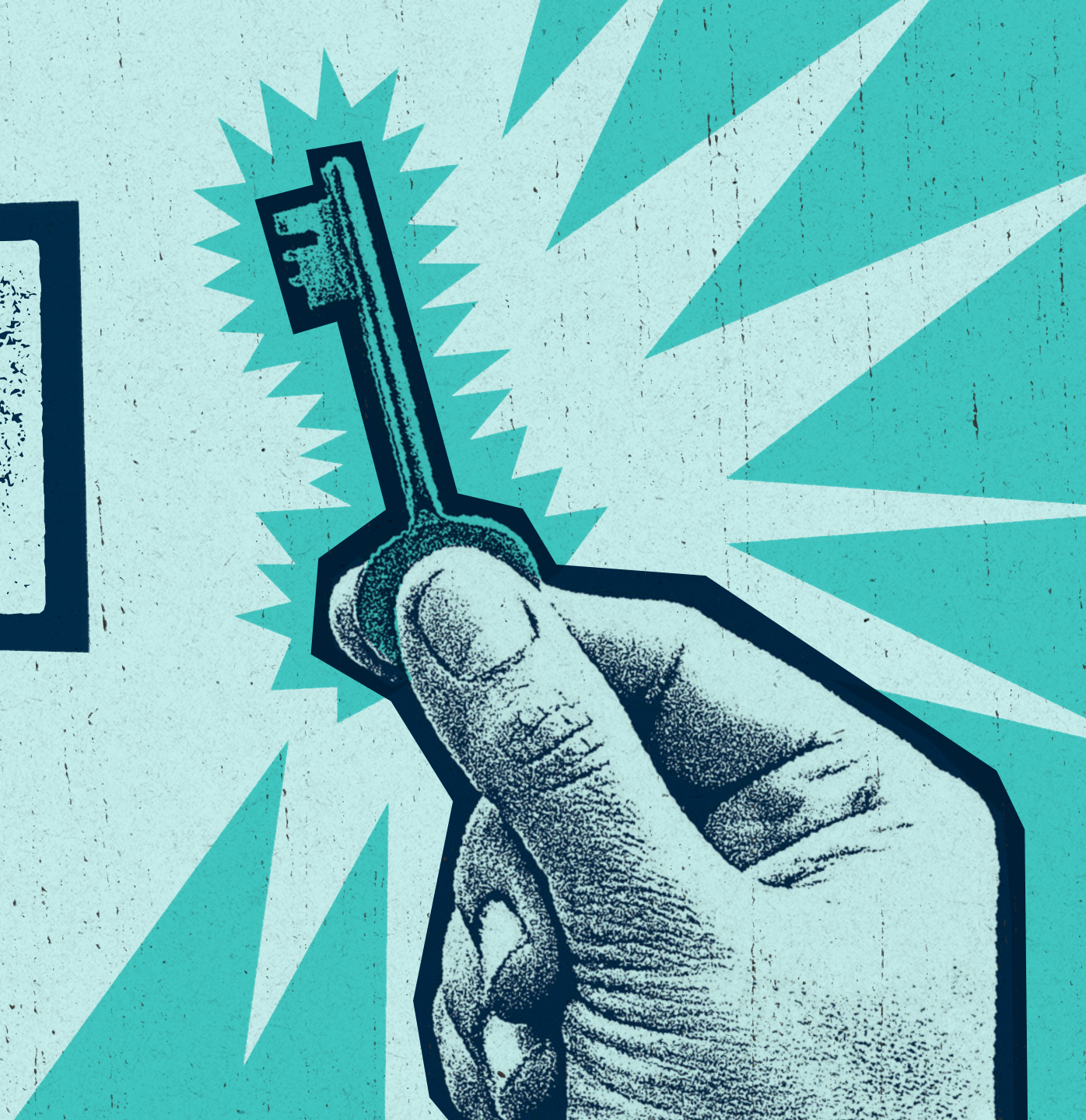
jumpcloud™ fc BRASIL

PAM

PARA O POVO

Por que a indústria tem
escondido uma ferramenta
essencial.
E por que isso precisa parar.



