As Seis Categorias Conhecidas de Ameaças de Wi-Fi que Visam sua Empresa e Como se Defender Delas

WatchGuard

Índice

O crescimento do Wi-Fi

O acesso Wi-Fi se tornou um estilo de vida. De dispositivos móveis a notebooks, videogames e aparelhos domésticos, quase tudo que você pode imaginar precisa de uma conexão sem fio. Na verdade, o número de dispositivo conectados deve ultrapassar 20,4 bilhões até 2020, de acordo com a Gartner.

Também vimos um enorme crescimento no número de pessoas que usam smartphones, com um salto de 35% em 2011 para 77% em 2018[1]. Como seus clientes e funcionários estão fazendo roaming com seus smartphones e outros dispositivos com conexão sem fio, você precisará oferecer a eles um acesso robusto. Mas e quanto aos riscos de segurança inerentes associados à Wi-Fi? Você pensou sobre as ameaças que estão à espreita só esperando que alguém se conecte para que elas possam roubar suas informações? .

Vamos dar uma olhada nas maiores ameaças sem fio que afetaram empresas exatamente com as suas nos últimos anos.

O número de **dispositivos conectados** deve **ultrapassar 20,4 bilhões** até **2020**, de acordo com a Gartner.

1. https://www.securedgenetworks.com/blog/wi-fi-planning-preparing-for-growth-in-a-mobile-first-world

Invasões de Wi-Fi notáveis

A **TJ Maxx** sofreu uma violação em julho de 2015 que foi o resultado de uma rede sem fio insegura. O hacker se instalou nas proximidades da empresa em St. Paul, no estado americano de Minnesota, com um notebook e uma antena em forma de telescópio, baixando pelo menos 45,7 milhões de números de cartão de crédito e débito, mas podendo ter obtido acesso a cerca de 200 milhões de números de cartão no total.[2]

Em um relatório da CNBC de dezembro de 2017, a **Starbucks** havia tomado as medidas necessárias para evitar que notebooks de clientes fossem usados para gerar criptomoedas. O Wi-Fi em uma de suas unidades em Buenos Aires foi invadida por hackers e modificada com um código incomum. Depois que um usuário se conectava, o provedor de conexão Wi-Fi conseguia usar o poder de processamento do cliente para minerar bitcoins[3]. .

Em março de 2018, vários oficiais de Atlanta foram vítimas de um ataque de ransomware SamSam que criptografou os arquivos em seus dispositivos. Para evitar a que o ransomware se espalhasse através da rede Wi-Fi, o Aeroporto Internacional de Atlanta, Hartsfield-Jackson, foi forçado a desativar o acesso a seus serviços de Wi-Fi. A decisão rápida da equipe de segurança em Atlanta possivelmente impediu que seus passageiros fossem infectados![4]

Então quais são as ameaças que podem atacar sua empresa e com as quais você precisa se preocupar?

2. https://www.zdnet.com/article/tjxs-failure-to-secure-wi-fi-could-cost-1b/

3. https://www.cnbc.com/2017/12/12/starbucks-customer-laptops-hacked-to-mine-cryptocurrency.html

4. https://www.secplicity.org/2018/03/23/the-worlds-busiest-airport-shuts-off-wi-fi-amid-a-ransomware-attack/

As seis categorias conhecidas de ameaças de Wi-Fi que visam sua empresa

Embora a lista de potenciais ameaças de Wi-Fi possa parecer infinita, há 6 categorias conhecidas contra as quais você precisa proteger sua empresa. Na próxima seção, abordaremos cada uma dessas categorias, como elas são, como funcionam e um exemplo da vida real que pode estar acontecendo na sua empresa neste exato momento.

Access point Evil Twin

O QUÊ

Um AP Evil Twin imita um AP legítimo falsificando seu SSID e endereço MAC exclusivo. Assim, os invasores podem interceptar o tráfego e inserir-se na troca de dados entre a vítima e os servidores que ela acessa enquanto está conectada ao access point Evil Twin.

COMO

Depois que a vítima se conecta, o invasor pode roubar credenciais, injetar códigos maliciosos nos browsers da vítima, redirecionar a vítima para um site de malware e muito mais.

