



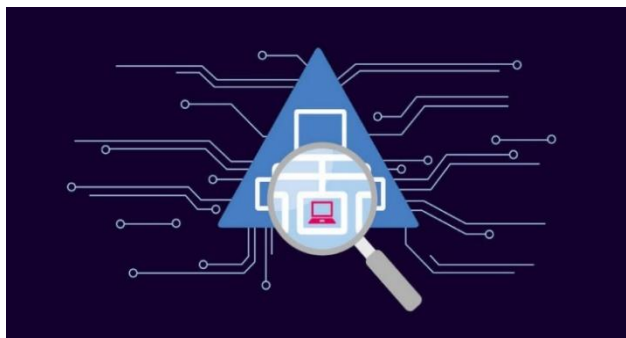
Seguro, Simples, Full Duplex Authentication® para aplicativos da Microsoft

O aumento repentino do trabalho remoto em um aplicativo em nuvem e no mundo móvel desafiou os profissionais de segurança de rede. O perímetro de segurança, que agora se estende às residências dos trabalhadores, ainda deve fornecer acesso seguro a uma variedade de aplicativos de negócios. Com os usuários de hoje também exigindo acesso a aplicativos locais e aplicativos em nuvem, as organizações não podem contar com a arquitetura de segurança de perímetro tradicional para proteger o acesso aos aplicativos. As equipes de TI e segurança cibernética agora são encarregadas de fornecer acesso seguro a recursos em um ambiente híbrido de várias nuvens. A maioria das infraestruturas de TI corporativas são baseadas nas plataformas Active Directory (local) e / ou Azure (nuvem) da Microsoft. **NoPass™** oferece uma variedade de recursos e soluções que verificam a confiança da força de trabalho e mudam com sucesso para o trabalho remoto, implementando e reforçando as práticas de confiança zero **NoPass™**.

NoPass™ é uma solução de autenticação segura que oferece as duas coisas de que você mais precisa: o mais alto nível de segurança de autenticação e a interface de usuário mais simples. Agora você pode ter a confiança de nunca se preocupar em comprometer suas credenciais online. A autenticação multifator sem senha **NoPass™** do Windows garante que apenas usuários autorizados tenham acesso a dados confidenciais em todos os seus sistemas. Com o **NoPass™**, é fácil para os usuários se autenticarem nos aplicativos de que precisam sem comprometer a segurança.



Integrar no AD com RADIUS



Os Serviços de Federação do Active Directory (ADFS) são o provedor de identidade de fato em um ambiente Microsoft. Muitas organizações o usarão para autenticar usuários do Office 365 em um Active Directory local. O suporte entre os provedores de serviços em nuvem está crescendo, permitindo que você autentique não apenas usuários do Office 365, mas usuários de uma variedade de aplicativos de negócios.

Em certas circunstâncias, você pode exigir autenticação multifator (MFA). Pronto para uso, o ADFS oferece suporte apenas para certificados X.509. Felizmente, existe o conceito de adaptadores de autenticação, permitindo que você aumente a segurança e a simplicidade usando um plug-in MFA. Na **Identité™**, desenvolvemos um plug-in RADIUS que permite solicitar aos usuários que insiram sua senha AD, fazer com que executem dois ou mais fatores adicionais de autenticação e enviar a resposta ao servidor **NoPass™** que atua como um cliente RADIUS, juntamente com as contas userPrincipalName, para validação e segurança de autenticação máxima.

O processo **NoPass™, Full Duplex Authentication®** segue um modelo de autenticação descentralizado. Esse recurso interrompe os ataques de personificação e evita que as credenciais sejam interceptadas por um “ataque Man In Middle” (MIM). **NoPass™** tem uma arquitetura flexível para se integrar facilmente com qualquer solução de autenticação de usuário.

Integração SSO federada com Azure Directory e Office 365

Office 365 is a cloud-based subscription service that brings together the best tools for the way people work today. By combining best-in-class apps like Excel and Outlook with powerful cloud services like OneDrive and Microsoft Teams, Office 365 lets anyone create and share anywhere on any device.

O Office 365 é um serviço de assinatura baseado em nuvem que reúne as melhores ferramentas para a forma como as pessoas trabalham hoje. Ao combinar os melhores aplicativos da classe, como Excel e Outlook, com poderosos serviços em nuvem como OneDrive e Microsoft Teams, o Office 365 permite que qualquer pessoa crie e compartilhe em qualquer lugar e em qualquer dispositivo.



NoPass™ fornece acesso seguro e transparente aos seus aplicativos móveis, em nuvem e corporativos. A integração do Office 365 com **NoPass™** atuando como o provedor de identidade é realizada por meio dos padrões abertos SAML e OIDC, que oferecem suporte a perfis de usuário ativos e passivos.

MFA - mais do que apenas um SMS OTP

O Azure fornece uma solução SMS OTP como 2FA para aumentar a segurança, mas com o aumento de phishing e outros ataques de identidade em nossos dias, a autenticação que requer um nome de usuário e senha (como RADIUS) pode estar potencialmente em risco. Esquemas sofisticados de engenharia social e táticas inteligentes podem enganar até os usuários mais experientes. Para combater isso, **NoPass™** introduziu sua solução MFA, que aumenta significativamente a segurança geral e é compatível com os principais protocolos de autenticação que estão no mercado.

