais como encontrar perspectivas de fusões e aquisições, parcerias, expansão geográfica, expansão de portfólio e outros.

Cada participante do mercado é analisado em relação a vários parâmetros de Excelência em tecnologia e Impacto no cliente. Em cada um dos parâmetros (ver gráficos), um índice é atribuído a cada fornecedor, de 1 (mais baixo) a 10 (mais alto). Essas classificações são designadas a cada participante do mercado com base nos resultados da pesquisa. Com base nas avaliações individuais dos participantes, os valores das coordenadas X e Y são calculados. Essas coordenadas são finalmente usadas para produzir a SPARK Matrix.

Excelência em tecnologia	Peso
Sofisticação da tecnologia	20%
Estratégia de diferencial competitivo	20%
Diversidade de aplicações	15%
Escalabilidade	15%
Integração e interoperabilidade	15%
Visão e roteiro	15%

Impacto no cliente	Peso
Estratégia e desempenho do produto	20%
Presença de mercado	20%
Histórico comprovado	15%
Facilidade de implementação e uso	15%
Excelência no atendimento ao cliente	15%
Proposta de valor exclusiva	15%

Critérios de avaliação: excelência em tecnologia

- **Sofisticação da tecnologia**: a capacidade de fornecer recursos funcionais e de produto abrangentes, inovações tecnológicas, arquitetura de produto/plataforma e outros.
- **Estratégia de diferencial competitivo**: a capacidade de se diferenciar dos concorrentes por meio de recursos funcionais e/ou inovações e/ou estratégia GTM, proposta de valor para o cliente e outros.

- **Diversidade de aplicações**: a capacidade de demonstrar a implementação do produto para uma variedade de setores da indústria e/ou diversos casos de uso.
- **Escalabilidade**: a capacidade de demonstrar que a solução oferece suporte à escalabilidade à nível empresarial, juntamente com exemplos de casos de clientes.
- **Integração e interoperabilidade**: a capacidade de oferecer plataformas de produtos e tecnologias que suportem a integração com as melhores tecnologias da categoria, fornecendo integrações prontas para uso e suporte e serviços com API aberta.
- **Visão e roteiro**: avaliação da estratégia de produto do fornecedor e roteiro com a análise das principais melhorias planejadas para oferecer produtos/tecnologia superiores e melhorar a experiência de propriedade do cliente.

