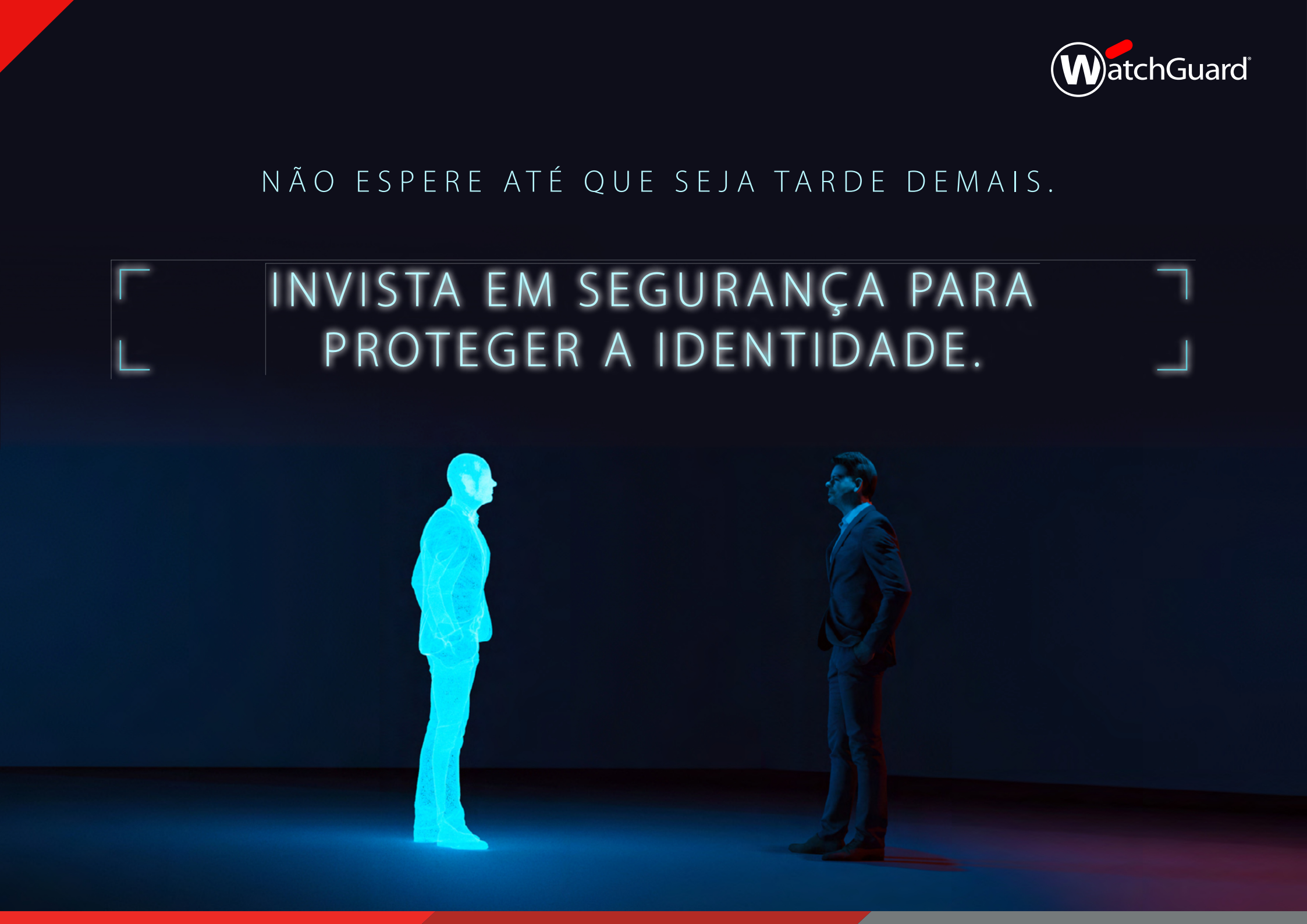
WatchGuard

NÃO ESPERE ATÉ QUE SEJA TARDE DEMAIS.

INVISTA EM SEGURANÇA PARA PROTEGER A IDENTIDADE.



Basta uma senha fraca para sofrer uma

… Até mesmo suas senhas "complexas" podem ser decodificadas.
O uso de senhas não é mais suficiente para manter seus ativos, contas e informações seguros.

Estas são algumas das evidências do porquê:

No ano de 2021, 82% das violações envolveram elementos humanos, incluindo credenciais roubadas.[1]

51% das pessoas usam a mesma senha para contas empresariais e pessoais.[2]

Em geral, as pessoas escolhem **senhas fracas**.