Há um grande problema com o PAM

O mercado hoje quer que você acredite que o Gerenciamento de Acesso Privilegiado (PAM) é algo feito apenas para os "peixes grandes"-

para as grandes corporações, com equipes de segurancça dedicadas e salas de controle central repletas de monitores exibindo cógigos em verde-neon e alertas vermelhos.

Mas isso simplesmente não soa realista - e você não está convencido.

É por isso que está lendo isto.

Você tem razão em ser cético.

Historicamente, o PAM tem sido associado a grandes empresas, com equipes de segurança prórpias. Mas o que foi, nem sempre é um bom indicador do que deveria ser.

E a verdade é: você precisa de PAM.

Todos precisam.

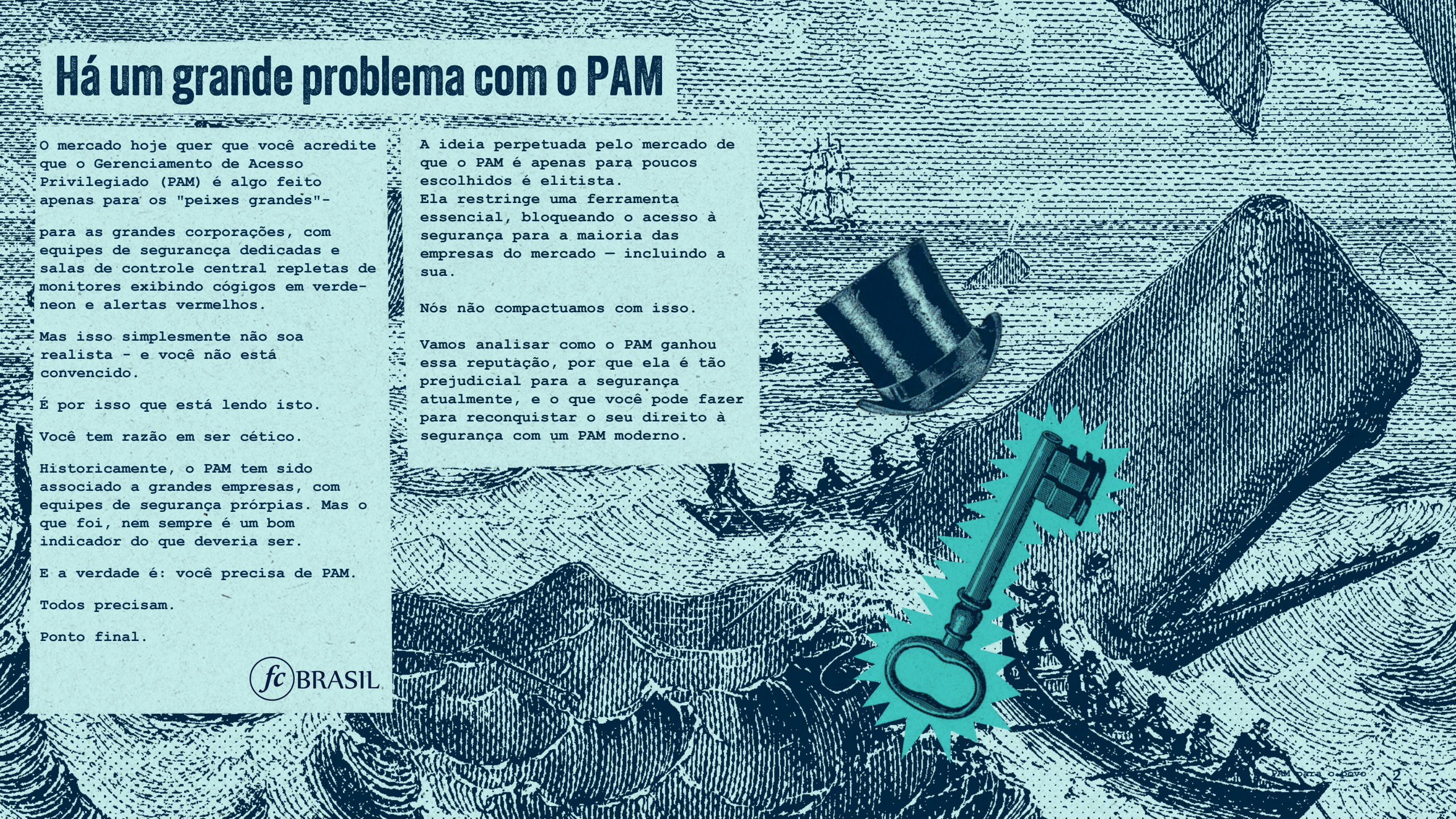
Ponto final.