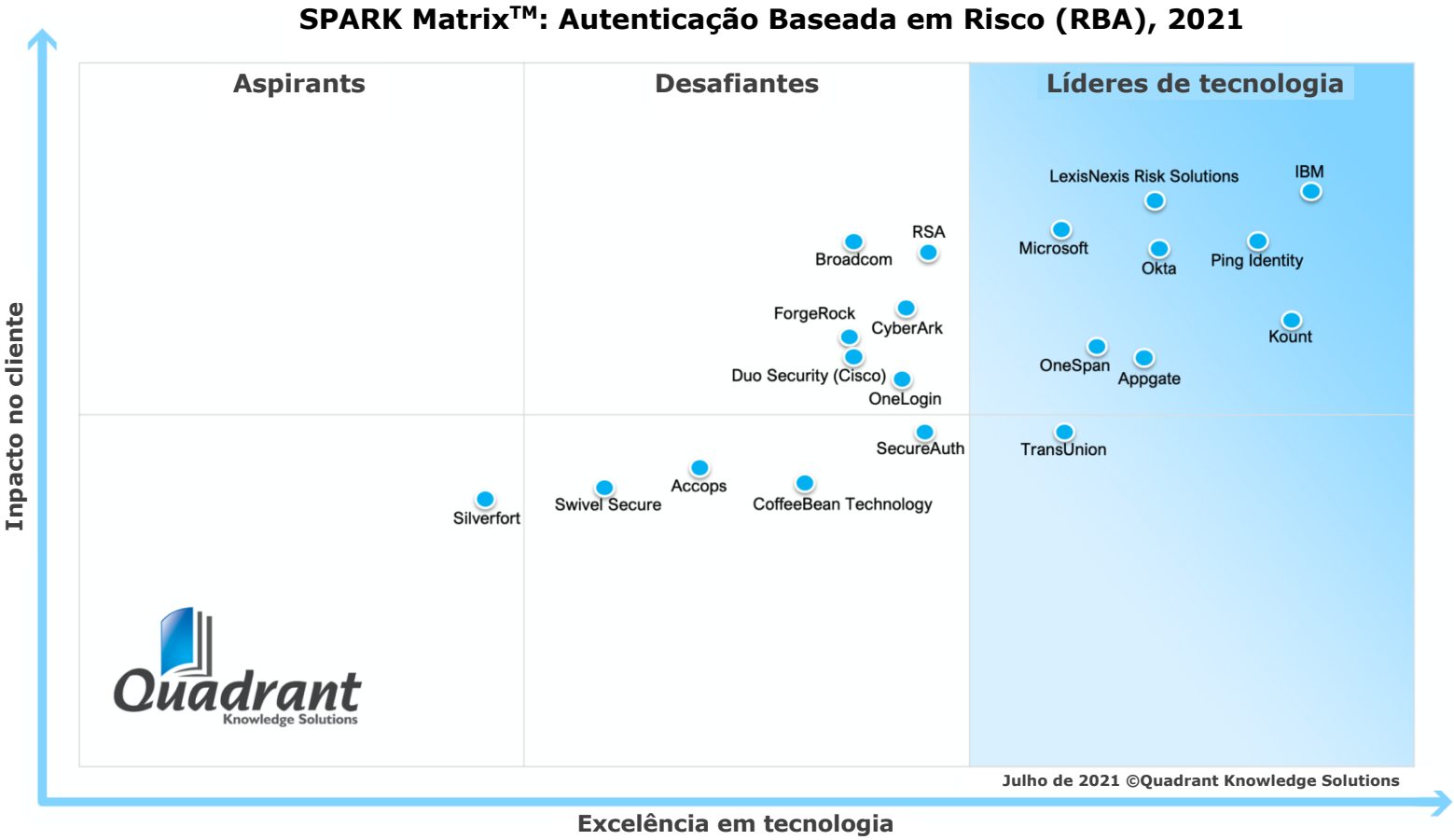
Critérios de avaliação: impacto no cliente

- **Estratégia e desempenho do produto**: avaliação de vários aspectos da estratégia e desempenho do produto em termos de disponibilidade do produto, relação custo-benefício, excelência na estratégia GTM e outros parâmetros específicos do produto.
- **Presença de mercado**: a capacidade de demonstrar receita, base de clientes e crescimento no mercado, juntamente com a presença em várias regiões geográficas e setores da indústria.
- **Histórico comprovado**: avaliação da base de clientes existente do segmento de empresas de pequeno/médio porte, empresas de médio e grande porte, taxa de crescimento e análise de estudos de caso de clientes.
- **Facilidade de implementação e uso**: a capacidade de fornecer experiência de implementação superior aos clientes, oferecendo suporte à implementação flexível ou capacidade de demonstrar experiência superior de compra, implementação e uso. Além disso, os produtos dos fornecedores são analisados em termos de oferta de uma interface de usuário intuitiva e experiência de propriedade.

- **Excelência no atendimento ao cliente**: a capacidade de demonstrar uma variedade de serviços profissionais de consultoria, treinamento e suporte. Além disso, a estratégia do parceiro de serviços da empresa ou a capacidade de integração do sistema em todas as regiões geográficas também é considerada.
- **Proposta de valor exclusiva**: a capacidade de demonstrar diferenciais exclusivos impulsionados pelas tendências contínuas do setor, convergência do setor, inovação tecnológica e outros.