Veja a Lista das 20 Senhas Mais Comuns em Violações Encontradas na Dark Web[3]:

1. 123456
2. 123456789
3. Qwerty
4. Senha
5. 12345
6. 12345678
7. 111111
8. 1234567
9. 123123
10. Qwerty123
11. 1q2w3e
12. 1234567890
13. PADRAO
14. 0
15. Abc123
16. 654321
17. 123321
18. Qwertyuiop
19. Iloveyou
20. 666666

Não é Difícil que as Senhas Caiam nas Mãos Erradas

Na dark web, um conjunto completo de credenciais custa entre US$ 8 e US$ 25,[4] o que torna a violação de sistemas um empreendimento barato e fácil. E se isso não funcionar, um cibercriminoso habilidoso pode quebrar as senhas da maioria das pessoas no tempo que você leva para ler a lista de senhas na página anterior.[5]

As senhas são fáceis de roubar e fornecem apenas uma linha de defesa. Caso um hacker consiga roubar a senha de apenas um funcionário, normalmente poderá acessar toda a sua rede. Depois de entrar, ele pode fazer o que quiser. Em geral, isso significa espalhar malwares ou roubar, modificar e excluir informações essenciais.

É Fácil Roubar sua Senha

O processo de roubar uma senha é assustadoramente fácil (e rentável) para os hackers. As ferramentas e tecnologias de detecção de senhas estão se tornando exponencialmente mais sofisticadas e automatizadas a ponto de não ser mais necessário "adivinhar" as senhas de forma manual. Mesmo quando necessário, algoritmos avançados, engenharia social (como ataques de phishing e Cavalos de Troia), atividades de keylogging e outros métodos permitem detectar e testar de maneira eficiente as senhas mais prováveis, e costumam ser bem-sucedidos.

Entre os métodos comuns para roubar senhas estão:

Ataque de dicionário

Os hackers tentam adivinhar a senha digitando uma lista comum de palavras de um "dicionário" de senhas. Os dicionários de senhas mais avançados incluem listas das palavras mais comuns usadas nas senhas. É um método relativamente simples, mas eficaz apenas para detectar senhas menos complexas. Se você usa palavras reais em qualquer uma das senhas, suas credenciais estão vulneráveis.

Ataque de força bruta

Embora não seja tão eficaz quanto um ataque de dicionário, o ataque de força bruta é mais eficiente para, eventualmente, adivinhar qual é a senha. Nesse método, os hackers usam ferramentas para testar repetidamente cada combinação possível de letras, números e símbolos da senha até decodificá-la. Outra abordagem parecida é o ataque de força bruta reversa, em que o hacker testa uma senha com vários nomes de usuário.

Ataque do tipo "rainbow"

Esse método usa uma tabela de consulta de hashes para decodificar hashes de senha (basicamente, senhas embaralhadas armazenadas nos bancos de dados dos sistemas) com mais eficácia do que os ataques de dicionário e força bruta.

Ataque de credencial stuffing (preenchimento de credenciais)

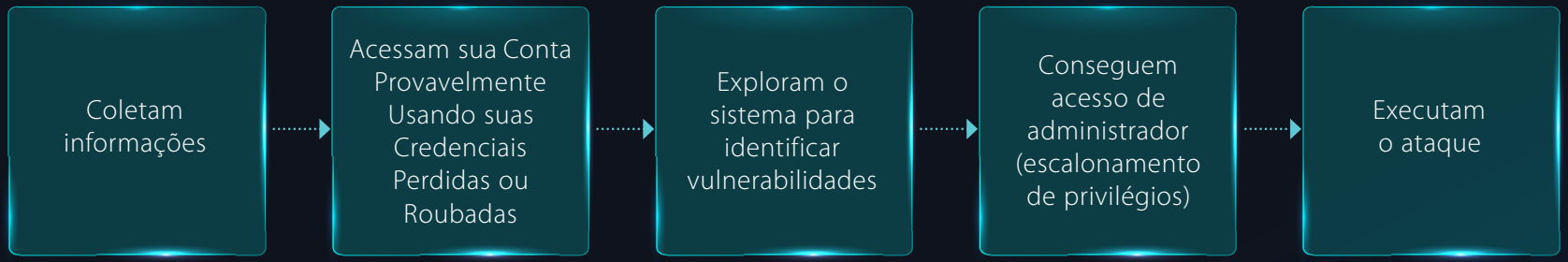
Como muitas pessoas usam as mesmas senhas ou variações das senhas em diversas contas, os hackers encontraram um jeito de executar automaticamente listas de bancos de dados contendo combinações de nome de usuário e senha violados no login de um site visado. Segundo a Shape Security, 90% das tentativas de login em sites de lojas são provenientes desse tipo de ataque, e o método é eficaz para os hackers em aproximadamente 3% das vezes.