Protegendo o acesso VPN e RDP Gateway para funcionários em casa

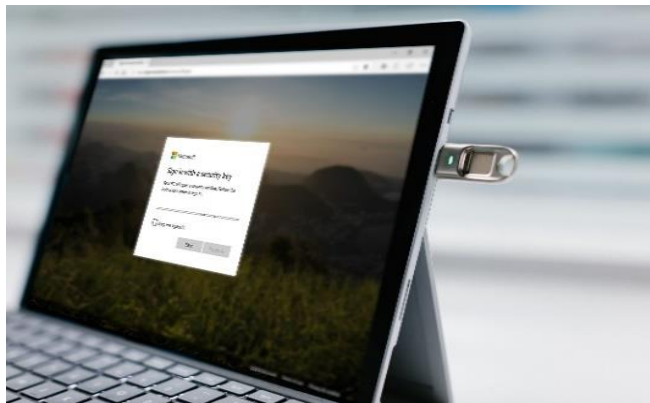
Se você já está executando seus aplicativos de desktop hospedados no local ou planejando mover essas cargas de trabalho para a nuvem, você precisa de uma conexão de rede segura para o escritório para os trabalhadores domésticos. O **NoPass™** se integra aos sistemas operacionais de cliente e servidor Microsoft Windows para adicionar autenticação multifator aos logins com uma solução que equilibra segurança e usabilidade. As políticas de acesso podem ser configuradas para bloquear o acesso a estações de trabalho remotas sensíveis de dispositivos que estão desatualizados ou não compatíveis com seus requisitos de segurança.

NoPass™ para Windows Logon adiciona **NoPass™** autenticação multifator para a área de trabalho do Windows e logins do servidor, tanto no console local quanto nas conexões de entrada da Área de Trabalho Remota (RDP) e VPN. Um fator será algo que o usuário possui, um token seguro. Isso é protegido pela patente pendente da IdentiTé, **Full Duplex Authentication®**, que é imune à falsificação de identidade. Outro fator que um usuário pode ser um token de hardware como um Yubikey. Se o dispositivo suporta biometria, então algo que o usuário é pode ser outro fator.

Cliente Nativo do Windows

O cliente de autenticação **NoPass™** para Windows oferece o mesmo multifator que o aplicativo móvel. Além disso, tokens de hardware nativos, como Yubikey e outros dispositivos de terceiros são suportados pelo cliente Windows, **NoPass™** é uma solução de autenticação de dois fatores fácil de usar que se encaixa perfeitamente nos fluxos de trabalho diários de seus usuários.

Alguns sites e serviços online permitem que os usuários protejam suas contas com uma senha gerada pelo celular que deve ser inserida manualmente e funciona apenas por um determinado período - normalmente 30-60 segundos. Tanto o cliente de autenticação Windows quanto o Mobile **NoPass™** podem proteger todos os sites com credenciais exclusivas protegidas pelo **Full Duplex Authentication®**. Todos os usuários mantêm todas as suas contas e credenciais em uma carteira digital virtual.



Integração de login do Windows (GINA), incluindo desbloqueio sem senha com smartphones habilitados para Bluetooth

O **NoPass™** permite que dispositivos sem fio equipados com Bluetooth sejam usados para segurança do computador (login, autenticação, bloqueio / desbloqueio). Seu telefone celular desempenha o papel de sua chave de acesso de seu PC:

- Logon automático do Windows quando um usuário se aproxima do computador (com o telefone celular).
- O computador será protegido por uma senha, mas você não precisa inseri-la manualmente.

NoPass™ é uma solução de autenticação genuína com substituição completa de senha, e não apenas um armário de PC primitivo como muitos outros programas onde você deve inserir uma senha manualmente de qualquer maneira para fazer o login.

Opções de implantação

Em Site

- Implantação altamente disponível
- Suporte a Docker e Kubernetes
- Proxy reverso
- Clustering e alta disponibilidade

NUVEM

- Nuvem privada implantável (ou seja, AWS, Azure, IBM)
- Alta escalabilidade
- Implante em quase todos os países
- Suporte para autoinscrição para testes e produção

Características do Produto

- Produto de autenticação sem senha simples e seguro
- O processo **NoPass™, Full Duplex Authentication®** segue um modelo de autenticação descentralizado. Funciona em conjunto com qualquer tecnologia de autenticação de usuário tradicional, como PIN, OTP, PKI e biometria
- SSO totalmente sem senha, fácil de instalar, atende às necessidades de qualquer organização também ganha
- Imagem inovadora e código OTP, conveniente ao usuário e segurança de força bruta muito maior
- Visão geral completa da administração - usando o painel de administração, defina políticas e restrições, como dispositivos e requisitos geográficos
- Arquitetura flexível para fácil integração com qualquer autenticação de usuário existente

Benefícios de NoPass™

Segurança

As credenciais de login são exclusivas em todos os sites, nunca saem do dispositivo do usuário e nunca são armazenadas em um servidor.

Conveniência

Os usuários desbloqueiam credenciais de login com métodos integrados simples, como leitores de impressão digital ou varreduras faciais.

Escalabilidade

O amplo uso de smartphones e nossa implantação na nuvem tornam muito fácil dimensionar qualquer autenticação existente.

Eficiência de custos

Economize milhões em custos de helpdesk e suporte de senha.

Privacidade

Proteja os usuários contra vazamentos de credenciais e phishing de senha.