FOLHETO

Autenticação de dois fatores Starling

Verificação de identidade segura e simples

Benefícios

- Aumenta a segurança para praticamente qualquer sistema ou aplicação
- Simplifica o gerenciamento contínuo ao não requerer os custos com infraestrutura e sem causar os problemas relacionados às soluções no local
- Facilita a adoção dos usuários ao fornecer opções de autenticação de utilização simples, tais como push para autenticação, textos SMS e chamadas telefônicas
- Habilita uma resposta rápida do Help Desk a problemas de autenticação do usuário em qualquer navegador da Web
- Reduz os riscos de violações de segurança de credenciais de autenticação comprometidas ou roubadas
- Fornece uma pista de auditoria abrangente para atender aos requisitos de conformidade

Visão geral

Independentemente de como as senhas sejam comprometidas, seja por comportamentos questionáveis dos usuários, por uso de senhas fracas ou simplesmente por roubo, será ruim para a reputação e para o resultado final de sua organização. Há uma maneira simples de aprimorar a segurança e prevenir a violação de dados ao exigir autenticação de dois fatores para obter acesso aos recursos de sua rede.

Com a Autenticação de dois fatores Starling, uma solução baseada em SaaS, é possível garantir a segurança de sua organização, tornar os usuários mais produtivos e reduzir drasticamente o volume de chamadas de redefinição de senha do seu Help Desk.

Torne o acesso do usuário seguro e simples

A maneira mais simples e segura de lidar com o problema da senha é pela autenticação de dois fatores (TFA). Entretanto, nem todas as soluções de dois fatores são iguais. Considere a forma de operação de sua organização, como os processos de autenticação podem se tornar mais eficientes, quais formatos de token serão necessários e o que funcionará com suas pilhas de aplicação e infraestrutura.

A autenticação de dois fatores Starling resolve o problema da senha sem gerar os custos de capital que vêm com soluções tradicionais no local. Seu painel de fácil utilização para administradores e opções de autenticação flexíveis para usuários finais permitem que as organizações verifiquem a identidade dos usuários de forma rápida e fácil.

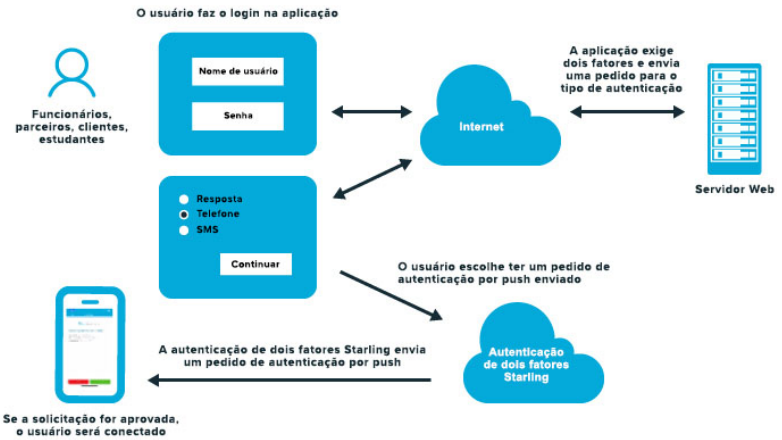

Figura 1: Arquitetura e módulos de autenticação de dois fatores Starling.

Recursos

Painel de administrador fácil de usar

O painel do administrador baseado em função com fluxo de trabalho de aprovação garante que os administradores e os associados do Help Desk recebam os direitos e as tarefas apropriados, ao mesmo tempo que facilita o gerenciamento de contas de usuários finais, a geração de códigos de resposta temporária e a execução de verificações de integridade para averiguar o funcionamento correto da aplicação móvel.

Múltiplos métodos de autenticação

Os usuários podem gerar senhas de uso único com as aplicações móveis de 2FA Starling para iOS, Android e Chrome, ou receber uma senha de uso único via SMS ou chamada telefônica.

Push para autenticação

Torne a autenticação de dois fatores ainda mais fácil para seus usuários: eles podem pular a senha de uso único ao optar pelo envio por push para autenticação após a inserção do nome de usuário e da senha em uma aplicação. Isso enviará um SMS de verificação à aplicação móvel do usuário para verificar se ele aprova ou recusa a solicitação de login na aplicação. Quando aprovada, eles serão automaticamente conectados à aplicação.

Tokens

A autenticação de dois fatores Starling possui diversas opções, inclusive aplicações móveis para iOS e Android, Chrome, mensagem SMS ou chamada telefônica.

Marca do token

Por meio do painel do Starling, os administradores podem facilmente personalizar a aparência do token na aplicação móvel para que ela corresponda à marca da empresa.

Adaptador do ADFS

Permite que as organizações implementem a autenticação de dois fatores a aplicações que utilizam o protocolo Microsoft WS-Federation, como o Office 365. Além disso, ele é compatível com outros protocolos de federação, inclusive o SAML 2.0, a fim de oferecer suporte a logins para aplicações em nuvem, como Google Apps e salesforce.com.

Agente Radius

Permite que as organizações ofereçam suporte à autenticação de dois fatores em tudo o que utilizar o protocolo RADIUS para autenticação.

Agente HTTP

Implemente a proteção da autenticação por dois fatores para sites IIS.

Login de desktop

Aprimore seu ambiente: adicione a autenticação de dois fatores aos computadores e servidores dos usuários unificando logins de usuário e fortalecendo a autenticação.

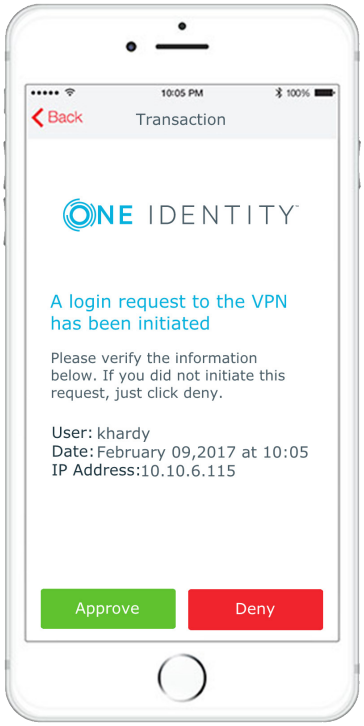

Figura 2: O Push para autenticação simplifica e protege o processo de login do usuário.

Sobre o One Identity

O One Identity ajuda as organizações a obter o melhor Gerenciamento de Identidades e Acessos (IAM). Com a nossa combinação exclusiva de ofertas, inclusive um portfólio de soluções de governança de identidades, gerenciamento de acessos, gerenciamento privilegiado e identidade como serviço, as organizações podem alcançar total potencial, sem obstáculos de segurança e protegidas contra ameaças. Saiba mais em OneIdentity.com