SailPoint

Sexta edição

O guia definitivo para segurança de identidade unificada

Como elevar sua segurança com forte segurança de identidade – não importa seu ponto de partida

Sumário

Segurança de identidade—o núcleo de suas operações de negócios 3

A necessidade de desenvolver um programa de segurança de identidade de longo prazo e sustentável 4

Identificar prioridades de negócios e estabelecer metas de negócios claras 6

1. Acelerar a concessão de acesso a usuários empresariais e liberar o pessoal de TI 7
2. Aumentar a produtividade dos usuários – não importando quem são, o que são ou onde estão 8
3. Reduzir custos, complexidade e erros humanos com a automatização de processos de identidade 9
4. Centralizar controles de acesso e políticas em toda a organização 10
5. Gerenciar o acesso tanto em aplicativos locais como na nuvem 11
6. Eliminar deficiências de auditoria e melhorar o desempenho das auditorias 12
7. Reduzir o custo da conformidade 13
8. Substituir um sistema de provisionamento já existente 14

Escolher um caminho de segurança de identidade com o melhor retorno 15

- Ponto de partida: acesso do usuário 16
- Ponto de partida: conformidade 17
- Ponto de partida: mitigação do risco cibernético 18
- Ponto de partida: governança de dados 19

O panorama geral: o que é necessário para alcançar seus objetivos de melhoria da segurança de identidade? 20

Enquadrar o panorama geral: garantir que seu programa de segurança de identidade seja bem-sucedido 22

Em que fase você está na sua jornada de segurança de identidade? 24

A SailPoint é o núcleo da segurança de identidade para a empresa moderna 26

- SailPoint Identity Security Cloud Business 27
- SailPoint Identity Security Cloud Business Plus 28
- Outras soluções de segurança de identidade da SailPoint 28

Primeiros passos 29

Segurança de identidade—o núcleo de suas operações de negócios

Os líderes empresariais de todos os setores estão reconhecendo que, atualmente, gerenciar identidades digitais e seus acessos em toda a organização é essencial para proteger a empresa e fornecer a agilidade de que ela precisa para obter todo o seu potencial. O gerenciamento eficaz de identidades é fundamental para permitir uma colaboração perfeita com parceiros de negócios, simplificar a eficiência operacional, cumprir os as regulamentações de conformidade, de segurança cibernética e privacidade cada vez mais numerosos, reduzir os riscos e recuperar-se de ataques cibernéticos.

A segurança de identidade (também conhecida como governança e administração de identidades de identidade e gerenciamento de identidade) protege as organizações descobrindo, gerenciando e protegendo o acesso à tecnologia para uma força de trabalho diversificada de identidades digitais. As identidades digitais incluem seres humanos - funcionários, terceiros, clientes, parceiros de negócios etc. - além de máquinas como RPAs (Robotic Process Automation, também conhecido como bots) ou dispositivos de OT/IoT.

Essas identidades se conectam a bilhões (sem "a mais de") de pontos de acesso de tecnologia, todos com diferentes níveis de requisitos de acesso que evoluem à medida que as necessidades dos negócios mudam. A segurança de identidade garante que cada identidade tenha o acesso necessário para fazer o seu trabalho – nem mais, nem menos. Com o acesso certo, a identidade pode continuar sua jornada digital com permissão para acessar dados, aplicativos, sistemas, plataformas de nuvem e outros recursos.

A segurança da identidade enfatiza a capacitação, a segurança e a conformidade, o que significa não apenas fornecer acesso, mas também controlar adequadamente esse acesso.

Este guia foi desenvolvido para ajudá-lo a entender o que procurar em uma solução que possa levar sua organização a um programa de segurança de identidade mais maduro. Você encontrará ajuda para definir as principais metas de negócios específicas que precisam ser alcançadas alcançar, entender quais são as perguntas certas que devem ser feitas e identificar os caminhos que lhe permitem obter vitórias rápidas na evolução de seu programa de segurança de identidade.

Você descobrirá o que é necessário hoje para que uma solução alcance as metas definidas, bem como o que procurar em um fornecedor que maximize seu sucesso. Por fim, encerramos com uma rápida introdução às soluções de segurança de identidade da SailPoint.

Esperamos que a leitura deste guia seja uma etapa útil em sua jornada para um programa de segurança de identidade bem-sucedido e preparado para o futuro. Entre em contato conosco ou acesse **www.sailpoint.com** quando desejar avançar.

A necessidade de desenvolver um programa de segurança de identidade de longo prazo e sustentável

Ter um programa de segurança de identidade robusto e moderno tem um impacto real em quase todos os vetores de ameaças em sua empresa, porque ele se integra com todas as suas aplicações de negócios, infraestrutura e dados críticos, o que o torna relevante para todas as partes interessadas que você precisa abordar para obter adesão.

As mudanças que afetam a segurança de uma organização chegam a todos nós. Os limites de uma empresa globalmente conectada hoje se estendem muito além do datacenter. A mudança para o trabalho remoto em qualquer lugar e serviços baseados em nuvem significam que operações de negócios mais críticas estão sendo executadas fora da rede corporativa. A proliferação de dispositivos móveis permite o acesso a qualquer hora/em qualquer lugar, e os parceiros de negócios e clientes esperam acesso sob demanda a aplicativos e dados corporativos. À medida que o perímetro de segurança da empresa evolui, as identidades são o novo firewall corporativo.

Além disso, as organizações enfrentam um risco maior à medida que os cibercriminosos têm mais oportunidades do que nunca de se infiltrar nas suas atividades. Vimos uma explosão tanto nas ameaças cibernéticas — inclusive ataques à cadeia de suprimentos de software, ransomware, ameaças persistentes avançadas — quanto nas regulamentações internacionais, federais, estaduais, locais e específicas do setor, que estão em constante mudança.

Um programa de segurança de identidade deve atender às necessidades imediatas e táticas da organização e, ao mesmo tempo, deve ser sustentável como parte de uma estratégia de melhoria de negócios em longo prazo. A segurança de identidade é essencial para gerenciar o acesso do usuário a aplicativos, sistemas, dados e ambientes de nuvem, sem comprometer a agilidade dos negócios, inibir a produtividade dos trabalhadores ou violar os regulamentos de conformidade.

Aqui estão algumas das perguntas que ajudarão todos os responsáveis pela segurança de identidade — desde a equipe de liderança sênior até aqueles que trabalham diretamente na segurança ou na segurança de suporte de TI — a determinar o quanto seu programa de segurança de identidade atual atende aos desafios enfrentados por sua empresa, incluindo os **quatro vetores de maturidade** de identidade de estratégia, modelo operacional, tecnologia/ferramentas e talento.