EXEMPLO

No seu horário de almoço, você decide que finalmente é hora de atualizar seu guarda-roupa – não há nada de errado nisso! Mas um hacker está usando um access point Evil Twin e você se conectou sem saber à cópia dele do seu SSID de Wi-Fi. Quando você fizer o pagamento e digitar as informações do seu cartão crédito para comprar aquele vestido novo, o hacker terá suas informações e estará pronto para vendê-las na dark web.

Access point mal configurado

O QUÊ

Em redes ocupadas onde novos APs estão sendo implantados, é muito provável que os administradores de rede acidentalmente cometam um erro de configuração, como tornar aberto um SSID privado, sem nenhuma criptografia, expondo potencialmente informações confidenciais à interceptação pelo ar.

COMO

Isso pode acontecer a qualquer momento em que um access point não estiver configurado adequadamente (por exemplo, deixando as configurações padrão inalteradas).

EXEMPLO

Um AP é enviado da empresa para seu novo escritório, e Charles, o recepcionista, se voluntaria para configurá-lo. Ele segue as instruções e instala o AP que agora está transmitindo um SSID aberto, vazando dados privados como uma peneira. Você não pode culpá-lo porque ele não é um profissional de TI, mas você ainda está com um AP mal configurado que pode ser um sério risco para sua organização.

Access point clandestino

O QUÊ

Um AP clandestino é um AP sem fio que foi instalado em uma rede segura sem uma autorização explícita de um administrador.

COMO

APs clandestinos são conectados à rede autorizada, normalmente com um SSID aberto, permitindo que invasores burlem sua segurança do perímetro. Isso pode ser feito com um AP físico ou um criado em software em um computador e conectado a uma rede autorizada.

EXEMPLO

Você é proprietário de uma loja de varejo com um grande fluxo de clientes constantemente. Em dias mais ocupados, é impossível monitorar todos a cada segundo. Um indivíduo pode facilmente ir até o armário de cabos e conectar o AP mais barato que encontrou e, então, obter acesso à rede segura e privada da empresa, podendo assumir o controle de sistemas de PDV para revelar números de cartão de crédito e muito mais.

Cliente clandestino (Rogue Client)

O QUÊ

Qualquer cliente previamente conectado à um AP clandestino ou outro AP malicioso dentro do alcance de uma rede privada é considerado um cliente clandestino.

COMO

Um cliente tipicamente é categorizado como clandestino se ele se conectar ao AP clandestino, Evil Twin ou outro AP malicioso enquanto estiver dentro do alcance de uma rede WLAN privada. O cliente pode ter sido vítima de uma série de ataques de interceptação (MitM) que incluem o carregamento de ransomworms, malware ou backdoors no cliente.

EXEMPLO

Você para no mesmo café a caminho do trabalho todos os dias. Já que você já se conectou à rede Wi-Fi do estabelecimento antes, seu telefone se conecta automaticamente assim que você entra pela porta. Infelizmente, naquele dia, alguém tinha configurado um AP Evil Twin, enganando seu telefone e o infectando enquanto você estava dentro do alcance da rede local sem fio privada (WLAN) com um ransomware para você levar para o escritório. Assim que você estiver de volta à sua mesa, seu telefone se conenctará ao Wi-Fi corporativo, e o ransomware começará a agir.