Engenharia social

Esta abordagem tem diferentes estilos, todos eles vinculados à ideia de enganar ou manipular pessoas para que forneçam suas informações ou realizem determinada ação. Entre os métodos comuns de engenharia social usados para roubar senhas estão ataque de phishing e Cavalo de Troia. Uma abordagem menos comum é olhar sobre o ombro (shoulder surfing), em que o hacker simplesmente observa o usuário digitar a senha.

Com mais sofisticação nas tecnologias e nas ferramentas dos hackers, a etapa mais simples da invasão costuma ser decodificar a senha. Na verdade, é tão fácil que muitas vezes sequer envolve suposição. A parte mais assustadora é que, não importa o nível de segurança da senha, basta que a senha de um colega seja fraca para colocar todo o sistema da empresa em risco de violação.

Hackers ganham dinheiro com credenciais perdidas ou roubadas ao possibilitar o roubo de dados ou o acesso a sistemas empresariais nos quais ransomware ou outros ataques de malware lucrativos podem ser executados. Roger Grimes, especialista em segurança de computadores e hacker ético (também conhecido como white hat), descreve esse processo no seu livro *HackingtheHacker*.



De acordo com Grimes:

> Se o hacker tiver feito seu dever de casa na etapa de identificação, esta etapa não será nem um pouco difícil.

Ou seja, os hackers conseguem acessarem suas contas facilmente. Alguns deles até cobrem os rastros ou criam uma porta dos fundos para acesso futuro, embora nem sempre seja o caso.

Como garantir que a pessoa com a senha é realmente quem ela diz ser? Como você pode manter a identidade real?

Os especialistas independentes e de agências governamentais do mundo todo oferecem conselhos valiosos sobre como proteger sistemas empresariais contra ataques. Segundo um alerta recente das autoridades de cibersegurança dos EUA, da Nova Zelândia, do Canadá, dos Países Baixos e do Reino Unido, fortalecer as credenciais com o uso de MFA e políticas de senha eficazes são práticas recomendadas contra o aumento dos ciberataques.[6] Não estamos falando de qualquer tipo de proteção de identidade e credenciais. À medida que os criminosos estão se tornando mais sofisticados, nossas soluções de segurança também estão. Por exemplo, em agosto de 2021, a CISA adicionou a autenticação de fator único à lista de Práticas de cibersegurança desaconselhadas,[7] uma mensagem clara para todas as organizações que confiam exclusivamente em senhas para proteção.

Muitas Organizações Tentaram Promover uma Mudança de Comportamento dos Funcionários em Relação às Senhas

Um método para diminuir o risco de roubo de senhas é treinar os funcionários para criar senhas mais complexas e redefini-las com mais frequência. Contudo, mudar o comportamento de cada um dos funcionários não é apenas desafiador, mas ineficaz neste caso.

Historicamente, a abordagem não funciona

Isso foi comprovado pelas milhões de empresas cujos bancos de dados foram invadidos e por dezenas de milhões de senhas vazadas que foram disponibilizadas on-line (podendo ser compradas na dark web).

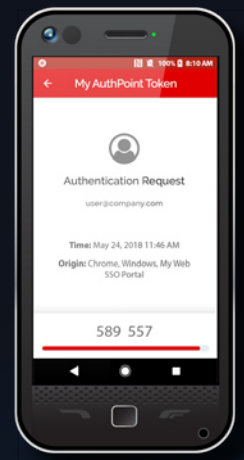
A experiência do usuário se torna complexa demais

Usar senhas únicas, totalmente aleatórias, de 16 caracteres em cada conta é complicado. O motivo para as pessoas usarem senhas simples é que as senhas são difíceis de memorizar. Muitos usuários criam algumas um pouco mais complexas, mas atenuam essa complexidade reutilizando a mesma senha (ou variações dela) em outras contas.

Se não é suficiente usar senhas, o que fazer?