fc BRASIL

A ideia perpetuada pelo mercado de que o PAM é apenas para poucos escolhidos é elitista.
Ela restringe uma ferramenta essencial, bloqueando o acesso à segurança para a maioria das empresas do mercado — incluindo a sua.

Nós não compactuamos com isso.

Vamos analisar como o PAM ganhou essa reputação, por que ela é tão prejudicial para a segurança atualmente, e o que você pode fazer para reconquistar o seu direito à segurança com um PAM moderno.



Por que o PAM é tão inacessível?

Há algumas razões pelas quais o PAM tem sido reservado para grandes empresas. Essas razões se encaixam fortemente na lógica do "sempre fizemos assim" — o que significa que está na hora de mudar.

Custos e exigência de recursos
As soluções de PAM costumam ser complexas, caras e exigem conhecimento especializado para serem gerenciadas. Os requisitos de instalação local (on-premise) impedem muitas empresas que operam totalmente na nuvem de utilizá-las.

Ênfase excessiva na equipe de segurança
A ideia de que o PAM é uma ferramenta exclusiva da área de segurança, e não algo que TI e Segurança possam usar em conjunto, desmotivou os fornecedores a criar soluções de PAM mais amigáveis para equipes de TI.

Falta de modernidade
Muitas soluções de PAM ainda operam com uma mentalidade ultrapassada. Isso as impede de se estender a todos os recursos modernos, como infraestruturas em nuvem, aplicações SaaS e atividades realizadas em navegadores.

Toda empresa merece acesso aos recursos de que precisa para se proteger. O PAM se tornou uma necessidade, até para empresas menores. Isso significa que elas também devem ter acesso ao PAM.

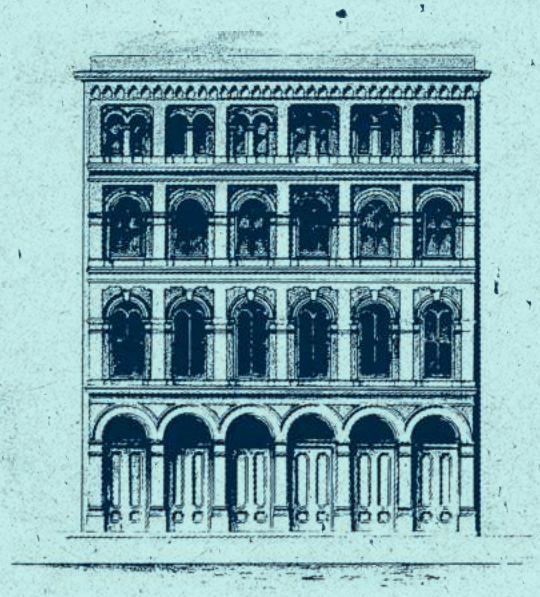
fc BRASIL

Por que todos precisam de PAM?

O PAM costuma ser associado a grandes organizações altamente regulamentadas, com necessidades de segurança complexas. Então, se você não lida com material ultrassecreto, pode ser fácil deixar o PAM de lado. Mas todas as empresas enfrentam ameaças existenciais de segurança — não apenas as maiores.

A ideia de que pequenas e médias empresas (PMEs) são pequenas demais para atrair a atenção de invasores simplesmente não é verdadeira. Em 2024, **46% das PMEs** foram vítimas de um ataque. Isso é quase metade — o suficiente para justificar preocupação séria e a necessidade de ação séria.

