FOLHETO

Defender®

Proteja seu perímetro com autenticação por dois fatores

Benefícios

- Segurança aprimorada para praticamente qualquer sistema ou aplicativo
- Aproveita a escalabilidade, a segurança e a conformidade do Active Directory
- Ativa o autorregistro de token e a renovação por usuários
- Acelera a resolução do Help Desk de problemas de autenticação do usuário
- Oferece suporte a qualquer token de hardware compatível com OATH
- Oferece uma trilha de auditoria abrangente para conformidade e análise forense

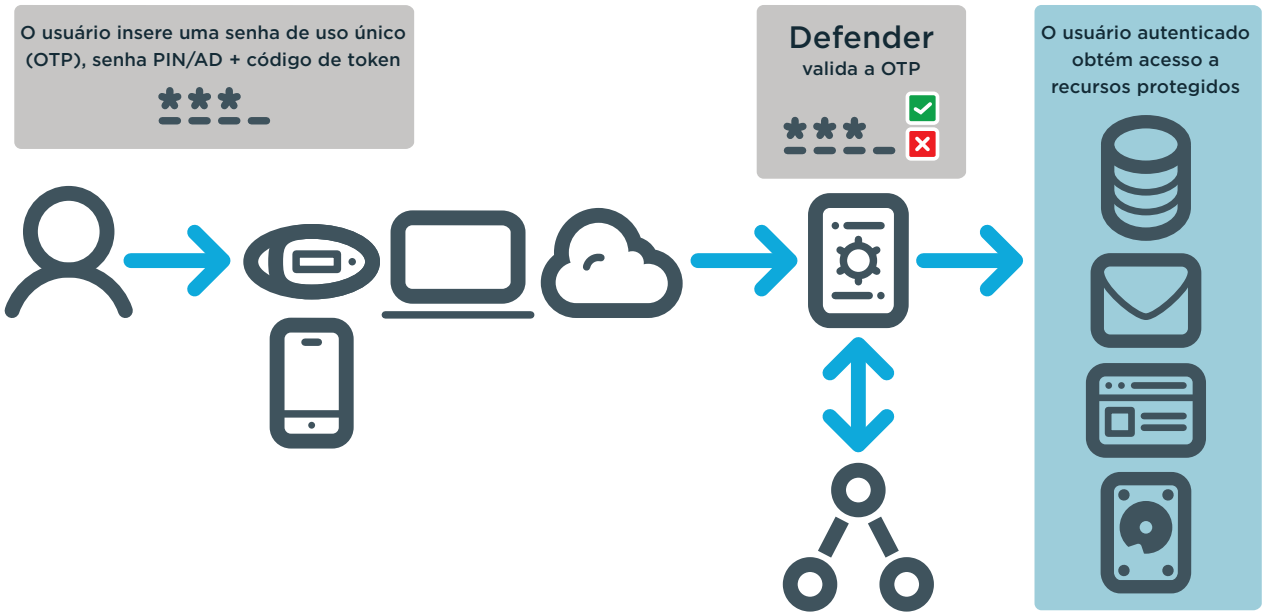
Requisitos do sistema

Para obter uma lista completa dos requisitos do sistema, acesse oneidentity.com/Defender

Hoje, exigências de conformidade e segurança levam as organizações a níveis de segurança além do nome de usuário e senha tradicionais. Autenticação por dois fatores: combinar "algo que você tem" (por exemplo, um token) com "algo que você sabe" (um nome de usuário e senha) ganhou destaque rapidamente nas iniciativas de conformidade e segurança da maioria das organizações. Tradicionalmente, as soluções de autenticação por dois fatores eram caras de serem implantadas e baseavam-se em interfaces e diretórios proprietários. Entretanto, o Defender® é totalmente baseado em padrões (OATH, RADIUS, Protocolo LDAP, PAM, etc.) e utiliza o Active Directory (AD) para administração e gerenciamento de identidades. Usar o AD não apenas aprimora a segurança e a escalabilidade, como também economiza dinheiro ao permitir que a equipe atual gerencie o Defender.

Além disso, o Defender permite que os usuários solicitem facilmente e autorregistrem com segurança tokens de hardware e software, o que reduz os custos e o tempo normalmente envolvidos na implantação da

ONE IDENTITY



O Defender aproveita os investimentos em infraestrutura de uma organização para aumentar a segurança de maneira flexível e econômica.

autenticação por dois fatores. O Defender oferece suporte a qualquer token de hardware compatível com OATH e também oferece vários tokens de software e baseados na Web. Ao usar os investimentos em infraestrutura da organização, fornecer ao usuário autorregistro e fornecer suporte a múltiplos tipos de token, o Defender permite que as organizações aumentem as medidas de segurança e a conformidade de maneira econômica e flexível.