Access point vizinho

O QUÊ

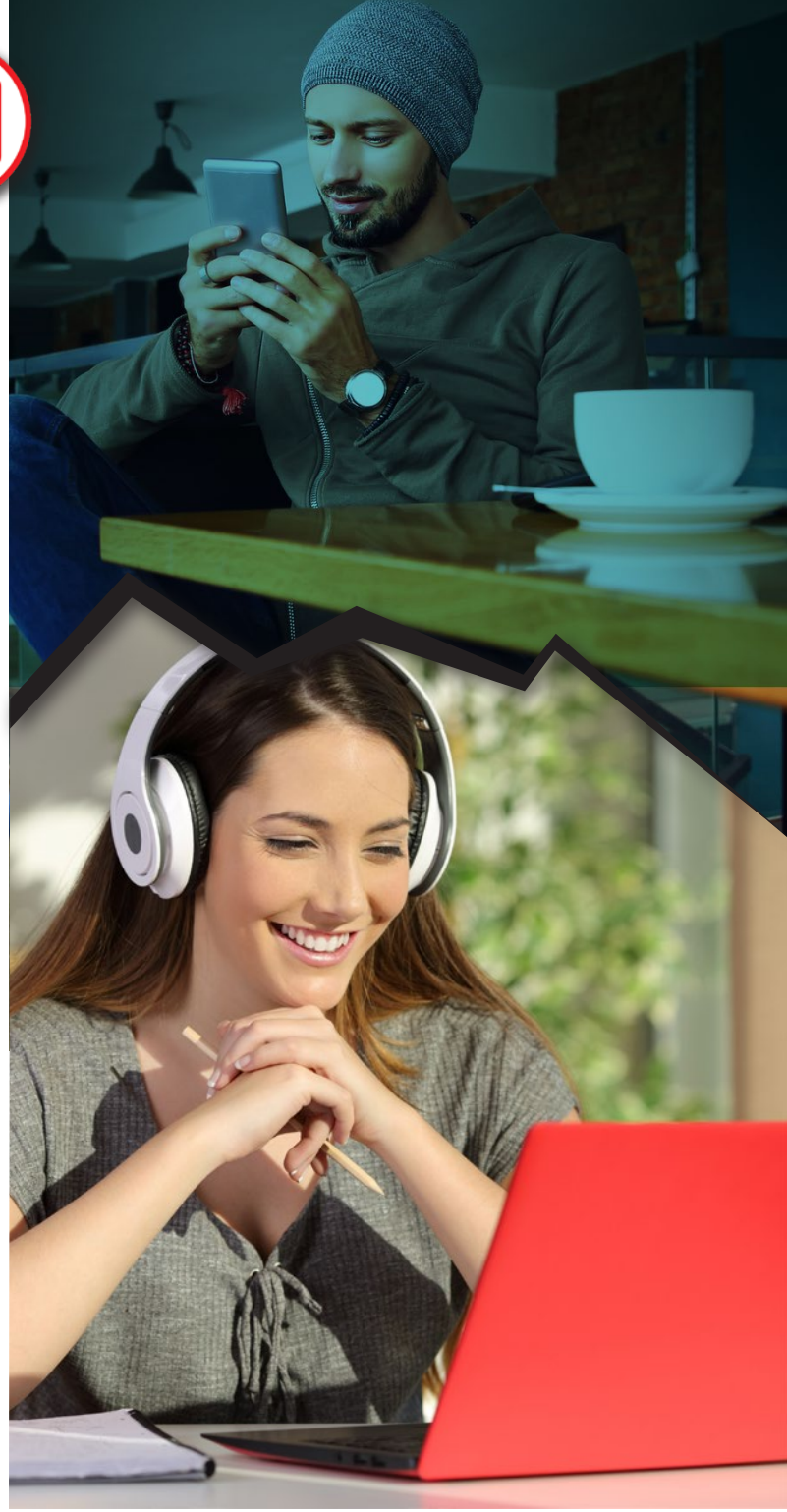
Quando um cliente autorizado se conecta a um AP vizinho, externo ou de convidados, burlando a segurança do perímetro da empresa e ignorando restrições de segurança definidas pelo firewall.

COMO

Não há nenhum truque super secreto de hacker nesse caso. Qualquer um dos seus funcionários pode estar (e provavelmente está) fazendo isso nesse momento. Ao optar por conectar seus dispositivos à rede de convidados ou à rede do café fora da empresa, seus funcionários estão burlando com facilidade a segurança que você incorporou à sua rede.

EXEMPLO

Janice, do departamento de marketing, não consegue ficar sem sua nova trilha sonora favorita todos os dias de manhã. A bateria de seu telefone está quase descarregada, então ela quer usar o computador da empresa para se conectar a um site de streaming. O firewall da empresa restringe o acesso a streaming de música, mas isso não é nenhum problema para Janice – ela simplesmente vai se conectar à Wi-Fi não segura do café e começar a ouvir suas músicas de qualquer forma. Infelizmente para você, um hacker está bebendo seu primeiro café, só esperando que ela se conecte e começar a trabalhar para acessar sua rede.