- **Nosso programa de segurança de identidade se alinha à estratégia** geral de negócios de modo que seja compreendido e utilizado em toda a organização?
- **Temos uma equipe dedicada para gerenciar** de forma centralizada nossa infraestrutura e operações de identidade?
- **Nosso modelo nos permite gerenciar de forma centralizada o acesso** de nossas identidades ou o gerenciamento é feito em silos, ou talvez não haja gerenciamento?
- **Estamos confiantes de que temos uma visão abrangente de todos os acessos das identidades** (funcionários, não funcionários e máquinas) em todos as aplicações aplicativos, sistemas, ambiente de nuvem e dados?
- **Já eliminamos atrasos e custos desnecessários da maneira como gerenciamos** atualmente a segurança de identidades e direitos de acesso por meio da automação para ajustar o acesso à medida que os usuários ingressam, mudam de função, assumem novos projetos ou deixam a organização?
- **Temos a tecnologia certa necessária** para ajudar a diminuir o risco representado por ações humanas, como phishing, malware, acesso de funcionários a informações confidenciais e vazamentos de dados internos?
- **Estamos satisfeitos com nossos recursos atuais para conectar e integrar** nosso crescente conjunto de soluções de nuvem e SaaS para obter a máxima segurança?
- **Temos certeza de que minimizamos o erro e o risco na maneira como gerenciamos identidades** e direitos de acesso — coisas que podem expor a organização a riscos comerciais, de marca e financeiros?
- **Alcançamos o equilíbrio ideal entre conceder** aos trabalhadores acesso que maximize sua produtividade e minimize riscos como acesso superprivilegiado, conflitante ou comprometido?
- **Estamos aplicando um modelo adequado de acesso menos privilegiado** para que as pessoas tenham apenas o acesso de que precisam para realizar seu trabalho no momento em que precisam, reduzindo a exposição de dados confidenciais e o impacto de um ataque cibernético?
- **Estamos confiantes de que estamos cumprindo todos os requisitos de regulamentação** e fornecendo prova de conformidade?
- **Podemos satisfazer os requisitos da nossa apólice de seguro de segurança cibernética** e estamos confiantes de que estaremos cobertos em caso de violação?

Identificar prioridades de negócios e estabelecer metas de negócios claras

Como você já descobriu, a segurança de identidade é um imperativo estratégico para organizações de todos os tamanhos. Desde as grandes empresas multinacionais a empresas de médio porte, assim como empresas menores e de rápido crescimento devem atender aos requisitos para proteger e governar o acesso a aplicações, sistemas e dados críticos, seja na nuvem ou localmente.

A segurança de identidade desempenha um papel crítico em permitir que as organizações cataloguem, analisem e compreendam os privilégios de acesso concedidos a todas as identidades associadas a funcionários, terceirizados, fornecedores, contas de serviço e até mesmo bots de software, para responder à pergunta crítica: "Quem tem acesso a quais dados?"

Ao mesmo tempo, a empresa ágil de hoje exige níveis mais rápidos e mais altos de prestação de serviços em um ambiente cada vez mais diversificado e dinâmico:

- A cada dia são integrados novos usuários, o que exige acesso imediato aos recursos da empresa.
- As funções e responsabilidades dos usuários mudam, ou seus relacionamentos com a empresa terminam, e o acesso deve ser rapidamente modificado ou revogado.
- Algumas aplicações e usuários representam um nível mais alto de risco para a organização do que outros e exigem um foco maioro.

O desafio passa a ser como atender às demandas de nível de serviço e, ao mesmo tempo, identificar e gerenciar atividades de alto risco, aplicar políticas e segurança, manter controles rigorosos e atender aos requisitos de conformidade.

Como existem muitos fatores de negócios diferentes que exigem a segurança de identidade, você pode se perguntar como e quando implementar os diferentes componentes de uma solução.

Como você identifica resultados com bom retorno do investimento? A resposta depende das prioridades do seu negócio e dos desafios imediatos que sua organização enfrenta.

Para começar, reflita e avalie seus problemas mais urgentes. Você entende o que deseja que sua solução o ajude a alcançar?

Aqui estão alguns objetivos de negócios comuns que podem ajudá-lo a determinar suas próprias prioridades exclusivas:

1. Acelerar a concessão de acesso a usuários corporativos e liberar o pessoal de TI
2. Aumentar a produtividade dos usuários – não importando quem são, o que são ou onde estão
3. Reduzir custos, complexidade e erros humanos com a automatização de processos de identidade
4. Centralizar controles de acesso e políticas em toda a organização
5. Gerenciar o acesso com alto nível de granularidade em aplicações de forma local e na nuvem
6. Eliminar deficiências de auditoria e melhorar o desempenho das auditorias
7. Reduzir o custo da conformidade
8. Substituir um sistema de provisionamento já existente

Vamos analisar mais detalhadamente cada um desses fatores de negócios para a segurança de identidade — as metas que as organizações esperam alcançar com mais frequência com sua implementação.

1 Acelerar a concessão de acesso a usuários corporativos e liberar o pessoal de TI

Em uma empresa de médio porte, o processo de fornecer às pessoas o acesso certo para realizar seu trabalho ainda é algo que requer muitas etapas manuais e o envolvimento da TI. Por causa do ambiente acelerado e dinâmico dos negócios hoje em dia, as empresas estão concedendo mais acessos do que as pessoas precisam, o que compromete sua segurança e dificulta os esforços de conformidade. Os usuários corporativos não podem esperar dias ou semanas para acessar os sistemas necessários para desempenhar suas funções de trabalho. A integração de novos usuários precisa acontecer logo no primeiro dia. Da mesma forma, as organizações não podem tolerar grandes intervalos no desprovisionamento dos acessos quando um usuário muda de cargo ou sai da organização.

As alterações no acesso do usuário devem ser realizadas quase que em tempo real, com intervenção mínima de TI, sem deixar de ser um processo controlado e auditável que seja visível para os negócios. O estado atual da segurança de identidade na maioria das organizações torna quase impossível fornecer níveis de serviço uniformes e eficazes para a empresa em virtude dos seguintes desafios:

- Uso intenso de processos diferentes de solicitação e alteração de acesso manual
- Falta de participação do usuário final e visibilidade dos processos de gerenciamento de identidade
- Métodos ad hoc para lidar com identidades externas e seus direitos de acesso
- O número crescente de aplicações baseados em nuvem que são gerenciados fora da TI
- Equipe de helpdesk sobrecarregada com solicitações de acesso e redefinições de senha

O que as organizações precisam é de uma maneira mais fácil e econômica de fornecer o acesso certo aos usuários certos e, ao mesmo tempo, oferecer uma segurança de identidade bem estruturada para os negócios. Com as ferramentas de autoatendimento corretas, os usuários corporativos podem gerenciar seu próprio acesso, desde a solicitação de novos acessos ou funções até a recuperação de senhas esquecidas por meio de interfaces intuitivas e favoráveis para o uso corporativo. Além disso, as soluções atuais de provisionamento de usuários oferecem opções de fácil configuração para automatizar todo o ciclo de vida de acesso de um usuário com base em informações de fontes autoritativas, como seus sistemas de Recursos Humanos e mudanças de funções. Minimizar a necessidade de mudanças manuais libera a equipe de TI para um trabalho mais estratégico.

Com o fornecimento de uma abordagem integrada que aproveita ferramentas de solicitação de acesso de autoatendimento favoráveis aos negócios e mudanças automatizadas no ciclo de vida, as soluções de segurança de identidade que têm como núcleo a inteligência e automação podem agilizar a concessão de acesso ao usuário em toda a sua organização, sem deixar de aplicar continuamente o privilégio mínimo, regras de governança e políticas de conformidade. Os usuários coporativos tornam-se participantes ativos no processo, gerenciando seu próprio acesso e senhas, monitorando o status das suas solicitações e modelando o seu acesso conforme a necessidade em um ambiente corporativo ágil. Tudo isso sem provocar atrasos na TI nem frustrar esses processos, resultando em uma carga de trabalho significativamente menor das equipes de helpdesk e operações de TI.

2 Aumento da produtividade dos usuários - não importando quem são, o que são ou onde estão

Quer você esteja gerenciando as identidades de usuários internos (funcionários, contratados e bots) ou externos (parceiros da cadeia de suprimentos, agentes, voluntários), o que você deseja é implementar tecnologias que reduzam o ônus de conceder o acesso certo aos dados certos para todos os tipos de usuários. Ter a estratégia certa de segurança de identidade não só reduz os custos internos e melhora a produtividade, mas também pode contribuir para o crescimento da receita e a lucratividade.

