

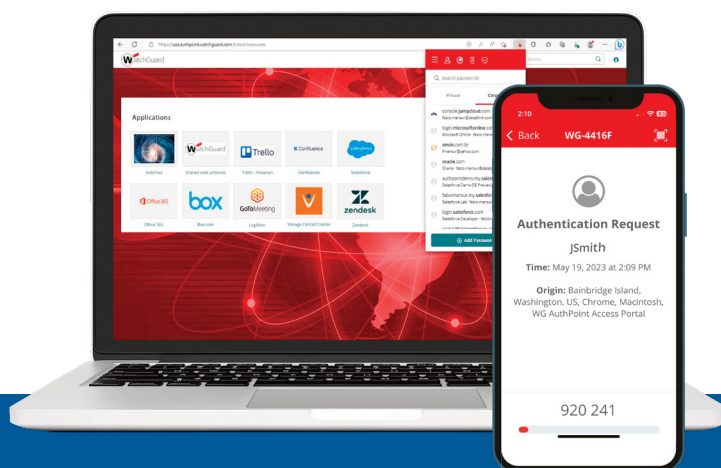
# AuthPoint Identity Security

Simple e único. Poderoso e seguro.

Apenas uma credencial comprometida já é suficiente para prejudicar seriamente ou até mesmo suspender as atividades de uma organização. A segurança de identidade precisa ser a primeira linha de defesa contra ciberataques.

O AuthPoint Identity Security fornece a segurança de que você precisa para proteger ativos, contas, informações e identidades de usuários. Com soluções de gerenciamento de credenciais e autenticação multifator econômicas, abrangentes e fáceis de usar, os funcionários da sua empresa poderão trabalhar de maneira confiável e sem preocupações. Além disso, atenda aos requisitos de Seguro Cibernético, conformidade e estruturas de segurança relacionados à autenticação de usuários e controle de acesso.

- Ofereça acesso remoto seguro com redes privadas virtuais (VPNs)
- Proporcione uma experiência integrada aos funcionários com tecnologia de segurança simples de usar
- Obtenha conformidade regulatória e atenda aos requisitos de Seguro Cibernético



*“O AuthPoint cumpre o que a MFA promete ao limitar o risco associado ao uso de senhas fracas sem dificultar o uso para funcionários e equipes de TI.*

*Tudo em um serviço de nuvem, sem precisar instalar hardware ou gerenciar software... Hoje, a MFA é considerada essencial para sua proteção. Uma solução simples e descomplicada da WatchGuard.”*

Tom Ruffolo  
CEO, eSecurity Solutions

## Principais Desafios das Empresas com as Identidades da Força de Trabalho



82%

Percentual de violações de dados que envolveram um elemento humano. O fator predominante são as pessoas.



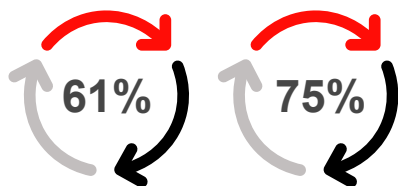
27

27 é a média do número de senhas que um funcionário médio precisa lembrar.



55%

Percentual de empresas que seguirão oferecendo suporte a postos de trabalho híbridos/remotos.



Corporações X Pequenas e Médias Empresas

Percentual de violações de dados que envolveram o uso de credenciais roubadas.



Local de Trabalho X Trabalho Remoto

Índices de reutilização de senhas em aplicativos e serviços



Percentual de empresas que planejam terceirizar a segurança e aumentar os controles de autenticação/acesso.

## Soluções do AuthPoint Identity Security

Mitigue os riscos associados aos ataques generalizados às credenciais da força de trabalho

### Autenticação Multifator (MFA): Estabeleça uma Verificação Consistente do Usuário

O AuthPoint MFS foi projetado para ser resistente à fadiga, o que permite medidas de autenticação mais eficientes com recursos como o toggle de phishing que impedem uma experiência de usuário problemática. Nossa VPN rápida e fácil de implantar e acesso remoto fornecem caminhos seguros com o mínimo de esforço. Com os métodos de autenticação off-line e on-line disponíveis, você garante que seu sistema sempre tenha uma segurança robusta com facilidade. Além disso, o amplo ecossistema de integrações e o padrão SAML fornecem acesso completo, dando às organizações a capacidade de controlar os privilégios de acesso de usuários de maneira rápida e eficaz.