Rede Ad-Hoc

O QUÊ

Uma conexão Wi-Fi ponto-a-ponto entre clientes que permite que dois dispositivos se comuniquem um com o outro diretamente, contornando suas políticas de segurança de rede e tornando o tráfego completamente invisível.

COMO

Com alguns simples ajustes em suas configurações, qualquer um dos seus funcionários pode configurar rapidamente uma rede ad-hoc entre os dispositivos de seus colegas. Isso pode gerar implicações legais e de segurança que podem impactar sua empresa.

EXEMPLO

A poucos minutos do início de uma reunião, o chefe de Carl AINDA está esperando o arquivo que ele prometeu que seria entregue de manhã. Demoraria muito se ele usasse o sistema seguro de compartilhamento de arquivos em rede aprovado pela empresa, então ele decide configurar uma rede ad-hoc para enviar o arquivo diretamente de um notebook para outro. Infelizmente para você, isso abre a porta para repercussões legais e de segurança para sua empresa.

Defendendo-se contra ameaças de Wi-Fi com um ambiente sem fio confiável

Em um mundo com mais e mais redes Wi-Fi abertas, os hackers de Wi-Fi conseguem não apenas roubar informações, mas espalhar malwares para computadores na rede que podem custar milhões para suas empresas. Você precisa de uma estrutura que te capacite para fornecer acesso Wi-Fi seguro e de alto desempenho aos seus clientes e funcionários.

Uma estrutura de **Ambiente Sem Fio Confiável** se baseia em três principais pilares que possibilitam o desempenho robusto que você deseja com a segurança de que você precisa. São eles:

1. **Desempenho líder de mercado**
2. **Gerenciamento escalável**
3. **Segurança abrangente verificada**

Vamos dar uma olhada em cada um deles e no que eles significam para sua empresa.

Desempenho líder de mercado 1

Você nunca deve se sentir forçado a comprometer sua segurança para alcançar os níveis de desempenho necessários para suportar a velocidade, as conexões e a densidade de clientes do seu ambiente de Wi-Fi. Como vimos, o desempenho lento em sua Wi-Fi corporativa pode ser uma desculpa fácil para um funcionário reencaminhar sua conexão para uma fonte de Wi-Fi menos segura, porém mais rápida.

Uma rede sem fio de alto desempenho não só mantém os funcionários conectados a redes seguras, mas também os mantém trabalhando no pico de sua eficiência. Qualquer período de inatividade aguardando pelo carregamento de algo é uma oportunidade de se distraírem, começarem a navegar pelo seu telefone ou usar esse tempo para dar uma volta pelo escritório.

Dependendo da sua empresa, oferecer uma Wi-Fi de alto desempenho pode ser a diferença entre uma ótima experiência do cliente e uma péssima resenha no Yelp. Para organizações como restaurantes, hotéis e até mesmo consultórios médicos, os clientes que estão planejando gastar uma quantidade significativa de tempo (e, frequentemente, dinheiro) precisam saber que eles podem confiar no desempenho da sua rede Wi-Fi. Uma conexão lenta ou inconsistente pode ser o fator determinante para seus clientes preferirem a concorrência - independentemente do quanto eles amam seu produto!

Uma rede sem fio de alto desempenho não só mantém os funcionários **conectados a redes seguras**, mas também os mantém **trabalhando no pico de sua eficiência**.

Por que a WatchGuard 1

Poder confiar no desempenho da sua conexão sem fio não deveria ser algo que tira seu sono - deveria ser algo que você sabe funcionará todos os dias.

A plataforma segura de gerenciamento de Wi-Fi em núvem e access points de última geração da WatchGuard, oferecem o desempenho que você precisa para apoiar sua empresa. Nossos modelos de access points são especificamente projetados para suportar ambientes de densidade média, como escolas, espaços de escritórios distribuídos, lojas de varejo, salas de reunião, restaurantes e escritórios da área da saúde, bem como ambientes de alta densidade, como campos universitários amplos, centros de conferência e shopping centers.