Os trabalhadores de hoje querem acesso a qualquer hora, em qualquer lugar, por meio de qualquer dispositivo. Cada minuto que um usuário tem que gastar esperando que o acesso seja concedido ou alterado, recuperando uma senha perdida ou fazendo com que o helpdesk redefina uma senha é um minuto improdutivo — e quando você multiplica o número crescente de aplicações pela quantidade de tempo desperdiçado, o alto preço do inconveniente se torna bastante visível.

Aqui estão algumas perguntas que você deve levar em consideração ao planejar sua estratégia para garantir que sua solução de segurança de identidade ofereça conveniência e melhore a adoção e a produtividade do usuário:

- **Você simplifica ao máximo o acesso de novos usuários** aos seus sistemas de negócios — mesmo que eles não tenham nenhum relacionamento prévio com sua organização?
- **Você é capaz de fornecer acesso rápido** e seguro a toda a gama de aplicações, sistemas e dados de que cada indivíduo precisa em sua função específica?
- **Você está fornecendo aos seus usuários recursos avançados de autoatendimento** que proporcionam à empresa a flexibilidade e a segurança de que eles precisam?

3 Reduzir custos, complexidade e erros humanos com a automatização de processos de identidade

Gerenciar os relacionamentos complexos entre milhares de usuários e milhões de privilégios de acesso continua a ser uma tarefa assustadora e cara para a maioria das organizações. Para muitos, as mudanças no acesso do usuário são iniciadas, aprovadas e implementadas por meio de processos fragmentados e desarticulados. Soma-se a isso o fato de que, na maioria das organizações, os processos e ferramentas usados para solicitar ou alterar o acesso do usuário são, em grande parte, manuais. O resultado é uma execução ineficiente, propensa a erros e dispendiosa de solicitações e alterações de acesso. A realidade é que isso foi muito além da capacidade humana e está exigindo muito da equipe de TI.

Sua organização enfrenta os seguintes problemas ao cumprir as alterações de acesso nos sistemas de TI corporativos?

- **Vários processos de front-end** são usados pela empresa para solicitar novos privilégios de acesso ou alterar aqueles já existentes
- **São necessários processos manuais** para executar as mudanças no acesso do usuário
- **Grande dependência de helpdesk ou administradores de TI** para avaliar e implementar alterações de acesso
- **São usados processos diferentes de provisionamento/desprovisionamento** para aplicações diferentes

Se essas situações soam familiares, é hora de adotar uma nova abordagem. Você precisa centralizar a concessão de acesso em diferentes recursos de TI que abrangem o datacenter e a nuvem e reduzir os custos associados ao gerenciamento da iniciação e atendimento de solicitações e alterações de acesso. A solução de segurança de identidade certa automatiza eventos do ciclo de vida da identidade, como a integração de novas contratações e o gerenciamento de transferências de trabalho, atribuindo ou alterando diretamente funções e direitos para corresponder à função de trabalho atual de um usuário. Também automatiza o processo de desligamento para remover os privilégios de acesso após a rescisão. Com a automatização desses eventos, as organizações podem efetivamente descobrir, gerenciar e proteger o acesso do usuário em escala, e reduzir o número de solicitações de autoatendimento iniciadas por usuários corporativos, o número de aprovações necessárias para conceder acesso e o número de chamadas para o helpdesk para concretizar essas alterações. A automação não apenas libera a equipe de TI, mas também pode ajudar a minimizar significativamente o risco decorrente do acesso excessivo do usuário e dos processos de provisionamento manuais e propensos a erros.

4 Centralizar controles de acesso e políticas em toda a Organização

A empresa moderna é um ecossistema digital com fluxos de trabalho impulsionados por diversas aplicações e armazenamentos de dados usados por funcionários e terceiros com diferentes direitos de acesso.

É preciso que esse complexo ecossistema promova maior produtividade com conectividade facilitada entre todos esses elementos, mas sem que haja o risco de comprometer a segurança de aplicações críticas para a empresa e dados confidenciais. Quando o gerenciamento de segurança de identidade é altamente fragmentado, o risco de erro e abuso aumenta.

As decisões sobre quem tem qual nível de acesso em diferentes aplicações usadas pela organização se tornam complicadas quando vinculadas a funções que podem mudar com frequência e exigem para acertar. Para algumas organizações, fornecer esse contex.to requer integrações e desenvolvimento customizados demorados e caros sempre que são integrados customizados. E depois testar novamente sempre que as aplicações forem atualizadas

Aqui estão algumas perguntas que você deve levar em consideração ao planejar sua estratégia para garantir que sua solução de segurança de identidade reduza o esforço e o custo de controlar o acesso em toda a sua organização:

- **Como a solução permite que você gerencie e controle melhor e de forma centralizada todos os tipos de acesso e identidade** em toda a organização de acordo com suas políticas?
- **A solução pode incorporar novos direitos de acesso ao modelo** existente para manter as funções atualizadas?
- Até que ponto isso permite **centralizar controles de acesso e políticas?**
- **Como a solução torna mais fácil incorporar a funcionalidade de identidade nas aplicações** em que os usuários confiam todos os dias, mesmo quando mudam de função?
- **Como a solução reduz o esforço necessário para garantir que novas aplicações forneçam o acesso certo** às pessoas certas para que você comece a perceber o valor agregado dessas aplicações o mais rápido possível?

No centro de um programa robusto está uma solução de segurança de identidade com políticas e controles centralizados que fornecem visibilidade de 360 graus para “quem tem acesso a quê” para todos os recursos — em todo o seu ecossistema digital. Isso ajuda a proteger a empresa como um todo, colocando a responsabilidade e o controle no seu devido lugar.

5 Gerenciar o acesso tanto em aplicações locais como na nuvem

Embora muitas empresas não tenham mais data centers locais, elas normalmente têm aplicações legadas que simplesmente migraram para a nuvem, substituindo um ambiente de virtualização por outro. O fato de um sistema legado ser hospedado na nuvem não o torna um aplicativo moderno; os mesmos requisitos ainda se aplicam ao gerenciamento de acesso e governança.

Somando-se à complexidade desse ambiente, as unidades de negócios estão ganhando mais autonomia para comprar e implantar aplicações — que muitas vezes podem abrigar dados corporativos confidenciais — sem consultar ou envolver a organização de TI.

Aqui estão alguns dos sinais de que sua organização pode ter dificuldade para gerenciar novas aplicações em nuvem:

- **A TI não está totalmente ciente das aplicações de nuvem de missão crítica** em produção em vários departamentos e unidades de negócios.
- **As unidades de negócios realizam sua própria administração de usuários** por meio de planilhas e atualizações manuais.
- **As unidades de negócios solicitam que a TI integre aplicações em nuvem** com diretórios para sincronização periódica.
- **As unidades de negócios compram suas próprias soluções de gerenciamento de identidade e acesso** — sem consultar a TI ou considerar qual infraestrutura de segurança de identidade já está em uso.
- Os processos de auditoria de TI, como as certificações de acesso, **não foram estendidos para abranger aplicações em nuvem.**

Uma solução de segurança de identidade robusta e moderna deve ajudar as empresas a adotarem a nuvem e, ao mesmo tempo, permitir que a organização de TI aplique efetivamente políticas de segurança de identidade centralizadas, detecte violações e demonstre total conformidade regulamentar. As soluções de segurança de identidade bem-sucedidas permitirão que você automatize os processos de conformidade e provisionamento para aplicações em nuvem da mesma maneira que os aplicativos locais.

6 Eliminar deficiências de auditoria e melhorar o desempenho das auditorias

A segurança da identidade é um ponto focal para auditorias de TI e uma das áreas mais comumente evidenciadas por conta de seus controles ineficazes. Durante muitas auditorias, os controles de identidade fracos frequentemente são detectados como pontos negativos na forma de deficiências de controle ou fraquezas materiais. E as auditorias são mais numerosas, com mais regulamentações que afetam as empresas do que já houve anteriormente. Sarbanes-Oxley (SOX), GDPR, HIPAA, CCPA e LGPD são apenas algumas das muitas estruturas regulatórias existentes.