SPARK Matrix™: Autenticação Baseada em Risco (RBA)
Avaliação e classificação de desempenho estratégico

Figura: SPARK Matrix™ de 2021
(Avaliação e classificação de desempenho estratégico)
Mercado de Autenticação Baseada em Risco (RBA)



Perfis dos fornecedores

O seguinte perfil de fornecedor é escrito com base nas informações fornecidas pelos executivos do fornecedor como parte do processo de pesquisa, juntamente com as informações disponibilizadas publicamente. A equipe de pesquisa da Quadrant também consultou o site da empresa, white papers, blogs e outras fontes para escrever o perfil. Um perfil detalhado do fornecedor e uma análise de todos os fornecedores, juntamente com vários cenários competitivos, estão disponíveis como uma entrega da pesquisa personalizada para nossos clientes. Os usuários são aconselhados a falar diretamente com os respectivos fornecedores para ter uma compreensão mais abrangente de suas capacidades técnicas. Os usuários são aconselhados a consultar a Quadrant Knowledge Solutions antes de tomar qualquer decisão de compra com relação à tecnologia de RBA e à seleção do fornecedor com base nos resultados da pesquisa aqui incluídos.

Appgate

URL: https://www.appgate.com/

Fundada em 2017 e sediada na Flórida, EUA, a Appgate é uma grande fornecedora de segurança, software e serviços prontos para nuvem e híbridos. A empresa oferece acesso de rede zero trust, proteção contra ameaças digitais, autenticação baseada em risco e serviços de consultoria sobre ameaças. A Appgate oferece uma solução de RBA robusta que inclui recursos como autenticação personalizável, monitoramento de transações e orquestração de risco.

A solução de autenticação da Appgate oferece autenticação multifator robusta por meio de SDKs móveis que permite a autenticação via notificação push, código QR, reconhecimento facial biométrico e OTPs por SMS ou e-mail. Esses recursos de autenticação personalizáveis oferecem proteção a nível de usuário, adaptando-se aos comportamentos conhecidos do usuário, usando o contexto para verificar os usuários, aprovar transações legítimas e impor fluxos de trabalho de autenticação. Esse recurso ajuda ainda mais as organizações a criar regras personalizadas para tomar ações imediatas, como autenticação progressiva, com base na tolerância a riscos e impor métodos de autenticação que funcionem melhor para a empresa.

Os recursos de monitoramento e autenticação de transações permitem que as empresas criem fluxos de trabalho personalizados e integrem soluções perfeitamente. A RBA da Appgate usa recursos de aprendizado de máquina equipados com um sistema flexível e baseado em regras para detecção robusta de risco transacional. Este modelo elimina a tomada de decisão binária, analisando variáveis de risco adicionais e oferecendo técnicas de autenticação sofisticadas. O recurso de orquestração de risco do tipo arrastar e soltar orientado a objetos facilita a vinculação de autenticação e monitoramento de transações, permitindo que as empresas criem um fluxo de trabalho de autenticação personalizável e contínuo com base nos limites de risco.

A solução de RBA da Appgate oferece uma abordagem em camadas para combater os riscos de autenticação e transações com eficiência. A solução permite a integração de sistemas para orquestrar perfeitamente em conjunto, oferecendo uma proteção aprimorada. Isso permite que as empresas autentiquem usuários, monitorem transações e implementem fluxos de trabalho com base na tolerância ao risco.