À medida que o local de trabalho se torna mais móvel e conectado, a segurança só fica mais difícil. Hoje, o acesso privilegiado vai muito além do administrador; muitos usuários agora têm algum nível de acesso a recursos privilegiados. Isso significa que todas as empresas precisam de ferramentas para combater ameaças na camada de identidade.
E isso significa que todas as empresas precisam de PAM.



fc BRASIL

Ninguém está a salvo

O efeito dominó dos ataques à cadeia de suprimentos

Um ataque à cadeia de suprimentos explora um fornecedor confiável para alcançar seus clientes. A violação se espalha como fogo em palha seca, à medida que os invasores usam acessos legítimos para se mover lateralmente pelas redes e infectar outros pontos de contato.
Em 2019, um ataque à cadeia de suprimentos ao software Orion, da SolarWinds, afetou **mais de 18.000 empresas.**
Em 2023, um ataque semelhante ao serviço de transferência de arquivos MOVEit afetou **mais de 1.000 organizações.**
Mesmo que o seu negócio não pareça um alvo de alto valor, ele não está imune a ataques. O PAM oferece uma camada essencial de proteção contra esse tipo de ameaça, podendo reduzir drasticamente seus efeitos ao monitorar e controlar o acesso privilegiado e bloquear movimentos laterais dentro da rede.

Onde as coisas deram errado?

Se todos precisam de PAM, por que nem todos têm? E por que nem todos conseguem obtê-lo?

Existem certos padrões que persistem entre os principais fornecedores de PAM. Esses padrões mantêm a falsa impressão de que o PAM é algo exclusivo para grandes empresas.

Ideais Legados

O PAM foi desenvolvido na época em que a infraestrutura era exclusivamente local (on-premises).
Esse formato (com todos os seus custos e complexidades) permaneceu entre muitos dos grandes fornecedores de PAM, porque as grandes empresas podem arcar com a manutenção de seus investimentos legados.

Tendência das Soluções Pontuais

Os fornecedores tendem a desenvolver ferramentas como soluções pontuais, e não de forma holística. Essa abordagem facilita a entrada inicial nas organizações, mas também estimula renovações contínuas de licenças e a dependência de serviços profissionais para manter e expandir o uso da ferramenta.

Os Fornecedores Preferem a Previsibilidade

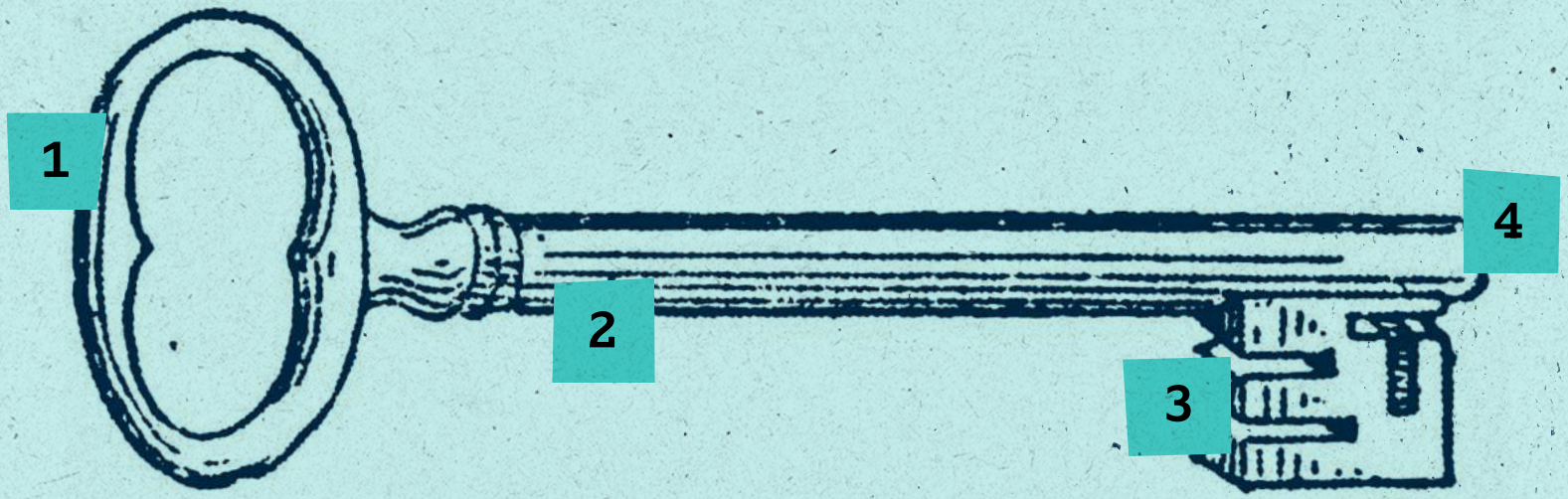
Se as grandes empresas continuam precisando de PAM devido a pressões externas, é mais fácil — e mais lucrativo, além de menos arriscado a curto prazo — para os fornecedores continuar vendendo para esse público do que se aventurar em territórios desconhecidos.