Aqui estão alguns dos riscos de identidade mais comuns que atraem a atenção dos auditores:

- **Contas órfãs:** acesso que permanece ativo para funcionários ou terceirizados após a rescisão devido à não remoção de privilégios.
- **Abuso dos diretos:** o acúmulo de privilégios ao longo do tempo por meio de transferências, promoções ou outras mudanças de funções, resultando em funcionários com acesso além do que é necessário para o seu trabalho.
- **Violações de segregação de funções/ Segregation of Duty (SoD):** acesso inadequado que resulta em controle excessivo sobre as transações corporativas ou a capacidade de executar tarefas conflitantes (como contas a pagar e contas a receber).
- **Contas de usuário privilegiadas mal gerenciadas:** as contas compartilhadas que normalmente são do domínio de usuários privilegiados são gerenciadas por meio de processos manuais e são muito difíceis de auditar.
- **Falta de visibilidade do acesso por função de trabalho:** os usuários corporativos têm dificuldade em interpretar dados técnicos de TI para tomar decisões de negócios sobre qual acesso é necessário para desempenhar uma função de trabalho específica.

Há outro risco de identidade comum que surge várias vezes durante o ano. Os gerentes de negócios obtêm uma lista de direitos para revisar e certificar para sua equipe. Sem contexto, e para agilizar o processo, muitos deles aprovam tudo mecanicamente, temendo que possam revogar acidentalmente o acesso necessário para seus funcionários. Com isso, ocorre o provisionamento excessivo, aumentando a superfície de ataque potencial. O risco de não conformidade também aumenta.

Se você foi malsucedido em uma auditoria devido à fraqueza em torno de qualquer um desses riscos de identidade, temos boas notícias. A solução de segurança de identidade certa melhorará sua visibilidade em áreas de riscos ou não conformes e automatizará seus processos para gerenciar esses riscos. Uma visão de toda a empresa de seus dados de identidade e recomendações de acesso habilitadas por IA pode ajudá-lo a analisar riscos de forma eficaz, tomar decisões de acesso mais fundamentadas e implementar os controles adequados de maneira automatizada e mais sustentável.

Além disso, o alinhamento do acesso do usuário com as funções de trabalho por meio da modelagem de funções fortalece os controles de acesso do usuário pelo fornecimento de um contexto de negócios valioso relativo ao modo pelo qual conjuntos específicos de acesso se relacionam à função de negócios subjacente executados por uma pessoa. As funções reduzem significativamente o número de direitos de acesso individuais que devem ser revisados e destacam o acesso concedido em um grau excessivo (exceções). Isso leva à maior precisão e a melhores decisões, resultando em menos possibilidade de resultados negativos de auditoria ou de ser malsucedido em mais uma auditoria. Também é um requisito importante que evidencia os benefícios da automação.

7 Reduzir o custo da conformidade

A conformidade pode ser complexa e difícil — e, portanto, dispendiosa. Cumprir as obrigações regulatórias e setoriais exige que as organizações revisem e certifiquem regularmente os privilégios de acesso dos usuários. Isso faz com que muitas empresas tenham constantemente dificuldades com processos propensos a erros e ineficientes, como a geração manual de relatórios de acesso e correção manual dos direitos de acesso inadequados do usuário.

Aqui estão alguns sinais que mostram que você precisa simplificar os processos de conformidade e reduzir os custos de conformidade:

- **Criar ou aproveitar várias soluções** locais para lidar com as necessidades de auditoria e conformidade
- **Contratação de funcionários ou consultores em tempo integra**l para lidar com projetos de conformidade, como certificações de acesso e aplicação de políticas de SoD
- **Exigir que os proprietários de aplicações exportem manualmente** e, em seguida, formatem os dados para a próxima auditoria
- **Usar ferramentas ineficientes, como planilhas e e-mail**, para executar os processos manuais de conformidade
- **Tratar os usuários de alto e baixo risco da mesma forma**, dando atenção insuficiente aos usuários de alto risco, ou gastando muito tempo e esforço com usuários de baixo risco

Para obter um melhor controle dos seus dados de identidade, será necessário substituir processos manuais dispendiosos baseados em papel por políticas definidas de modo centralizado e processos de certificação de acesso automatizados.

Agindo assim, você não apenas pode reduzir significativamente o custo da conformidade, mas também pode estabelecer práticas que podem ser repetidas para um esforço de certificação de acesso mais uniforme, auditável, confiável, eficiente e de fácil gerenciamento.

Se você sente dificuldade para implementar efetivamente os processos de conformidade e integrá-los em seus sistemas e infraestrutura, uma solução moderna de segurança de identidade é o ponto de partida de que você precisa para melhorar sua eficácia e reduzir os custos de conformidade sustentável e contínua.

8 Substituir um sistema de provisionamento já existente

Muitas organizações têm uma ou mais soluções legadas de provisionamento de usuários que não atendem mais às suas necessidades, não fazem o que o fornecedor prometeu que faria ou, o que é mais grave, já não têm mais suporte ou deixarão de ter no futuro.

Você está enfrentando algum dos seguintes problemas com sua solução de provisionamento existente?

- Seu projeto está atrasado e acima do orçamento.
- Você não tem a cobertura necessária para integração com aplicações.
- Você gasta muito tempo e esforço criando e mantendo conectores "customizados".
- Você gasta mais tempo gerenciando e mantendo o ambiente do que usando de fato a solução.
- Atualizações e upgrades são caros e demorados, especialmente se a solução tiver sido personalizada.
- Seu produto de provisionamento está sendo "aposentado" e deve ser substituído.
- Você tem pontos fracos de conformidade relacionados a processos de desligamento ineficazes, aumento de direitos, violações de SoD e outras coisas.

Agora é a hora de resolver esses problemas e migrar para longe de sua plataforma de provisionamento herdada. Invista em uma tecnologia que atenda aos seus desafios atuais e futuros de provisionamento, melhore sua estratégia geral de segurança de identidade, integre-se a todos os sistemas com os quais você precisa se integrar e nunca exija que você realize outro upgrade. Procure uma solução que proporcione à sua organização uma transição suave e permita que você adote uma abordagem não disruptiva e escalonada, aproveitando ao máximo seu investimento existente à medida que você faz a transição para uma solução de próxima geração.

A nova solução também deve ser capaz de equilibrar os principais requisitos de provisionamento do usuário — adicionar, alterar, excluir contas de usuário e gerenciamento de senhas — com interfaces e processos fáceis de usar que capacitem os usuários de negócios a solicitar e gerenciar o acesso como preferirem. Uma solução que aproveita a IA para automatizar esses processos é ideal não apenas para melhorar a eficiência da TI, mas também para minimizar significativamente os riscos.

E, por fim, o que é mais importante: deve oferecer uma abordagem integrada para a segurança da identidade. A governança e a conformidade devem ser tratadas como uma atividade integrada em sua infraestrutura de identidade, não como processos separados.

Escolher um caminho de segurança de identidade com o melhor retorno

Agora que você identificou suas metas de negócios para melhorar a segurança de identidade, pense sobre as etapas necessárias para alcançá-las. Você tem vários caminhos para escolher e pode priorizá-los com base nos requisitos e objetivos de negócios exclusivos da sua organização. Nesta seção, descrevemos como maximizar seu sucesso no menor tempo possível para obter vitórias rápidas, ao mesmo tempo em que estabelece uma base sólida para um programa de segurança de identidade preparado para o futuro.