Além disso, nossos access points com MIMO de vários usuários (MU-MIMO) permitem o downstream de vários dispositivos de clientes simultaneamente. Isso reduzirá o tempo que cada dispositivo deve aguardar para a transmissão do access point, acelerando assim sua rede!

O melhor de tudo é que você oferece acesso sem fio de alto desempenho aos seus funcionários e clientes sem ter que desativar nenhuma das suas configurações de segurança. Implemente segurança total de Wi-Fi sem retardar seu desempenho – essa sim é uma Wi-Fi que beneficia a todos.

A plataforma segura de gerenciamento de Wi-Fi em núvem e access points de última geração da WatchGuard, oferecem **o desempenho de que você precisa para apoiar sua empresa**.

Gerenciamento escalável 2

Ter uma ótima solução de Wi-Fi que seja difícil de gerenciar não ajuda você a proteger ou operar melhor a conectividade sem fio da sua empresa. Você precisa de uma solução que seja fácil de instalar e gerenciar, dando a você controle sobre toda sua rede sem fio, independentemente do tamanho, a partir de uma única interface, além de permitir que você execute os principais processos para proteger o ambiente e os usuários.

À medida que sua empresa cresce, sua implantação de Wi-Fi deve crescer facilmente com você. A centralização do gerenciamento do Wi-Fi permite que você leve sua empresa de um access point sem fio a inúmeros access points em vários locais, sem infraestrutura de controladores.

No mundo conectado via Wi-Fi de hoje, você também precisa visualizar informações cruciais, como cobertura e intensidade do sinal, consumo de banda sem fio por clientes, utilização de access points, visibilidade de aplicativos e distribuição de clientes, para ter uma visão global do que está acontecendo em sua empresa. Ser capaz de visualizar esses dados com facilidade, bem como gerar relatórios personalizáveis sobre tais dados, significa que você pode saber o que está acontecendo em sua empresa sem gastar horas analisando um painel.

A centralização do gerenciamento de Wi-Fi permite que você leve sua empresa de um a inúmeros access points em vários locais, sem infraestrutura de controladores.

Por que a WatchGuard 2

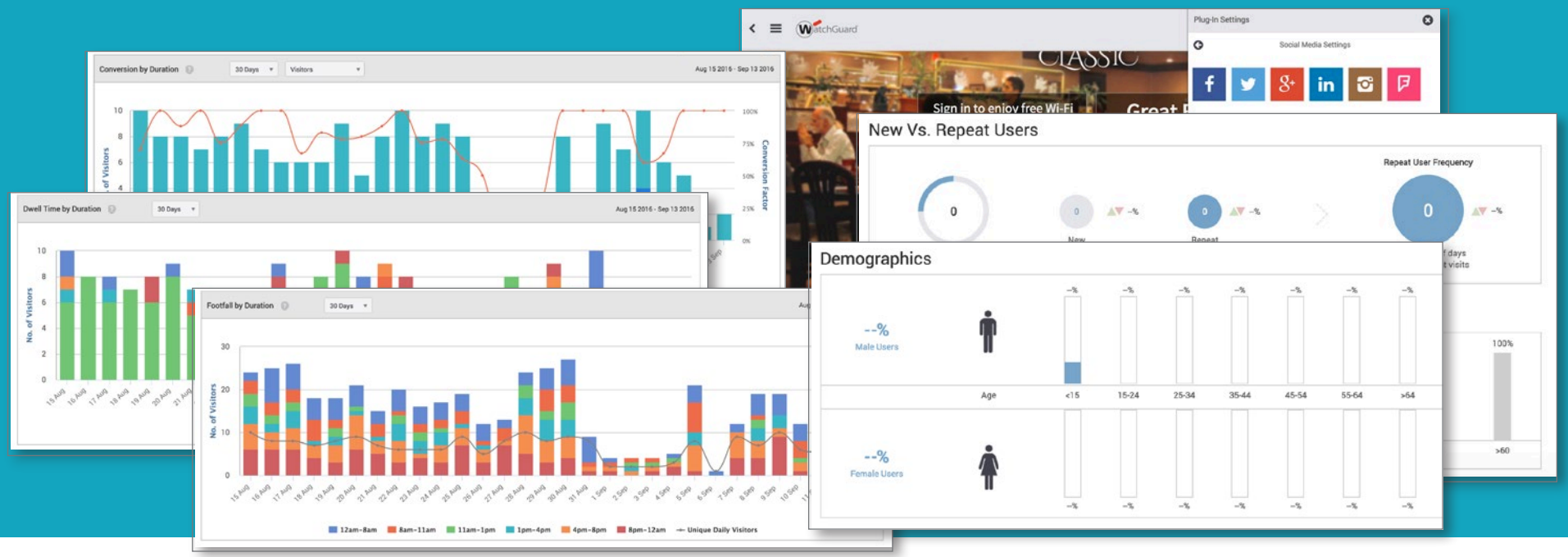
Fácil de configurar e gerenciar, o Wi-Fi Cloud permite que você controle toda a sua rede sem fio a partir de uma única interface, ao mesmo tempo que permite que você agrupe access points da maneira que for mais fácil para você, incluindo agrupamento por local, prédio, andar ou até mesmo cliente, caso você seja um prestador de serviços gerenciado.