"PAM é apenas para a área de Segurança"

Como as soluções de PAM continuam sendo divulgadas e desenvolvidas para equipes de segurança de grandes empresas, são justamente essas equipes que as compram e utilizam. Essa profecia autorrealizável bloqueia a inovação, mesmo diante de uma necessidade evidente de mudança.

Esses padrões são frustrantes. Mas padrões podem mudar.

Como é o PAM moderno e acessível?



1. Atende ao ambiente de trabalho moderno em todas as suas formas.

2. Permitir a colaboração entre TI e Segurança, independentemente de como essas responsabilidades sejam distribuídas.

3. Ser acessível sob a perspectiva de custos, esforços e recursos.

4. Integrar-se total e completamente a cada transação de acesso.

1. O PAM deve atender ao ambiente de trabalho moderno

O objetivo do PAM está no próprio nome: proteger e gerenciar o acesso privilegiado dentro do seu ambiente. Mas, para realmente proteger esse acesso, o PAM precisa abranger tudo o que faz parte do seu ecossistema.

Ele deve ser capaz de:

Gerencie o acesso dos colaboradores onde quer que eles trabalhem

Esteja você no escritório, totalmente remoto ou em um modelo híbrido, o ambiente de trabalho é permanentemente móvel.

Uma solução de PAM não é realmente completa se não for capaz de gerenciar o acesso em todos esses cenários.

Gerencie o acesso aos recursos onde quer que ele ocorra

Não deve ser necessário fazer malabarismos dignos de circo para administrar privilégios em todos os recursos que você gerencia.

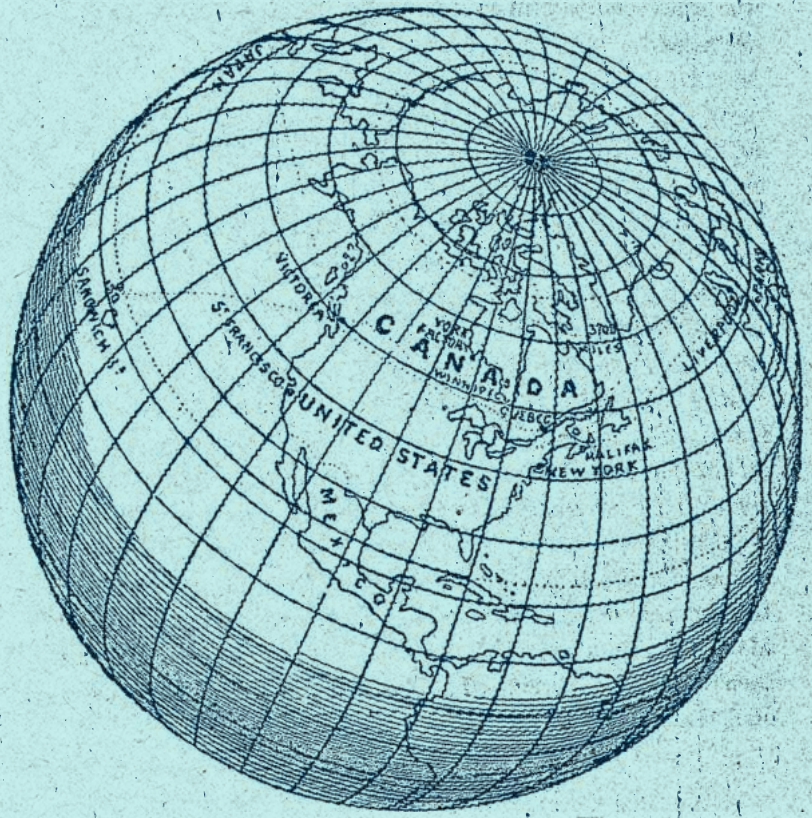
O PAM precisa abranger aplicações SaaS, infraestruturas em nuvem e locais (on-premises), bancos de dados, atividades em navegadores e muito mais.

