FOLHETO

Password Manager

Capacite os usuários, reduza os custos de suporte e reforce a segurança

Benefícios

- Reduz o envolvimento das equipes de TI e Help Desk no gerenciamento rotineiro de senhas
- Reduz substancialmente o tempo de inatividade dos usuários
- Fornece retorno imediato do investimento
- Aprimora a satisfação do usuário e da equipe de TI devido à facilidade de uso e implementação simples
- Aumenta a segurança da rede
- Permite a sincronização de senhas entre sistemas diferentes
- Integra-se à autenticação de múltiplos fatores do Defender para maior segurança

Visão geral

A maioria das solicitações enviadas ao Help Desk é para a redefinição de senhas. E, conforme as organizações buscam ter políticas de segurança mais sólidas, a dificuldade do gerenciamento de senhas fica cada vez maior. Exigir senhas mais complexas e que devem ser alteradas com mais frequência aumenta a probabilidade de elas serem esquecidas pelos usuários, o que faz com que eles tenham de ligar para o suporte. O problema aumenta à medida que as organizações aplicam senhas para múltiplos sistemas e aplicações diferentes. Como resultado, muitas organizações devem escolher entre o aumento da segurança e a redução de custos de suporte ao usuário.

O Password Manager é uma solução simples, segura e de autoatendimento que permite que os usuários finais redefinam senhas esquecidas e desbloqueiem suas contas. Ele permite que seus administradores implementem políticas de senha mais rígidas, ao mesmo tempo que reduz a carga de trabalho do Help Desk. Com o Password Manager, as organizações não precisam sacrificar a segurança para reduzir os custos.

Recursos

Aprimore a segurança

O Password Manager permite que as organizações adotem políticas de acesso a dados mais seguras, além do controle oferecido nativamente no Microsoft® Active Directory®. Ele aumenta a segurança ao eliminar erros do Help Desk, reduzir a necessidade de os usuários anotarem suas senhas e dificultar a adivinhação de senhas e invasões. A criptografia de dados integrada oferece suporte ao acesso global, ao mesmo tempo que mantém a segurança dos dados.

A participação dos usuários assegura o retorno do seu investimento

O Password Manager permite que os usuários lidem sozinhos com as tarefas mais básicas de senha, o que lhe permite economizar orçamento de TI e obter um rápido retorno do seu investimento.

Faça um investimento inteligente

O Password Manager é uma solução de longo prazo para um problema em crescimento. Ele é um investimento inteligente para qualquer empresa que busca aumentar a eficiência operacional da equipe de TI e aprimorar a segurança.

- Custo-benefício no uso da infraestrutura do Active Directory: o Password Manager permite que você aproveite ainda mais a sua infraestrutura do Active Directory. Também é possível implementá-lo rapidamente e

obter ROI imediato. Além disso, ele fornece uma política de senha baseada em grupo mais granular do que a do Windows Server.

- Redução da carga de trabalho e custo do Help Desk, além do aumento da produtividade do usuário: com o Password Manager, os usuários podem redefinir suas próprias senhas e desbloquear suas contas sem envolver o Help Desk ou o suporte administrativo.
- Ajuda ao usuário sob demanda: o Password Manager fornece explicações de políticas de senha on-line. Além disso, ele oferece automaticamente um feedback para os usuários quando as regras de configuração de senha não são atendidas e pode gerar senhas compatíveis para os usuários sem a assistência do Help Desk.
- Extensões GINA para caixa de diálogo de login do Windows: para simplificar redefinições de senha aos usuários, os administradores podem fazer com que a tela de login no Windows exiba um botão para redefinir as senhas antes do login. Isso elimina a necessidade de configurar quiosques públicos ou sistemas telefônicos caros.

Aplique padrões organizacionais

O Password Manager é compatível com o maior número possível de políticas organizacionais e padrões de segurança de dados.

- Aplicação rigorosa de política: o Password Manager impõe padrões definidos pelo administrador, registra as tentativas de autenticação sem sucesso e bloqueia as contas correspondentes, se necessário.
- Inscrição garantida: o Password Manager fornece vários mecanismos que garantem que os usuários se inscrevam e utilizem o software, o que garante sua eficácia.
- Autenticação confiável: os perfis pessoais de perguntas e respostas dos usuários contêm perguntas com respostas únicas que são fáceis de serem lembradas pelos usuários, mas difíceis de serem adivinhadas por outras pessoas. Além disso, o Password Manager pode ser implementado com o Defender para solicitar uma autenticação por senha de uso único (OTP) mais segura com o perfil de perguntas e respostas (ou como um substituto).
- Segurança e simplicidade: o Password Manager integra-se perfeitamente ao Windows, o que lhe permite atender aos usuários de múltiplos domínios, com ou sem relações de confiança. A criptografia de dados eficiente e a comunicação segura são fornecidas por meio do suporte a tecnologias de segurança líderes, como SHA-256 e CryptoAPI da Microsoft.

Monitore a atividade do sistema

O Password Manager fornece aos administradores recursos sólidos de registro e relatórios, o que facilita o monitoramento da atividade do sistema e a correção de eventuais irregularidades.

Ofereça suporte a iniciativas de gerenciamento de identidade

O Password Manager possui uma interface Web com grande capacidade de resposta e oferece suporte de gerenciamento de senhas para qualquer sistema conectado ao Microsoft Identity Integration Server (MIIS). Ele também se estende aos sistemas operacionais que não são da Microsoft, como Unix e Linux, com o Authentication Services, além da adição de autenticação de dois fatores pelo Defender.

Assinatura híbrida do One Identity

Expanda os recursos do Password Manager com a Assinatura híbrida do One Identity que oferece recursos e serviços adicionais oferecidos pela nuvem. Obtenha acesso à Autenticação de dois fatores Starling para proteger o acesso administrativo e de usuário final no Password Manager ao substituir o Suplemento de verificação por telefone. Uma única assinatura permite todas as implementações da solução One Identity.

Sobre o One Identity

O One Identity, um software de negócio da Quest, permite que as organizações implementem uma estratégia de segurança centrada na identidade, seja ela no local, na nuvem ou em um ambiente híbrido. Com nosso portfólio integrado e amplo de ofertas de gerenciamento de identidade, incluindo gerenciamento, governança de identidades e gerenciamento de acessos privilegiados e de administração, as organizações podem alcançar todo o seu potencial nos locais em que a segurança foi implementada ao colocar as identidades no centro do programa, habilitar acesso adequado em todos os tipos de usuários, sistemas e dados. Saiba mais em OneIdentity.com.

Datasheet_2019_PasswordManager_US_RS_55939