Relatórios, widgets de painel, modelos de configuração e diversas informações de análise são visíveis no Wi-Fi Cloud da WatchGuard. Os administradores podem criar pastas aninhadas ilimitadas para representar prédios, andares ou qualquer outro grupo, oferecendo visibilidade da pasta em geral ou permitindo que você visualize somente as informações de análise de um nível específico.

Com o Wi-Fi Cloud, os administradores de rede têm visibilidade sobre aplicativos que estão em operação na rede Wi-Fi. Monitore e gere relatórios sobre mais de 1.300 aplicativos de camada 2 ou superior (como Facebook, YouTube, Instagram etc.) e atribua políticas de uso razoáveis para minimizar o congestionamento da rede.

Por fim, fique atualizado sobre seu ambiente sem fio com modelos predefinidos e personalizáveis e gere automaticamente relatórios sobre ameaças de Wi-Fi, inventário de clientes, status de conformidade e desempenho. O avançado mecanismo de geração de relatórios do Wi-Fi Cloud permite que você agende os relatórios com envio automático para os destinatários de e-mail de sua escolha.

Relatórios, widgets de painel, modelos de configuração e **diversas informações de análise** são **visíveis** no **Wi-Fi Cloud da WatchGuard.**



Segurança abrangente verificada 3

Muitos fornecedores de Wi-Fi de hoje em dia acabam sendo ambíguos quando se trata de oferecer um Wi-Fi seguro. Como qualquer outra área de segurança de sua empresa, você precisa comprovar que a solução protegerá sua empresa dos ataques.

Uma solução de segurança verdadeiramente abrangente oferecerá três principais benefícios:

- Fornecer proteção automática contra as seis categorias conhecidas de ameaças de Wi-Fi discutidas anteriormente
- Permitir que access points legítimos operem no mesmo espaço aéreo
- Impedir que os usuários se conectem a access points de Wi-Fi não autorizados

Tem sido um grande desafio encontrar esse tipo de dados de segurança com a maioria dos fornecedores, já que, francamente, o teste de eficácia da segurança das soluções de Wi-Fi nunca tinha sido feito. Até agora.

Em uma série de testes recentes e inéditos, a empresa especialista em relatórios e líder do setor, a Miercom, desafiou alguns dos principais access points a suportar aplicativos em tempo real enquanto fazia simultaneamente a detecção e prevenção de ameaças comuns à segurança sem fio. Os testes incluíram seis categorias conhecidas de ameaças Wi-Fi, e a Miercom registrou o tempo de detecção da ameaça E o tempo de prevenção de cada ameaça.