Faça isso sem precisar de uma VPN

As VPNs são caras, difíceis de escalar e pouco amigáveis tanto para o usuário quanto para o trabalho remoto.

Elas não se alinham aos princípios centrais do Zero Trust, pois defendem o perímetro e não o nível de identidade.

O PAM não deve depender de uma VPN para funcionar.



As soluções de PAM legadas não foram projetadas para atender a essas necessidades e não são suficientes para os ambientes de trabalho modernos.

2. O PAM deve ser ací em custos e recursos

Nem todas as empresas possuem infraestrutura local (on-premises), e esse número está diminuindo à medida que a nuvem se torna o padrão. Ao mesmo tempo, algumas empresas ainda mantêm infraestruturas locais que precisam proteger, e as soluções de PAM também devem ser capazes de lidar com isso.

Mesmo assim, existem alguns fatores que tornam o PAM inacessível para a maioria das empresas:

Resource Requirements

Many PAM solutions are complex and require specific expertise to operate them. This bars those without a Security team from using PAM solutions.

PAM should be designed to be used by either Security or IT teams.

Requisitos de Arquitetura

Muitas ferramentas de PAM legadas operam, pelo menos em parte, em infraestruturas locais (on-premises), o que transfere para o cliente a responsabilidade pela hospedagem.
As ferramentas de PAM não devem exigir infraestrutura local (on-premises) como condição para serem utilizadas.

Requisitos de Recursos

Muitas soluções de PAM são complexas e exigem conhecimento técnico especializado para serem operadas.
Isso impede empresas sem uma equipe de segurança de utilizarem essas soluções.
O PAM deve ser projetado para ser usado tanto por equipes de Segurança quanto por equipes de TI.

Custo

Considerando licenças, implementação, manutenção de servidores e equipe, fica claro que o custo do PAM continua proibitivo para pequenas e médias empresas (PMEs).
Os fornecedores devem oferecer soluções de PAM acessíveis voltadas para PMEs.

Considerando licenças, implementação, manutenção de servidores e pessoal, fica evidente que o custo do PAM ainda é altamente proibitivo para pequenas e médias empresas (PMEs). Os fornecedores precisam disponibilizar soluções de PAM mais acessíveis adaptadas à realidade das PMEs.

fc BRASIL

3. O PAM deve apoiar a intregração entre TI e Segurança

O mercado continua tratando o PAM como uma solução exclusiva para a área de Segurança. Mas **91% dos profissionais de Segurança** afirmam que a colaboração com a equipe de TI é essencial para sua estratégia.

Se a sua empresa não possui uma equipe de Segurança, o time de TI ainda deve conseguir usar o PAM. Se possui uma equipe de Segurança, ela deve trabalhar o PAM de forma colaborativa com o TI.

Para que o PAM seja realmente acessível, ele precisa ser utilizável por equipes de TI, tenham elas ou não experiência profunda em segurança.