Encontre o seu ponto de partida

Depois de estabelecer suas principais prioridades e metas, você terá uma melhor compreensão do que deve alcançar primeiro. Concentrando-se em algumas oportunidades de "vitória rápida", você pode acelerar e criar impulso para as fases futuras de seus projetos.

Uma abordagem adicional para a implementação do projeto ajuda você a se concentrar, garantindo que você lide com aplicações de alta prioridade e grupos de usuários que são mais afetados por seus objetivos declarados. Demonstrando pequenas e rápidas vitórias logo no começo, você cria confiança na solução, ajuda a garantir a adoção contínua e facilita a obtenção de financiamento para mais projetos.

Ponto de partida: acesso do usuário

Se sua organização está tendo dificuldades com processos ineficientes e/ou não compatíveis para conceder novos privilégios de acesso ou fazer alterações nos privilégios de acesso existentes para funcionários e não funcionários, incluindo terceirizados, temporários e parceiros, pode ser mais proveitoso concentrar-se em automatizar a integração, o desligamento e as mudanças intermediárias.

Veja como começar:

1 Ativar solicitação de acesso de autoatendimento

Uma das melhores maneiras de começar a melhorar o acesso do usuário é se concentrar primeiro nos usuários corporativos. Capacitar os usuários de negócios para que encontrem e solicitem acesso sem a assistência do helpdesk ou dos administradores de TI pode evitar dores de cabeça e poupar dinheiro ao mesmo tempo.

2 Automatizar o processamento de acesso

Outra vitória rápida é automatizar o atendimento de solicitações de acesso com recomendações baseadas em IA. Você pode maximizar a economia de custos gerada concentrando-se inicialmente em algumas aplicações de alta rotatividade, em que as contas de usuário são criadas, atualizadas ou excluídas regularmente, e depois estender a todas as aplicações a partir daquele ponto.

3 Automatizar a atribuição de acesso

O maior retorno sobre o investimento é obtido com a automatização da atribuição de acesso. Esse processo pode aproveitar os dados de identidade de seus sistemas de RH ou outras fontes autoritativas para automatizar completamente a atribuição de acesso para identidades humanas e não humanas.

4 Simplificar o gerenciamento de senhas

O gerenciamento de senhas fornece um caminho rápido para o sucesso do seu projeto de segurança de identidade porque permite que os usuários finais redefinam senhas esquecidas e ignorem o helpdesk. Usando a mesma interface de usuário corporativo fácil de usar, os usuários podem alterar ou redefinir senhas nos sistemas de destino.

Ponto de partida: conformidade

Se as deficiências de auditoria e o alto custo da conformidade forem os principais problemas em sua organização, é aconselhável concentrar-se na automação de conformidade inicialmente. Você já pode estar no processo de estabelecer um "modelo de acesso com o menor privilégio", conforme exigido por muitas estruturas regulatórias, além de ser um elemento-chave para aplicar uma abordagem de Zero Trust à segurança de identidade. Com o menor privilégio, você garante que as pessoas tenham apenas o acesso de que precisam para realizar sua função de trabalho de modo que, se uma identidade ou uma conta for violada, a exposição dessa violação seja limitada ao acesso que a pessoa deveria ter, em vez de acesso superprivilegiado que os usuários frequentemente têm, o que poderia levar a multas mais altas e mais exposição.

Veja como começar:

1 Ganhar visibilidade centralizada

O ponto de partida para qualquer projeto de conformidade deve ser a compreensão do estado atual dos usuários obtida por meio de uma visão central do acesso à identidade em toda a organização. Esta etapa envolve a criação de um único repositório para informações de usuário e acesso, integrando e agregando dados de suas fontes autorizadas, como sistemas de RH e bancos de dados de contratados, além de recursos de destino.

2 Identificar e fechar todas as contas órfãs

Encontrar e eliminar contas órfãs é uma das medidas de mitigação de risco mais eficazes que você pode adotar no seu projeto de conformidade. Depois de identificar essas contas de alto risco, você pode iniciar ações de correção para todas as contas sem dono — remover, marcar como serviço ou, quando possível, correlacionar a identidades conhecidas.

3 Detectar e solucionar comportamentos atípicos

O próximo passo no processo de limpeza de dados é identificar comportamentos atípicos: usuários que têm acesso significativamente diferente do que pode ser esperado. À medida que você criar o caso de negócios para seu programa de segurança de identidade, procure uma solução com IA que possa identificar usuários de risco e comportamentos atípicos de acesso e fortalecer significativamente a segurança com a detecção e correção de vulnerabilidades.

4 Automatizar as certificações de acesso

Em seguida, gere uma campanha de certificação que possa ajudar a automatizar as avaliações de acesso para todos os usuários. Hoje, sua equipe pode ser auxiliada por recomendações orientadas por IA, que simplificam e encurtam o ciclo de revisão da certificação. Sua equipe terá facilidade em decidir se é seguro aprovar ou negar o acesso. As certificações iniciais devem ser usadas para estabelecer uma base de referência de dados confiável.

Ponto de partida: mitigação do risco cibernético

À medida que os ambientes de trabalho se tornam mais complexos e continuam migrando para a nuvem, os invasores estão cada vez mais utilizando a identidade como um vetor. As violações de dados representam um sério risco para a empresa, com consequências que vão desde perdas financeiras até danos à reputação e tempo de inatividade. Se você sofreu recentemente uma violação, sabe em primeira mão que é preciso apenas uma identidade comprometida para potencialmente custar a uma empresa dezenas (até centenas) de milhões de dólares em perda de receita e multas regulatórias.

Adotar uma abordagem manual em silos para gerenciar e governar o acesso é a maior ameaça aos sistemas de negócios híbridos e de várias aplicações da sua empresa. Deixar de unificar os controles de segurança de identidade e o monitoramento de SoD no SAP ERP, S/4HANA e outras aplicações em seu ecossistema de negócios pode resultar em fraudes dispendiosas e prejudiciais, violações de dados e deficiências de auditoria. É por isso que as organizações devem implementar estratégias adequadas de mitigação de riscos cibernéticos para se proteger desse tipo de evento.

Veja como começar:

1. **Fique à frente dos riscos**, identificando violações de SoD e riscos de acesso confidenciais em todos os sistemas ERP. Procure riscos contínuos por usuário, função e processos de negócios. As soluções de segurança de identidade automatizadas e baseadas em IA podem fornecer a visibilidade e as informações acionáveis necessárias para obter visibilidade e análise profundas do histórico de acesso de um usuário.

2. **Aproveite a IA** para ajudá-lo a detectar e evitar combinações de acesso nocivas que podem levar a fraudes ou roubo de dados. A IA facilita a identificação de riscos em escala e o monitoramento de comportamentos, ajudando você a construir uma organização mais resistente.

3. **A IA também pode ajudar a identificar e prevenir o risco** de acesso antes do provisionamento e ter a inteligência necessária para executar análises de sensibilidade (cenários “What If”). Implemente um processo para elevar ou conceder acesso de emergência com controles automatizados e revisões simplificadas.

4. **Automatize fluxos de trabalho para administradores e revisores** para garantir ciclos de revisão de acesso periódico. Mantenha toda a sua equipe — TI, auditoria, conformidade, proprietários de empresas de segurança e membros do conselho — continuamente informada sobre ameaças com relatórios.

5. Em longo prazo, **torne a mitigação de riscos cibernéticos uma parte do projeto de segurança**, implementações e atividades de remediação.

Ponto de partida: governança de dados

Agora, a maioria dos dados corporativos armazenados em serviços de compartilhamento de arquivos baseados em nuvem, como Box, SharePoint e Google Drive, está sujeita mais do que nunca a ataques em número crescente, incluindo ameaças internas. Se sua organização tem dificuldade em entender quais dados confidenciais e dados de PII são armazenados em arquivos de seus sistemas de arquivos (por exemplo, dentro de pastas do Microsoft Teams ou Box e sites do SharePoint), faz sentido começar com a Governança de Dados.