### Gerenciador de Senhas Corporativas: Otimize a Segurança das Senhas e a Experiência do Usuário

O Gerenciador de Senhas Corporativas fornece às empresas mais controle sobre a qualidade das senhas, reduz a necessidade de redefini-las e atenua problemas relacionados à sua reutilização, compartilhamento ou roubo. As senhas criadas com um gerenciador são virtualmente impossíveis de decodificar, mas não fornecem os recursos que as empresas precisam. Com o Gerenciador de Senhas Corporativas da WatchGuard, quando os usuários precisarem acessar os aplicativos ou sistemas, poderão recuperar as senhas corporativas, pessoais e de cofres compartilhados por meio do aplicativo e/ou da extensão do navegador do AuthPoint. Com isso, as empresas adicionam aplicativos em nuvem sem SAML ao Portal de SSO na web para uma autenticação mais forte e uma experiência estável de SSO.



### Monitoramento da Dark Web: Tome Medidas Quando as Credenciais Caírem nas Darknets

O Monitoramento da Dark Web é um serviço proativo que notifica os clientes quando credenciais comprometidas de domínios monitorados são encontradas em um banco de dados de credenciais recém-adquirido publicado em nosso serviço. As notificações podem ser enviadas aos usuários envolvidos na violação e aos administradores, para que os usuários possam alterar a própria senha de maneira proativa. Com apenas uma licença, é possível monitorar até três domínios.

## Hackers Não Invadem – Eles Fazem Login

O AuthPoint Permite um Ambiente de Acesso Adaptativo com Mais Produtividade e Menos Gastos



### Estrutura de Risco Zero-Trust

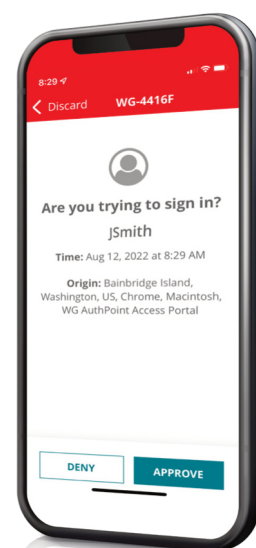
A adoção de zero-trust não pode acontecer sem a segurança de identidade. As Nossas políticas de acesso baseadas em risco permitem o acesso do usuário certo no momento certo. O AuthPoint fornece autenticação personalizável e políticas de risco sem custo adicional, incluindo recursos de rede, tempo, delimitação geográfica e geokinetics.

### Ampla Cobertura com SSO (Autenticação Única)

A segurança do AuthPoint com SSO (Autenticação única) facilita o acesso dos usuários a múltiplos aplicativos na nuvem, VPNs e redes com apenas um conjunto de credenciais. Isso combate os desafios apresentados pela sobrecarga de senhas e reduz o risco de vulnerabilidades de segurança devido a senhas fracas e custos associados à redefinição de senhas.

### Baixo Custo Total de Propriedade (TCO)

Empresas com recursos limitados de TI e segurança se beneficiam de uma proteção de MFA que é fácil de implantar e gerenciar pela nuvem. Não importa se você implantou apenas MFA ou apenas o Total Identity Security, o AuthPoint oferece uma estrutura de preços completa por usuário, por mês, para que as empresas adotem totalmente as medidas de segurança de identidade sem custo adicional.