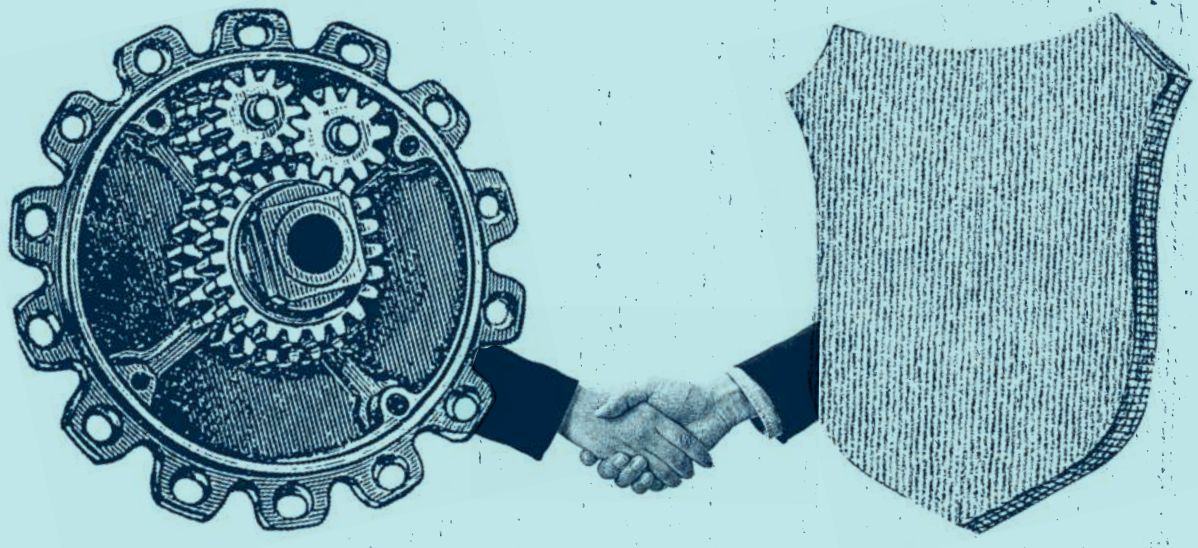
Isso significa que as ferramentas de PAM devem:

Oferecer soluções dimensionadas e projetadas para empresas de menor porte.

Fornecer contexto e análises voltadas para administradores não especializados.

Criar integrações nativas e interfaces fáceis de usar.

Fornecer contexto e análises voltadas para administradores não especializados.



4. O PAM deve ser totalmente integrado

A abrangência é fundamental para uma solução de segurança eficaz. Uma solução que não seja abrangente deixa pontos cegos vulneráveis.

E se soluções de segurança são tratadas como abrangentes quando não são, esses pontos cegos ficam sem atenção, colocando você em uma situação ainda pior do que no começo.

Para que o PAM seja realmente abrangente, ele precisa se estender a tudo no seu ambiente, cobrindo cada transação de acesso.

Uma plataforma que combine o PAM com a gestão central de TI pode ajudar a garantir essa abrangência.

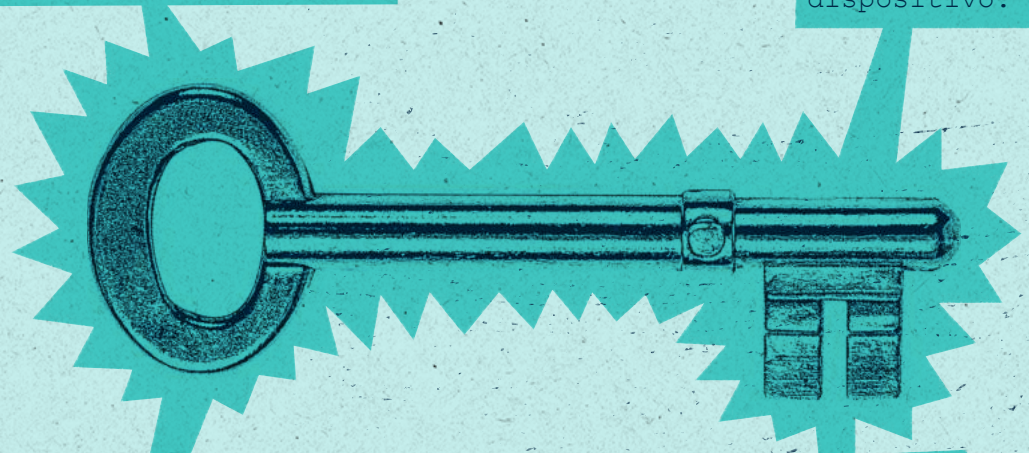
A melhor maneira de alcançar isso é com uma solução de PAM totalmente integrada em:

Identidade

A segurança na camada de identidade é essencial tanto para o modelo Zero Trust quanto para o PAM. O PAM deve proteger o acesso na camada de identidade, e não no perímetro legado.