Veja como começar:

1. **É necessário que você saiba onde seus arquivos confidenciais estão armazenados**, incluindo relatórios fora do seu sistema financeiro e propriedade intelectual. Se o seu departamento de marketing já exportou quantidades significativas de detalhes de contato do cliente para uma campanha, você sabe se depois disso esses dados foram tratados adequadamente?

2. **Atualize seus conhecimentos sobre quem tem direitos de acesso** a dados não estruturados, regulamentados e confidenciais. É necessário ter a capacidade de monitorar, controlar e certificar quem tem acesso a esses dados e entender por que isso ocorre.

3. Conforme mencionado na seção sobre conformidade, **intensifique os controles de acesso**: remova o acesso superprivilegiado ou não utilizado, monitore atividades maliciosas e adote medidas corretivas automaticamente em tempo real. Certifique o acesso aos dados para atender aos requisitos de conformidade e auditoria.

O panorama geral: o que é necessário para alcançar seus objetivos de melhoria da segurança de identidade?

Antes de começar a avaliar os detalhes de soluções individuais de segurança de identidade, você pode tornar sua jornada de compra um pouco mais tranquila se compreender o "panorama geral" do que é necessário para alcançar seus objetivos estratégicos de negócios. Existem três áreas principais de capacidade que são o requisito mínimo para as principais soluções de segurança de identidade hoje.

Primeiro, essas soluções devem ajudá-lo a alcançar um nível muito mais profundo de visibilidade e inteligência dos direitos de acesso disponíveis, fornecendo a visão necessária para garantir que você possa remediar o acesso desnecessário e garantir a segurança de cada identidade:

- Obtenha os dados certos sobre cada identidade (humana e máquina) para avaliar melhor a que elas têm acesso no momento, como o acesso está sendo usado e a que essas identidades devem ter acesso – o que gera decisões de identidade mais inteligentes e mais conscientes do contexto.
- Compreenda, relate e gerencie dinamicamente políticas críticas de segurança de identidade em todo o ambiente corporativo em constante evolução da atualidade.
- Obtenha uma visão de 360 graus de todas as identidades e seu respectivo acesso, utilizando essa inteligência para detectar e resolver anomalias de acesso, evitar combinações de acesso tóxicas e reduzir o risco de acesso, ao mesmo tempo em que permite que os negócios sejam realizados na velocidade e escala necessários.

Em segundo lugar, para simplificar com sucesso os processos de identidade e descobrir, gerenciar e proteger melhor o acesso dos usuários e liberar seus funcionários para que se concentrem em inovação, colaboração e produtividade, uma solução de segurança de identidade deve permitir que você:

- Substitua processos manuais por fluxos de trabalho automatizados e inteligentes para garantir o acesso oportuno e ideal a recursos e dados empresariais essenciais.
- Aplique tecnologias como IA e aprendizado de máquina para monitorar sua organização à medida que ela evolui – permitindo que você adapte de forma autônoma os modelos e políticas de acesso para que sua segurança permaneça atualizada e em conformidade com os requisitos de regulamentações e da empresa.
- Simplifique a administração de programas de segurança de identidade automatizando decisões importantes de identidade, como solicitações de acesso, modelagem de perfis funcionais e certificações de acesso, economizando tempo e liberando as equipes de TI para que concentrem em outras atividades.

Em terceiro lugar, a solução deve ampliar sua capacidade de incorporar o contexto de identidade em todo o ambiente híbrido e gerenciar e controlar de modo centralizado o acesso a todos os dados, aplicações, sistemas e infraestrutura de nuvem:

- Integre-se perfeitamente com os sistemas de negócios e segurança já existentes para infundir o contexto e as decisões de identidade no fluxo de trabalho diário da empresa, criando uma experiência sem atrito e voltada para o usuário que melhora o tempo de retorno.
- Crie uma estrutura sólida de segurança incorporando dados de identidade em toda a sua empresa para obter uma visibilidade holística do acesso e uso da tecnologia.
- Gerencie e controle de forma centralizada todos os tipos de acesso e identidade em todos os todas as aplicações com um mecanismo de política robusto para permitir uma estratégia holística de segurança e conformidade.

Combinadas, essas três áreas de capacidade permitem a uma empresa:

- Proteger e dar suporte à próxima geração de programas de transformação e inovação de tecnologia de negócios, bem como fusões e desinvestimentos, com controles de identidade corporativa flexíveis e escaláveis incorporados.
- Melhorar consideravelmente a eficiência operacional e reduzir os custos associados às operações de segurança.
- Mitigar o risco de multas indesejadas, interrupção das operações de negócios e perda de reputação pública devido à falta de conformidade regulatória.

Enquadrar o panorama geral: garantir que seu programa de segurança de identidade seja bem-sucedido

Como sua experiência com soluções de segurança de identidade provavelmente já mostrou, a tecnologia é apenas uma parte de qualquer solução que você implementar. Quando você fizer parceria com um fornecedor para produtos e serviços que tenham valor, procure uma função de gestão de sucesso do cliente que possa apoiar você em todas as etapas do processo.

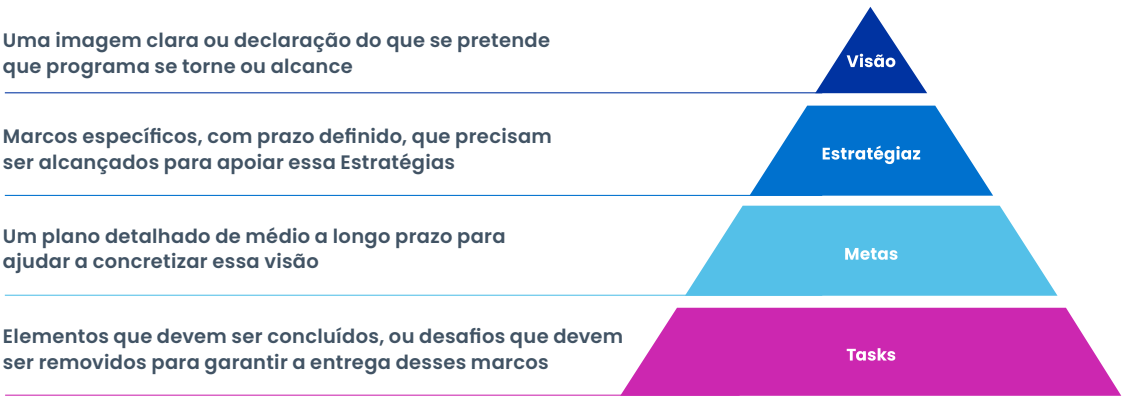
Como seu fornecedor define o sucesso do cliente?

- Como seu parceiro, ele deve oferecer uma estrutura de engajamento sob medida para garantir que você permaneça no caminho certo para alcançar os resultados de negócios desejados em um caso de negócios holístico de segurança de identidade.
- Você deve esperar que ele atue como consultor, entendendo e apoiando seu caso de negócios de segurança de identidade e desenvolvendo um modelo de engajamento eficaz que seja apropriado.
- Os principais elementos que você deve procurar em um programa de gestão de sucesso do cliente são três:

1 Um Gerente de Sucesso do Cliente, com opção para escolher a partir de pool compartilhado ou CSM nomeado, que pode aproveitar os seguintes serviços oferecidos pelo fornecedor:

- **Programas de aprendizagem**
- **Consultores técnicos**
- **Equipes de consultoria**
- **Perspectivas de produtos**
- **Avaliações de valor**
- **Eventos peer-to-peer**

Plano de sucesso do cliente: criar a conexão entre a visão e as tarefas



2 Um plano personalizado de sucesso do cliente (CSP) que:

- Esclarece sua visão e imagem de valor para a segurança de identidade refletindo as metas das principais partes interessadas (por exemplo, segurança cibernética, liderança de TI, auditores, reguladores, finanças)
- Estabelece medidas tangíveis e marcos
- Documenta uma estrutura de engajamento estabelecida para garantir o progresso, por exemplo:

  Modelo Digital: engajamentos baseados na web, compartilhamento de melhores práticas, divulgação agendada, convites para eventos virtuais com opções de serviços adicionais e triagem de problemas.