Perspectiva do analista

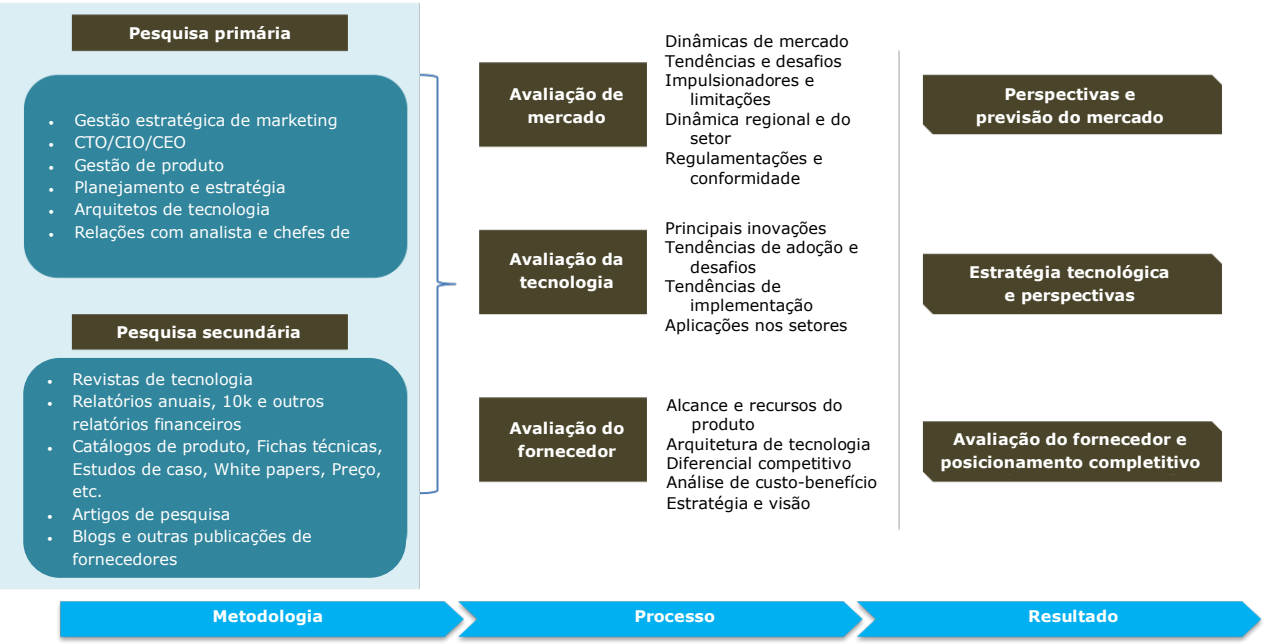
A seguir está a análise dos recursos da Appgate no mercado de RBA:

- A solução de RBA detecta e mitiga anomalias de comportamento do dispositivo e do usuário em tempo real por meio da identificação do dispositivo e autenticação multifator. Ela é impulsionada por um aprendizado de máquina robusto e regras rígidas, oferecendo um gerenciamento perfeito de fraudes com um console simplificado. A solução fornece autenticação sem atrito com inteligência de ameaças, detecção ágil de fraudes, facilidade de integração, identificação de dispositivo confiável e uma interface de arrastar e soltar, tornando-os assim os principais diferenciais.

- Do ponto de vista da presença geográfica, a empresa tem uma presença importante na Europa, América do Sul e Japão. A empresa oferece suporte a vários casos de uso por meio de monitoramento e autenticação eficazes de transações, autenticação baseada em risco e contexto e integração contínua.

Metodologias da pesquisa

A Quadrant Knowledge Solutions usa uma abordagem abrangente para conduzir pesquisas de perspectivas de mercado global para várias tecnologias. A abordagem de pesquisa da Quadrant fornece aos nossos analistas a estrutura mais eficaz para identificar tendências de mercado e tecnologia e ajuda na formulação de estratégias de crescimento significativas para nossos clientes. Todas as seções do nosso relatório de pesquisa são preparadas com um tempo considerável e processo de reflexão antes de passar para a próxima etapa. A seguir está uma breve descrição das principais seções das metodologias da nossa pesquisa.



Pesquisa secundária

A seguir estão as principais fontes de informações para a realização da pesquisas secundária:

Banco de dados interno da Quadrant

A Quadrant Knowledge Solutions mantém um banco de dados proprietário em vários mercados tecnológicos. Este banco de dados fornece ao nosso analista uma base adequada para iniciar o projeto de pesquisa. Este banco de dados inclui informações das seguintes fontes:

- Relatórios anuais e outros relatórios financeiros
- Listas de participantes do setor
- Dados secundários publicados sobre empresas e seus produtos

- Banco de dados de tamanhos de mercado e previsão para diferentes segmentos de mercado
- Principais tendências de mercado e tecnologia

Pesquisa de literatura

A Quadrant Knowledge Solutions aproveita várias assinaturas de revistas e outras publicações que abordam uma ampla gama de assuntos relacionados à pesquisa tecnológica. Também usamos a extensa biblioteca de diretórios e periódicos em vários domínios de tecnologia. Nossos analistas usam postagens de blog, white papers, estudos de caso e outras literaturas publicadas pelos principais fornecedores de tecnologia, especialistas online e publicações de notícias do setor.