Dispositivos

Ter um único dispositivo por colaborador já não é mais o padrão de trabalho.O PAM precisa proteger o acesso em qualquer dispositivo.



Acesso

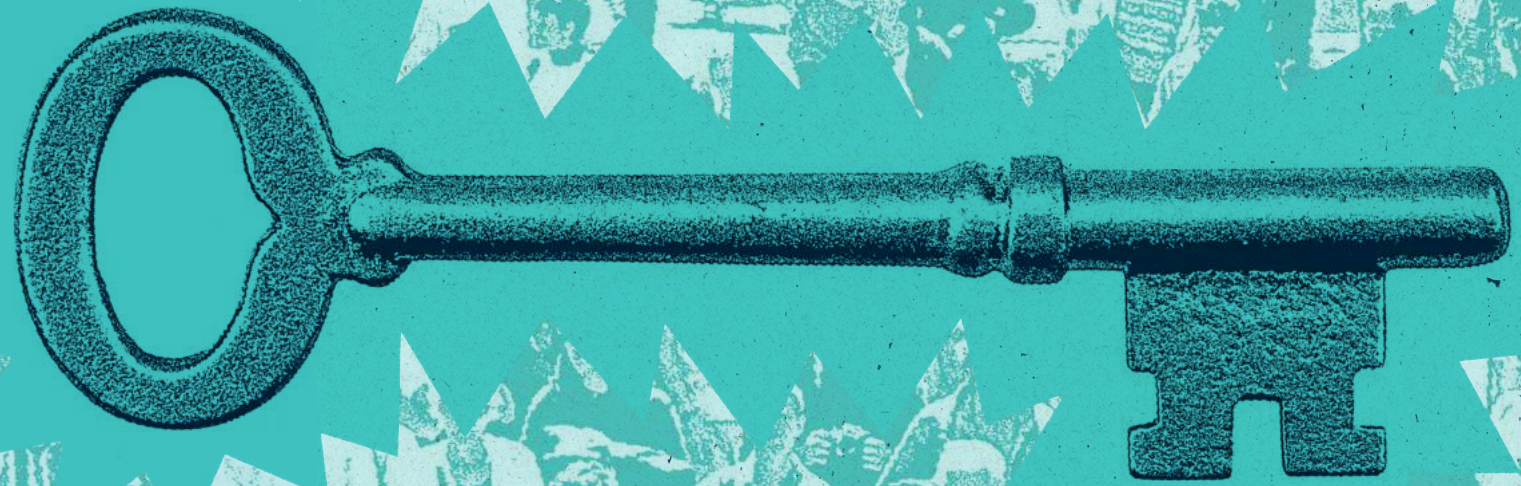
O escopo do PAM deve abranger todas as transações de acesso, independentemente de onde ocorram.

SaaS

A maior parte dos negócios ocorre na nuvem, e o PAM deve ser capaz de proteger esses recursos.

fc BRASIL

Traremos o



PAM para o povo!

Você precisa de PAM, mas os fornecedores não estão oferecendo opções acessíveis.
Fica claro que há uma lacuna no mercado.
Isso significa que é hora de mudar.

A JumpCloud foi criada como uma alternativa moderna e acessível aos gigantes do mercado.
Democratizar soluções faz parte do nosso DNA.
Por isso, estamos trazendo o PAM até você.

A JumpCloud adquiriu recentemente a VaultOne, uma solução moderna de PAM, para tornar o PAM acessível e eficiente para empresas de todos os tamanhos.

O JumpCloud PAM oferece um caminho claro para proteger cada ativo crítico, simplificar a conformidade e enfrentar com confiança os maiores desafios de segurança da atualidade.

fc BRASIL

fc BRASIL

A FCBrasil é uma empresa de distribuição de software especializada em segurança da informação. Estabelecemos parcerias com fabricantes qualificados e com produtos de grande potencial de vendas no mercado brasileiro e da América Latina. Ajudamos nossos canais de venda a atenderem seus clientes, oferecendo suporte na pré-venda e na pós-venda, além de treinamentos nas soluções distribuídas para que a revenda possa estar cada vez mais capacitada.