  Modelo Medium-touch a high-touch: plano detalhado de sucesso do cliente, análises de CSP, planejamento futuro e mitigação de riscos, triagem de problemas e planejamento de melhoria.

  Modelo High-touch: revisões mais frequentes de CSP, planejamento estratégico, verificações mensais, exposição ao roteiro do fornecedor, facilitação do conselho consultivo do cliente (CAB), patrocínio executivo.

3 Resultados verificados que ajudam você a mostrar o retorno do investimento da empresa em termos de:

- Melhoria da conformidade e redução do esforço despendido em auditorias internas
- Maior produtividade por meio do provisionamento mais rápido do acesso de novos usuários
- Capacidade mais rápida de detectar e reagir a ciberataques
- Riscos de acesso significativamente reduzidos, eliminando o atraso no desprovisionamento de contas de funcionários e terceiros
- Custos reduzidos de helpdesk por meio da automação de tíquetes de helpdesk antes processados manualmente, como solicitações de acesso de autoatendimento e redefinições de senha

Em que fase você está na sua jornada de segurança de identidade?

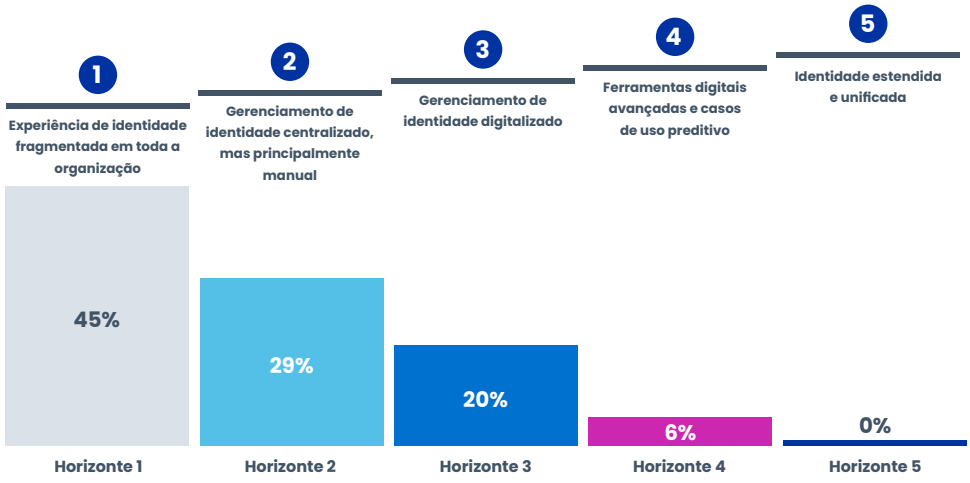
Uma pesquisa com mais de 340 empresas globais obteve respostas sobre a estratégia de segurança de identidade, capacidades técnicas, modelo operacional e talento, testando mais de 50 capacidades nesses tópicos.

A análise, relatada em Horizontes da Segurança de Identidade, revelou cinco horizontes que são comuns em quase todos os programas de identidade corporativa:

- No Horizonte 1, o nível de maturidade mais baixo, as empresas não têm a estratégia e a tecnologia para habilitar identidades digitais
- As que estão no Horizonte 2 adotaram um pouco de tecnologia de identidade, mas ainda se baseiam, em sua maioria, em processos manuais
- As organizações do Horizonte 3 adotaram recursos de identidade em escala
- As que estão no Horizonte 4 automatizaram em escala e usam inteligência artificial (IA) para habilitar identidades digitais
- O Horizonte 5 está mais próximo do futuro da identidade e serve como um ponto crítico de controle na redução do risco de segurança cibernética e no suporte aos negócios na inovação tecnológica da próxima geração

45% das empresas se enquadram no Horizonte 1 – estão no início da jornada de identidade

Distribuição das empresas nos cinco horizontes de jornada de identidade do cliente (n=348)



As % são do número total de organizações no estudo

Conclusão

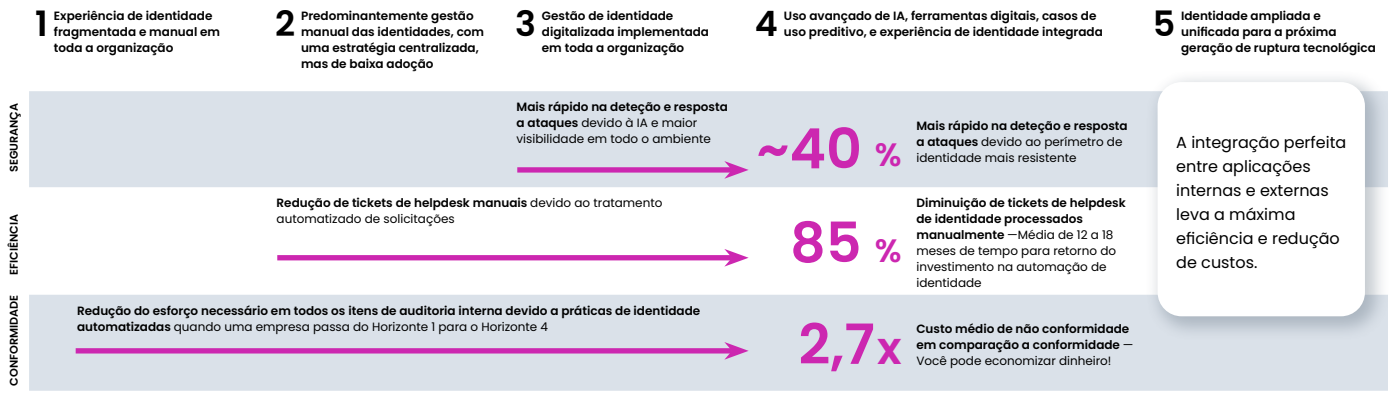
- A maioria das empresas ainda está atrasada na jornada de identidade, o que deixa um valor significativo a ser ganho.
- Exceto algumas empresas de tecnologia, quase nenhuma empresa está no Horizonte 5
- As empresas no Horizonte 2 estão apenas no início da jornada de identidade, uma vez que seu programa de identidade ainda é principalmente manual e reativo

Fonte: **Horizontes da Segurança de Identidade**, SailPoint, 2022.

Quase metade das organizações pesquisadas ainda estão no Horizonte 1, tendo apenas começado suas jornadas de identidade. Devido às crescentes ameaças cibernéticas e à aceleração da inovação digital, essas empresas precisam fazer mais para aumentar sua capacidade quanto à identidade digital do usuário.

Aquelas que avançam em suas jornadas já consideram a segurança de identidade um fator essencial estratégico para a inovação e a segurança nos negócios e reconhecem os benefícios de um programa avançado de segurança de identidade.

Os clientes melhoram sua conscientização de segurança e resiliência à medida que avançam em sua jornada



10% de topo

A maioria das empresas seguras que obtiveram benefícios significativos de segurança e maior resiliência cibernética são as que investiram em sua segurança de identidades

Source: **Horizons of Identity Security**, SailPoint, 2022.