	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
Teste	Detectar	Evitar	Detectar	Evitar	Detectar	Evitar	Detectar	Evitar
AP clandestino (Rogue AP)	P	P	F	N/A	F	MP	F	N/A
Cliente clandestino (Rogue Client)	P	P	F	N/A	F	MP	N/A	MP
AP vizinho	P	P	P	P	F	N/A	F	N/A
Rede Ad-Hoc	P	P	F	N/A	F	N/A	P	N/A
AP "Evil Twin"	P	P	P	F	P	MP	P	F
AP mal configurado	P	P	P	N/A	N/A	N/A	N/A	N/A
Ameaças simultâneas	P	P	F	F	F	F	F	F

P = Aprovado
F = Reprovado
MP = Aprovação marginal
N/A = Recurso não suportado

Confira o relatório completo da Miercom: **www.watchguard.com/wifi-security-report**

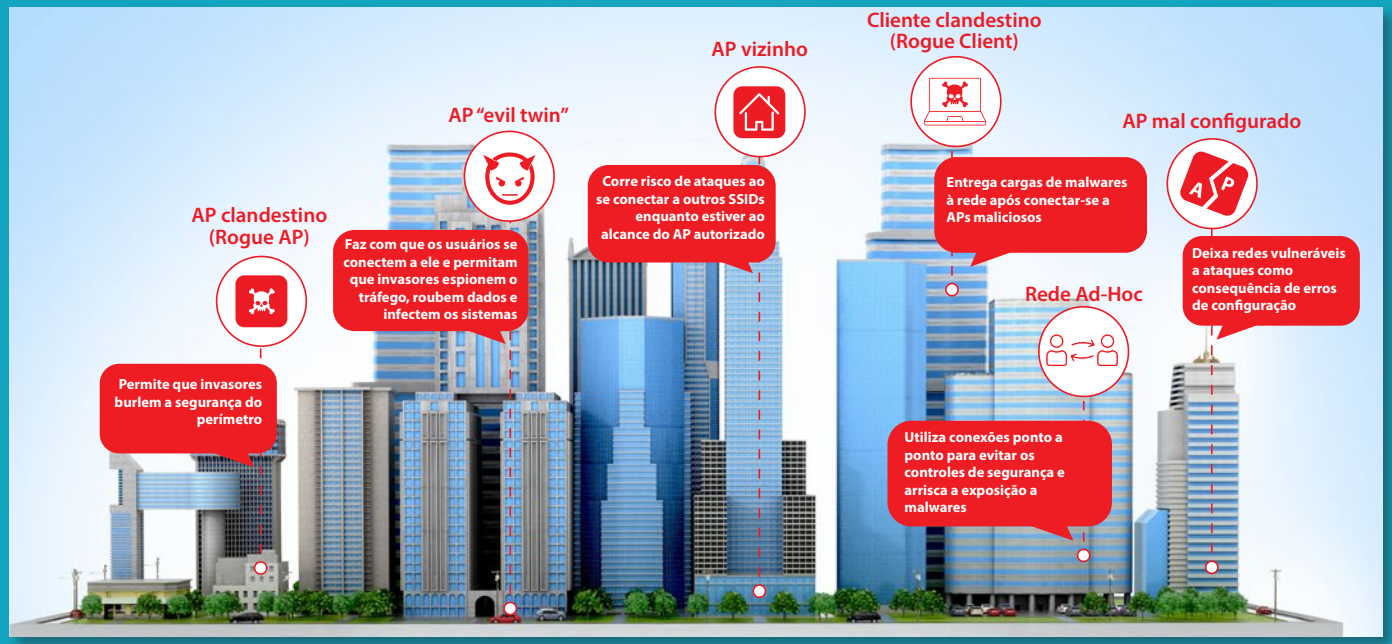
Por que a WatchGuard 3

A WatchGuard é o único fornecedor a não apenas detectar, mas evitar automaticamente as seis categorias conhecidas de ataque de Wi-Fi. A solução Wi-Fi da WatchGuard também foi a única a conseguir detectar e evitar todas as ameaças simultaneamente em menos de 20 segundos.

Nosso sistema patenteado de Sistema de Prevenção de Intrusão Sem Fio (WIPS) é diferente de qualquer outra solução de segurança de Wi-Fi no mercado, garantindo que você tenha proteção Wi-Fi automatizada e precisa para sua empresa. Enquanto outros fornecedores usam assinaturas e contam em peso com regras de correlação de endereços MAC que podem resultar em um alto volume de falsos positivos, nossa tecnologia de marcadores de pacotes protege seu espaço aéreo com poucos ou nenhum falso positivo.