A autenticação multifator (MFA) adiciona uma camada extra de segurança aos logins, além do simples nome de usuário e senha. Ela ajuda a garantir que os hackers não acessem seus sistemas se uma das senhas dos seus funcionários for comprometida. A abordagem multifator é mais vantajosa do que a autenticação de fator único principalmente por incluir o seguinte:

- Algo que você tem *(token, celular)*
- Algo que você sabe *(senha, PIN)*
- Algo que você é *(impressão digital, reconhecimento facial)*



Advertência: Nem Todas as Soluções de MFA são Criadas da Mesma Maneira

A autenticação multifator por SMS não é mais um método seguro e confiável. Os usuários com autenticação por SMS devem migrar para outros métodos imediatamente. Nas Diretrizes de identidade digital de 2016, o National Institute of Standards and Technology (NIST) encorajou os usuários a deixarem de usar a autenticação por SMS:

"Devido ao risco que mensagens SMS ou chamadas de voz têm de serem interceptadas ou redirecionadas, quem implementa novos sistemas precisa considerar com cuidado autenticadores alternativos. A autenticação fora de banda usando [SMS ou voz] está suspensa e sua remoção de edições futuras desta diretriz está sendo considerada."

A Harvard Business Review foi além, declarando: "pode ser argumentado que a autenticação por SMS se tornou mais um vetor de ataque do que uma medida de segurança".

O motivo pelo qual a autenticação por SMS é arriscada é que as mensagens de texto são vulneráveis à interceptação. O Reddit foi uma vítima notória disso em 2018. Ele publicou um comentário sobre o ataque no próprio site atribuindo a invasão à fraqueza da autenticação por SMS: "Descobrimos que a autenticação baseada em SMS não é tão segura quanto gostaríamos, e o ataque principal foi via interceptação de SMS. Estamos frisando isso para incentivar todos a usarem autenticação de dois fatores baseada em token.

Embora a MFA por SMS seja melhor do que confiar apenas em um nome de usuário e senha, ela ainda deixa os usuários vulneráveis a invasões por hackers. Para diminuir o risco, as empresas devem contar com MFA que use apenas métodos mais fortes de autenticação.

Proteger a Senha Também é Importante!

Embora a MFA já ajude muito, as senhas ainda são consideradas na validação de identidades. Por isso, os especialistas em cibersegurança também recomendam o fortalecimento e o monitoramento das credenciais. Em especial, um produto como um gerenciador de senhas de nível empresarial é uma proposta vantajosa para diversas empresas. Além de promover o uso de senhas complexas e únicas, ele oferece aos usuários uma ferramenta a ser acessada e usada para relembrar as senhas com facilidade e segurança quando necessário. Melhor ainda, o gerenciador de senhas e a MFA podem ser implantados e gerenciados juntos para oferecer uma solução eficaz que atenda aos requisitos específicos das empresas.

Com o forte comércio de credenciais perdidas/roubadas na dark web, o serviço de monitoramento também pode fornecer às empresas um tempo valioso de resposta ao avisá-las sobre a violação antes que as credenciais envolvidas sejam usadas em um ataque.

No pacote AuthPoint Total Identity Security, a WatchGuard oferece uma solução de autenticação multifator fácil de usar com um gerenciador de senhas corporativas e um serviço de monitoramento da dark web.

Como funciona o AuthPoint Total Identity Security?

O AuthPoint MFA é um serviço de autenticação multifator (MFA) que ajuda as empresas a manter seus ativos, informações e identidades de usuários seguros. Ele exige que os usuários apliquem dois ou mais fatores de autenticação para fazer login, em vez de confiar apenas em uma senha. Além disso, o Total Identity Security inclui nosso gerenciador de senhas corporativas e um serviço de monitoramento da dark web. O pacote oferece o seguinte:

Várias camadas de autenticação

As empresas podem reduzir significativamente o risco de invasão às suas contas. Se um hacker conseguir a senha de um funcionário, ainda haverá outra camada de segurança para impedir a invasão.

Gerenciamento no WatchGuard Cloud: uma única interface para facilitar a administração

Os produtos AuthPoint Total Identity Security são totalmente gerenciados no Cloud. Assim, não é preciso implementar hardwares nem atualizar softwares caros.

Satisfação do usuário e adesão simplificada

Os usuários aprovam ou negam logins com um só toque no aplicativo móvel AuthPoint. Depois de estarem conectados, os usuários utilizam o single sign-on (SSO) para acessar aplicativos e ambientes com rapidez. Melhor ainda, o gerenciador de senhas corporativas está disponível no aplicativo AuthPoint e pode ser usado para senhas corporativas e pessoais.

Uma solução feita para empresas

Ao contrário de tokens e gerenciadores de senhas criados para consumidores, o AuthPoint foi desenvolvido especialmente para os casos de uso corporativos. Por exemplo, ele autentica os usuários na inicialização do Windows/macOS, incluindo o acesso on-line e off-line. Isso quer dizer que os usuários poderão fazer login com segurança mesmo se acessarem suas contas no avião.