A SailPoint é o núcleo da segurança de identidade para a empresa moderna

A SailPoint é a principal fornecedora de segurança de identidade para a empresa moderna, permitindo que organizações complexas em todo o mundo criem uma base de segurança capaz de se defender contra as ameaças mais urgentes da atualidade.

No núcleo da segurança de identidade da SailPoint estão a inteligência artificial e o aprendizado de máquina. Uma base que protege as organizações por meio da automatização da descoberta, o gerenciamento e o controle de TODOS os acessos dos usuários.

Com a SailPoint, você pode garantir que cada identidade, humana ou não, tenha o acesso necessário para fazer o seu trabalho: nem mais, nem menos. A SailPoint oferece, em média, um retorno de investimento de 345% em 5 anos. Alguns resultados bem-sucedidos de estudos de caso de clientes reais são:

Eficiência de TI

90%

das tarefas de identidade automatizadas e melhoradas

Certificação de acesso

1 ano > **1** mês

Acesso de novo usuário

14 horas to **2.5** minutos

Cancelamento de contas encerradas

30+

dias a minutos

Solicitação de acesso de autoatendimento

62mil solicitações atendidas automaticamente

0 chamadas de helpdesk

Redefinições de senha

5,5mil executadas automaticamente

0 chamadas de helpdesk

Escolha entre nossas soluções de segurança de identidade inteligentes, autônomas e integradas as que melhor se encaixam na fase em que você está em sua jornada de segurança de identidade, combinando a escala, a velocidade e as necessidades ambientais de sua empresa.

Procurando a tecnologia SaaS líder de mercado que lhe permite amadurecer o seu programa de segurança de identidade em seu próprio ritmo?

SailPoint Identity Security Cloud

Com a IA e o aprendizado de máquina em seu núcleo, o Identity Security Cloud da SailPoint é um pacote de recursos SaaS que oferece inteligência incomparável, automação sem atrito e integração abrangente que permite às empresas a gestão de acesso nos ambientes de nuvem mais complexos.

Nossa experiência de trabalho com as principais marcas globais possibilitou saber exatamente o que é necessário hoje: produtos baseados em SaaS direcionados e organizados que funcionam juntos como uma única solução.

Escolha o pacote que melhor se encaixa à fase em que você está em sua jornada de segurança de identidade.

Deseja iniciar ou redefinir um programa de segurança de identidade?

O SailPoint Identity Security Cloud Business reúne todos os principais recursos de segurança de identidade de que as organizações precisam ao iniciar ou redefinir um programa de segurança de identidade.

Solicitações e aprovações de acesso
Capacite usuários e aprovadores com ferramentas de solicitação fáceis de usar.

Certificações de acesso
Prevenir o risco de excesso de provisionamento revogando o acesso desnecessário de usuários.

Informações de acesso
Obtenha uma visualização completa do histórico de acesso, identifique comportamentos de acesso atípicos e gere relatórios de acesso detalhados.

Provisionamento automatizado
Ofereça aos colaboradores o acesso onde quer que estejam – automaticamente e com segurança.

Separação de funções
Detecte e evite conflitos de interesse e possíveis fraudes.

Recomendações
Usar informações orientados por IA para fazer solicitações e tomar decisões de acesso bem fundamentadas.

Aproveite mais de 100 conectores prontos para uso, um conjunto completo de APIs, gatilhos de eventos e recursos adicionais para estender a segurança de identidade em um ambiente híbrido.

Procurando recursos de segurança de identidade mais avançados em uma única solução SaaS?

O SailPoint Identity Security Cloud Business Plus

Modelagem de acesso

Defina novos perfis funcionais que devem ser novos perfis funcionais e monitore continuamente as atualizações dos perfis funcionais existentes, com sugestões de otimizações para esses perfis funcionais.

Gerenciamento de Direitos de Infraestrutura em Nuvem

Tome decisões de acesso de IaaS mais rápidas e bem fundamentadas e detecte riscos potenciais.

Gerenciamento de SaaS da SailPoint

Descubra e mitigue os riscos de acesso ocultos devido à TI invisível (shadow-IT), mantendo sob controle todos os aplicativos de SaaS.

Outras soluções de segurança de identidade da SailPoint

Gerenciamento de risco de acesso

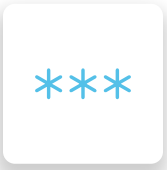
Automatize a análise de risco de acesso em tempo real, simplifique os processos de GRC e identifique os riscos em potencial antes que o acesso seja concedido aos usuários.

Gerenciamento de risco de não funcionário

Execute estratégias de gerenciamento de acesso de identidade e ciclo de vida baseadas em risco para não funcionários.

Gerenciador de acesso a arquivos

Obtenha visibilidade e controle sobre dados não estruturados, descubra exatamente onde seus dados residem e quais informações confidenciais eles contêm.



Gerenciamento de senhas

Minimize as chamadas para o helpdesk, fornecendo aos usuários acesso de autoatendimento.

Primeiros passos

Com este guia do comprador em mãos, agora você tem:

- Ajuda para identificar as metas de negócios mais importantes que você deseja alcançar para melhorar os resultados de segurança de identidade que merecem investimento
- Os recursos que você deve procurar em uma solução para ajudar a realizar esses objetivos
- Conhecimento sobre como as soluções de segurança de identidade da SailPoint, juntamente com seu vasto ecossistema de parceiros, oferecem esses recursos para ajudá-lo a ter sucesso

Como primeiro passo no desenvolvimento de seu plano para melhorar seu programa de segurança de identidade, experimente nossa ferramenta de avaliação de maturidade on-line **www.sailpoint.com/identity-security-maturity** para entender qual horizonte de segurança de identidade sua empresa alcançou e entender como você pode avançar com confiança.

Leve toda a organização para fazer a jornada em vez de apenas a equipe de TI ou de IAM, criando um caso de negócios e estabelecendo propriedade e necessidade claras.

A SailPoint pode ajudá-lo a criar seu caso de negócios. O processo de Avaliação de Valor de Negócios da SailPoint (disponível gratuitamente) permitirá que você construa um caso de negócios detalhado com base em seus desafios e oportunidades específicos:

- Compreenda os desafios específicos de negócios de segurança de identidade e lacunas de funcionalidade que existem no ambiente atual e como as soluções SailPoint podem abordá-los.
- Quantifique os benefícios tangíveis e intangíveis que podem ocorrer, incluindo benefícios de produtividade e eficácia, usando benchmarks do setor, melhores práticas e especificidades de seus processos.
- Forneça um caso de negócios exclusivo para o seu projeto e empresa: análises de retorno sobre o investimento, VPL e payback, com resultados em um formato necessário para o processo de revisão e aprovação da justificativa de custo interno/despesa de capital.

Estamos sempre à sua disposição e teremos satisfação em esclarecer qualquer dúvida que você ainda possa ter. Para ajudar a ajustar seus objetivos de negócios e criar um roteiro de transformação, entre em contato conosco na SailPoint.

www.sailpoint.com

Sobre a SailPoint

A SailPoint ajuda a empresa moderna a gerenciar e proteger o acesso a aplicações e dados de maneira integrada e segura, através da lente de identidade, em velocidade e escala. Como líder da categoria, reinventamos continuamente a segurança de identidade como a base da empresa segura. A SailPoint oferece uma plataforma unificada, inteligente e extensível, criada para defender contra as atuais ameaças cibernéticas dinâmicas e centradas na identidade, ao mesmo tempo que aumenta a produtividade e a eficiência. A SailPoint ajuda muitas das mais complexas e sofisticadas empresas do mundo a criar um ecossistema tecnológico seguro que alimenta a transformação dos negócios.

sailpoint.com/pt-br

SP2306-2408