O WIPS da WatchGuard é a única solução no mercado que verifica todos os access points na área e classifica-os como autorizados, externos ou clandestinos. Ao diferenciar de forma rápida e confiável os access points e clientes, você pode garantir que os APs e clientes autorizados terão o acesso que precisam, os APs e clientes externos permanecerão isolados, e os APs e clientes clandestinos serão bloqueados da conexão.

A WatchGuard é o **único fornecedor** a não apenas **detectar,** mas também **evitar automaticamente as seis** categorias **conhecidas de ataque de Wi-Fi**.



A ÚNICA Escolha para seu Ambiente Sem Fio Confiável

A WatchGuard é a única empresa a oferecer às organizações as tecnologias e soluções para criar um Ambiente Sem Fio Confiável, oferecendo os três principais fundamentos - desempenho líder de mercado, gerenciamento escalável e segurança abrangente verificada, protegendo contra todas as seis categorias conhecidas de ameaças de Wi-Fi.

Em todas as áreas, em todos os testes, a WatchGuard é a única escolha.

Os principais resultados do relatório da Miercom concluíram que a WatchGuard foi o único fornecedor a:

- Detectar automaticamente e evitar as seis categorias conhecidas de ataque de Wi-Fi simultaneamente ao mesmo tempo que mantém o desempenho
- Oferecer suporte à detecção e prevenção automáticas de rogue APs e rogue clients;
- Detectar e evitar comunicações de endpoints automaticamente por meio de conexão Wi-Fi ad-hoc;
- Automaticamente evitar conexões a APs "Evil Twin" e conexões perigosas a APs mal configurados, como SSIDs privados sem criptografia.

Saiba mais sobre como criar seu Ambiente Sem Fio Confiável com a WatchGuard hoje mesmo!

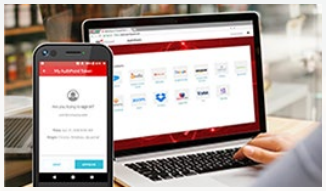
Watchguard.com/trustedwirelessenvironment




A PLATAFORMA DE SEGURANÇA UNIFICADA 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 proteção da categoria, de nível corporativo, para qualquer organização, independentemente do tamanho ou do conhecimento técnico.



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.

Wi-Fi Seguro na Nuvem

A solução Wi-Fi Seguro da WatchGuard, revolucionária no mercado de hoje, foi projetada para oferecer um espaço aéreo seguro e protegido para ambientes de Wi-Fi, ao mesmo tempo em que elimina dores de cabeça administrativas e reduz 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.

Segurança de Endpoint

A Segurança de Endpoint da WatchGuard oferece um portfólio avançado e nativo da nuvem que protege todo tipo de empresa contra ataques cibernéticos atuais e futuros. A principal solução, a EPDR da WatchGuard, 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 Busca de Ameaças.

Saiba mais

Para obter detalhes adicionais, fale com o revendedor autorizado da WatchGuard ou acesse **www.trustedwirelessenvironment.com**

Sobre a WatchGuard

A WatchGuard® Technologies, Inc. é a líder global em segurança de rede, Wi-Fi protegida, autenticação de múltiplos fatores e inteligência de rede. Os premiados produtos e serviços da empresa são adotados em todo o mundo por cerca de 10 mil revendedores de segurança e prestadores de serviços para proteger mais de 80 mil clientes. A missão da empresa é tornar a segurança de nível corporativo acessível a empresas de todos os tipos e tamanhos com simplicidade, tornando a WatchGuard a solução ideal para empresas distribuídas e para pequenas e médias empresas. A WatchGuard tem sede em Seattle, Washington, EUA, com escritórios na América do Norte, Europa, Ásia-Pacífico e América Latina. Para saber mais, acesse **WatchGuard.com**.

Vendas da América do Norte: 1.800.734.9905 • Vendas internacionais: 1.206.613.0895 • Web: www.watchguard.com/wifi