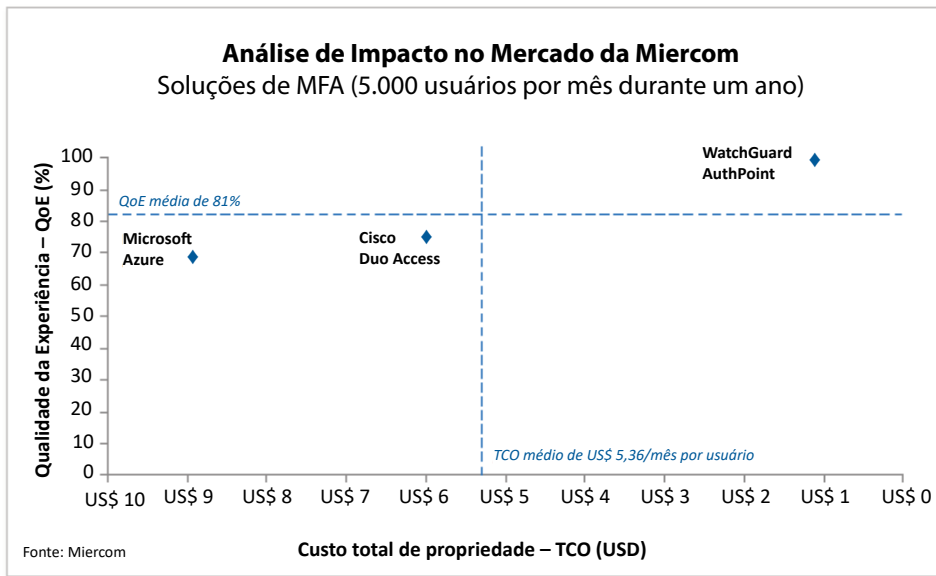


## Validação Técnica da Miercom

A Miercom, um laboratório de TI que fornece validação de terceiros, concedeu à solução AuthPoint MFA da WatchGuard a certificação Performance Verified. A avaliação testou o AuthPoint e validou sua usabilidade e desempenho em comparação com as MFAs do Cisco Duo e do Azure.

## Alto Valor e ROI Competitivo

A WatchGuard demonstrou ter o maior valor com a qualidade de sua experiência. A WatchGuard ofereceu um amplo conjunto de recursos nativos em uma compra única, enquanto outras soluções além de terem maior complexidade e custo, exigiam a compra de assinaturas extras.



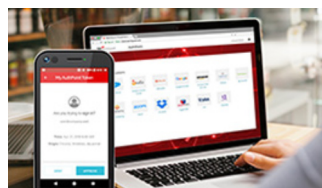
Os quadrantes são formados com base nos valores médios. A WatchGuard aparece no quadrante superior direito, mostrando que teve a qualidade da experiência (QoE) mais alta com o custo mais baixo em comparação aos fornecedores da concorrência. A Cisco e a Microsoft não ofereceram a mesma quantidade de funcionalidades, facilidade de uso nem interface intuitiva que a WatchGuard.

## O PORTFÓLIO WATCHGUARD



### Segurança de Rede

A WatchGuard oferece uma ampla variedade de soluções de segurança de rede, incluindo modelos de mesa e appliances 1U, até firewalls virtuais e na nuvem. Nossos appliances Firebox® oferecem serviços de segurança essenciais, desde IPS padrão, filtragem de URL, gateway AV, controle de aplicativos e antispam até proteções avançadas, como sandboxing de arquivos, filtragem de DNS e muito mais. Com deep packet inspection (DPI) de alto desempenho, você pode aproveitar todos os nossos serviços de segurança contra tentativas de ataques escondidas em canais criptografados, como HTTPS. Além disso, cada Firebox oferece SD-WAN pronto para usar, melhorando a resiliência e o desempenho da rede.



### Segurança de Identidade

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. O AuthPoint também oferece uma experiência de usuário otimizada com métodos de autenticação on-line e off-line, além de um portal de aplicativos web para permitir um fácil acesso de logon único.



### Wi-Fi Seguro na Nuvem

As soluções de Wi-Fi seguras e gerenciadas na nuvem da WatchGuard fornecem um espaço aéreo seguro e protegido para ambientes de Wi-Fi, eliminando problemas administrativos e reduzindo significativamente o custo. De home offices a amplos ambientes corporativos, a WatchGuard oferece tecnologia Wi-Fi 6 com criptografia WPA3 segura. Com o WatchGuard Cloud, diversos recursos ficam a apenas um clique de distância: configuração e administração de políticas da rede Wi-Fi, implantação sem contato, portais de login personalizados, configuração de VPN, ferramentas amplas de envolvimento, visibilidade da análise empresarial e atualizações.



### Segurança de Endpoint

As soluções de Segurança de Endpoint da WatchGuard ajudam você a proteger os dispositivos contra ciberameaças. O WatchGuard EPDR e o WatchGuard Advanced EPDR, nossas principais soluções de endpoint com tecnologia de IA, aprimoram a sua postura de segurança ao integrar recursos de proteção de endpoint (EPP), detecção e resposta (EDR) e nossos serviços de Aplicação Zero-Trust e Busca de Ameaças. Tudo isso está integrado ao WatchGuard Cloud e ao ThreatSync, fornecendo visibilidade e inteligência valiosas, além de aumentar a detecção e resposta entre produtos (XDR).

## 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](http://WatchGuard.com/br).