Recursos

Centrado no Active Directory: use a escalabilidade, a segurança e a conformidade do Active Directory para fornecer autenticação por dois fatores a qualquer sistema, aplicativo ou recurso, além de aproveitar o diretório corporativo já estabelecido, em vez de criar um proprietário adicional. A atribuição de token de usuário é simplesmente um atributo adicional para propriedades de um usuário no Active Directory.

Administração baseada na Web: forneça aos administradores do Defender, ao Help Desk e aos usuários finais opções de gerenciamento e implantação de token, visualização de registro em tempo real, solução de problemas e acesso a relatórios com o Portal de gerenciamento do Defender baseado na Web.

Autorregistro de token: permita que os usuários solicitem tokens de hardware ou de software com base em uma política definida por administradores e que, em seguida, atribuam esse token às contas dos usuários de maneira rápida e fácil por meio de um mecanismo seguro.

Solução de problemas do Help Desk: permita que os administradores do Defender e do Help Desk solucionem, diagnostiquem e resolvam problemas relacionados à autenticação de usuários com apenas alguns cliques do mouse em qualquer navegador da Web. Visualize uma lista atual das tentativas de autenticação e das rotas com resultados associados, possíveis razões de falhas e etapas de resolução com apenas um clique. Além disso, visualize os detalhes da conta do usuário e os tokens atribuídos com a habilidade de testar ou redefinir rapidamente o PIN, fornecer uma resposta temporária de token ou redefinir ou desbloquear a conta.

Flexibilidade de token: implante qualquer token de hardware compatível com OATH do seu fornecedor de token preferencial. O Defender também oferece uma ampla variedade de tokens de software para as plataformas móveis mais populares e implantadas. Uma licença universal de token de software facilita a reemissão da licença adequada do dispositivo quando um usuário decide alternar plataformas móveis.

Acesso seguro ao webmail: permita o acesso seguro e baseado na Web para o seu sistema de e-mail corporativo

"Após anos de uso, o Defender mostrou ser uma solução sólida e eficiente. Não consigo me lembrar de uma vez em que ele tenha falhado. Ele é tão fácil de usar e passou a estar tão integrado ao que fazemos que não consigo pensar nele como uma solução separada."

Gregory Pronovost
Diretor assistente de TI
Cidade de Bakersfield

a partir de qualquer navegador da Web, a qualquer hora, em qualquer lugar, com o Webthority, uma solução de proxy reverso incluída no Defender. Além disso, você pode exigir o uso do token do Defender para o acesso para garantir a autenticação apropriada, independentemente do ponto de acesso.

Migração ZeroIMPACT: realize uma migração gradual para o Defender de uma solução de autenticação legada encarregada com o ZeroIMPACT. Com o Defender e o sistema legado em execução lado a lado, todas as solicitações de autenticação do usuário são direcionadas ao Defender. Se o usuário ainda não estiver definido no Defender, a solicitação de autenticação será transmitida de modo transparente por meio do recurso de proxy para a solução de autenticação atual. Essa abordagem permite aos administradores migrar usuários para o Defender conforme seus tokens legados expiram.

Administração centralizada: integre o Defender ao Active Directory e aproveite todas as vantagens do gerenciamento centralizado de informações do diretório por meio de uma interface do usuário comum e familiar. A atribuição de token do usuário é simplesmente um atributo adicional para as propriedades de um usuário no Active Directory que torna a administração de segurança mais eficiente.

Criptografia: proteja as comunicações ao associar um DES (Data Encryption Standard, Padrão de Criptografia de Dados) de gerenciamento ao Servidor de segurança do Defender. O Defender oferece suporte à criptografia AES, DES ou Triple DES.

Pluggable authentication module (PAM): especifique que os serviços e usuários definidos em seus sistemas UNIX/Linux sejam autenticados pelo Defender com seu módulo Defender para PAM.

Sobre o One Identity

A família One Identity de soluções de gerenciamento de identidades e acessos (IAM) oferece IAM para o mundo real, inclusive soluções centradas nos negócios, modulares e integradas preparadas para o futuro para governança de identidades, gerenciamento de acesso e gerenciamento privilegiado.

Saiba mais em OneIdentity.com

Datasheet-Defender-US-KJ-pt_BR-WL-25672

ONE IDENTITY