Contribuições dos participantes do setor

Os analistas da Quadrant coletam documentos relevantes, como white papers, catálogos, estudos de caso, listas de preços, planilhas de dados e outros relatórios de todos os principais participantes do setor.

Pesquisa primária

Os analistas da Quadrant usam um processo de duas etapas para conduzir pesquisas primárias que nos ajudam a captar informações de mercado significativas e mais precisas. Abaixo segue o processo de duas etapas da nossa pesquisa primária:

Estimativa de mercado: com base na abordagem top-down e bottom-up, nosso analista analisa todos os participantes do setor para estimar seus negócios no mercado de tecnologia para vários segmentos de mercado. Também buscamos informações e verificação de desempenho dos negócios dos clientes como parte de nossas entrevistas na pesquisa primária ou por meio de um questionário de mercado detalhado. A equipe de pesquisa da Quadrant conduz uma análise detalhada dos comentários e contribuições fornecidos pelos participantes do setor.

Entrevista com clientes: a equipe de analistas da Quadrant conduz uma entrevista telefônica detalhada com todos os principais participantes do setor para obter suas perspectivas da dinâmica atual e futura do mercado. Nosso analista também obtém detalhes sobre sua experiência em primeira mão com a versão demo do produto do fornecedor para compreender suas funcionalidades tecnológicas, experiência do usuário, recursos do produto e outros aspectos. Com base nos requisitos, os analistas da Quadrant entrevistam mais de uma pessoa de cada um dos participantes do mercado para verificar a precisão das informações fornecidas. Normalmente, entramos em contato com funcionários do cliente em uma das seguintes funções:

- Gestão estratégica de marketing
- Gestão de produtos
- Planejamento de produto
- Planejamento e estratégia

Comentários dos parceiros de canal e usuários finais

A equipe de pesquisa da Quadrant consulta vários parceiros de canal de vendas, incluindo distribuidores, integradores de sistema e consultores para compreender a perspectiva detalhada do mercado. Nossos analistas também obtêm comentários de usuários finais de vários setores e regiões geográficas para entender os principais problemas, tendências de tecnologia e recursos do fornecedor no mercado de tecnologia.

Análise de dados: previsão de mercado e análise da concorrência

A equipe de analistas da Quadrant reúne todas as informações necessárias de pesquisas secundárias e primárias para gerar um banco de dados eletrônico. Esses bancos de dados são então analisados, verificados e cruzados de várias maneiras para obter o panorama certo do mercado em geral e seus segmentos. Após analisar todos os dados de mercado, tendências do setor, tendências de mercado, tendências de tecnologia e principais problemas, preparamos previsões de mercado preliminares. Esta previsão preliminar do mercado é testada com base em vários cenários de mercado, cenário econômico, tendências do setor e dinâmica econômica. Por fim, a equipe de analistas chega ao cenário de previsão mais preciso para o mercado em geral e seus segmentos.

Além das previsões de mercado, nossa equipe realiza uma análise detalhada dos participantes do setor para preparar o cenário competitivo e uma análise de posicionamento de mercado para o mercado em geral, bem como para vários segmentos de mercado.

SPARK Matrix: avaliação e classificação de desempenho estratégico

A SPARK Matrix da Quadrant Knowledge Solutions fornece uma síntese do posicionamento de mercado dos principais participantes. A representação da SPARK Matrix fornece uma representação visual dos participantes do mercado e percepções estratégicas sobre como cada fornecedor se classifica em relação aos seus concorrentes, em relação a vários parâmetros de desempenho com base na categoria de excelência em tecnologia e impacto no cliente.

Preparação do relatório final

Após a finalização das análises e previsões de mercado, nosso analista prepara os gráficos, quadros e tabelas necessários para obter mais percepções e preparar o relatório final de pesquisa. Nosso relatório final de pesquisa conta com informações, incluindo previsões de mercado; analise competitiva; principais tendências de mercado e tecnologia; impulsionadores de mercado; perfis de fornecedores e outros.