A proteção avançada está disponível por menos do que você paga por seu cappuccino matinal

Você colocaria sua empresa em risco apostando na segurança da senha de cada funcionário? Invista na segurança da identidade com o AuthPoint. Ele é econômico, poderoso e fácil de usar.

Invista na segurança da identidade com o WatchGuard AuthPoint

WatchGuard

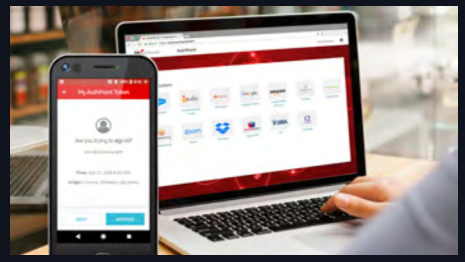
Portfólio da WatchGuard

Segurança de Rede

As soluções de segurança de rede da WatchGuard foram projetadas desde o início para oferecer implantação, uso e gerenciamento simplificados – com o maior nível de segurança possível. O foco da nossa abordagem exclusiva à segurança de rede é oferecer a melhor segurança da categoria, de nível corporativo, para qualquer organização, independentemente do tamanho ou do conhecimento técnico.

Wi-Fi Seguro

As soluções de Wi-Fi Seguro da WatchGuard são verdadeiras revoluções no mercado atual. Elas foram criadas para oferecer um espaço aéreo seguro e protegido para ambientes de Wi-Fi, ao mesmo tempo em que eliminam problemas administrativos e reduzem muito o custo. Com ferramentas de envolvimento expansivas e visibilidade da análise do negócio, a tecnologia oferece a vantagem competitiva necessária para que as empresas tenham sucesso.



Autenticação Multifator

O WatchGuard AuthPoint® é a solução certa para preencher a lacuna da segurança baseada em senhas por meio da autenticação multifator em uma plataforma na nuvem fácil de usar. A abordagem exclusiva da WatchGuard acrescenta o "DNA do telefone celular" como um fator de identificação para assegurar que somente a pessoa correta tenha acesso a redes confidenciais e a aplicativos em nuvem.

Segurança de Endpoint

A Segurança de Endpoint da WatchGuard é um portfólio de segurança de endpoint avançado e nativo em nuvem. Ela protege empresas de todos os tipos contra ciberataques atuais e futuros. A principal solução, o WatchGuard EPDR tem tecnologia de inteligência artificial e melhora imediatamente a postura de segurança das organizações. O produto combina recursos de Proteção de Endpoints (EPP) e Detecção e Resposta (EDR) com Serviços de Aplicação Zero Trust e Threat Hunting.

Referências:

1. https://www.verizon.com/business/resources/reports/dbir/
2. https://www.spiceworks.com/it-security/identity-access-management/news/world-password-day-2022/)
3. https://www.cnbc.com/2022/02/27/most-common-passwords-hackers-leak-on-the-dark-web-lookout-report.html
4. https://www.securitymagazine.com/articles/94405-a-look-into-the-pricing-of-stolen-identities-for-sale-on-dark-web
5. https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity
6. https://www.cisa.gov/uscert/ncas/alerts/aa22-137a
7. https://www.cisa.gov/uscert/ncas/current-activity/2021/08/30/cisa-adds-single-factor-authentication-list-bad-practices

Sobre a WatchGuard

A WatchGuard® Technologies, Inc. é líder global em cibersegurança unificada. Nossa abordagem de Plataforma de Segurança Unificada® foi criada exclusivamente para que os provedores de serviços gerenciados forneçam segurança de ponta que aumenta a escala e a velocidade dos negócios, além de melhorar a eficiência operacional. Adotados em todo o mundo por mais de 17 mil parceiros de segurança e prestadores de serviços para proteger mais de 250 mil clientes, os premiados produtos e serviços da empresa incluem segurança e inteligência de rede, proteção avançada de endpoint, autenticação multifator e Wi-Fi seguro. Juntos, eles oferecem uma plataforma de segurança com cinco elementos indispensáveis: segurança abrangente, conhecimento compartilhado, clareza e controle, alinhamento operacional e automação. A WatchGuard tem sua sede em Seattle, no estado de Washington, nos EUA, e escritórios na América do Norte, Europa, Ásia-Pacífico e América Latina. Para saber mais, acesse WatchGuard.com/br.

VENDAS NO BRASIL (11) 3164-3031 São Paulo / (41) 3073-1663 Curitiba WEB www.secureone.com.br