


A Implementação de Redes Zero Trust em Tempos de COVID-19

Índice

INTRODUÇÃO

A pandemia de coronavírus expôs as inadequações de continuidade do negócio de muitas organizações e destacou como é lento o progresso da transformação digital. À medida que a situação é controlada, percebemos que muitas empresas estão a passar por um momento de intensa racionalização, planeando a continuidade das suas operações nos curto e médio prazos e tentando definir o caminho que devem seguir. O desafio é ainda maior ao examinar as opções de proteção para os seus recursos humanos, dados e aplicações à distância por um período prolongado. Quem sabe até indefinidamente.

Esta nova realidade faz com que seja necessário abandonar o modelo de segurança tradicional centrado na rede - que pressupõe que todos os dispositivos e utilizadores que por ela circulam dela são fiáveis. Com a maioria dos utilizadores a trabalhar remotamente, a adesão a abordagens de segurança zero trust intensificou-se, principalmente nos ambientes empresariais. Empresas em crescimento, que geralmente não contam com especialistas internos em segurança, têm tido dificuldades acrescidas nesta matéria.

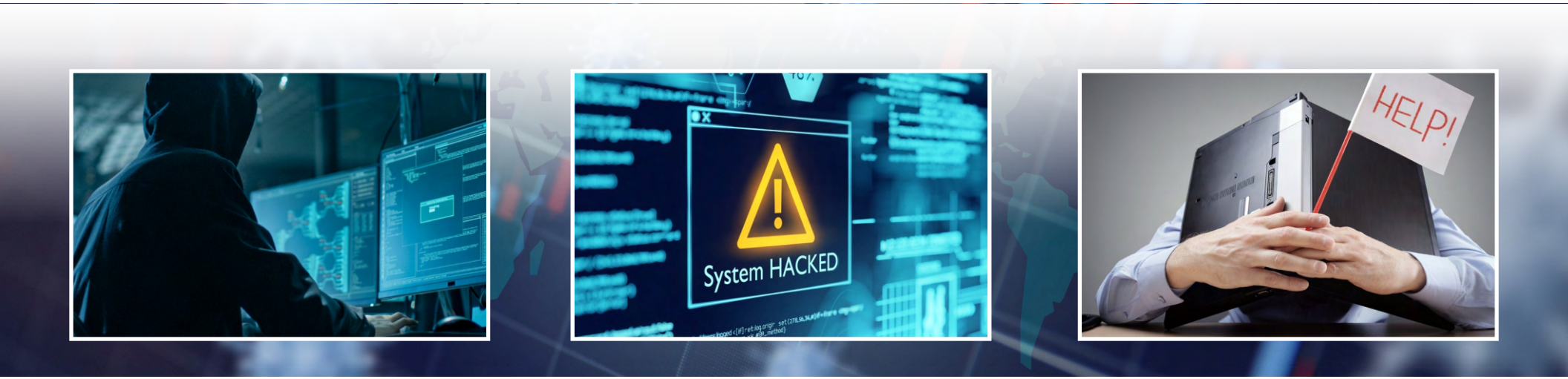
Neste eBook, abordaremos a forma como a dinâmica da COVID-19 impactou a segurança, descreveremos a importância de assumir uma abordagem zero trust e discutiremos de que modo a WatchGuard pode ajudar a sua empresa a contar com a segurança de que precisa durante este período desafiante.

O TRABALHO REMOTO ESTÁ A AUMENTAR AS VIOLAÇÕES DE SEGURANÇA

Mesmo com todas as mudanças causadas pela COVID-19, certas coisas permanecem iguais, como a ameaça dos ciberataques a empresas, que continuam a proliferar e são cada vez mais sofisticados. Infelizmente, enquanto algumas empresas estão em "modo de sobrevivência", os cibercriminosos aproveitam a oportunidade para identificar vulnerabilidades e estabelecer alvos:

- Os ataques de phishing aumentaram drasticamente com dezenas de domínios maliciosos a surgir diariamente e a tirar partido da ansiedade gerada pelo coronavírus. No auge da crise, a Microsoft reportou 70 mil ataques diários ligados ao tema COVID-19, e isto só nos EUA.[1] Muitas dessas campanhas usaram kits de phishing conhecidos, adaptados para ao contexto atual.[2]
- Com a explosão no uso de plataformas de videoconferência, como o ZOOM, que passou de 10 milhões para mais de 200 milhões de utilizadores simultâneos, a CISA lançou um alerta sobre ciberagentes maliciosos que procuram explorar o crescimento no uso de plataformas de comunicação populares através do envio de e-mails de phishing que incluíam ficheiros maliciosos.[3]
- Só nas primeiras semanas da crise, investigadores de segurança observaram um pico de 41% no número de dispositivos com RDP expostos na Internet usando uma porta TCP padrão 3389 altamente vulnerável.[4]
- Sites falsos que fingem disponibilizar clientes VPN legítimos e prometem proteger as pessoas conseguiram enganar muitos utilizadores, que transferiram e instalaram malware nas suas próprias máquinas.[5]
- E os criminosos podem estar na porta ao lado, aproveitando o facto de o edifício estar repleto de teletrabalhadores, com quase 50% do tráfego de IP constituído por Wi-Fi.[6]

1 https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/
2 https://threatpost.com/covid-19-scam-scramble-cybercrooks-recycle/154383/
3 https://us-cert.cisa.gov/ncas/alerts/aa20-099a
4 https://www.bankinfosecurity.com/covid-19-driving-surge-in-unsafe-remote-connectivity-a-14035
5 https://www.cybereason.com/blog/just-because-youre-home-doesnt-mean-youre-safe
6 https://www.rehmann.com/resources-insights/business-wisdom-2/item/2740-it-leadership-8-remote-workforce-tips-for-optimal-access-security-and-productivity



A AMPLIAÇÃO DA PROTEÇÃO DE VPN NÃO É SUFICIENTE

O uso de redes VPN cresceu drasticamente, com um aumento de 50% no tráfego só numa semana. Só nos Estados Unidos, o uso de VPNs cresceu 150% em apenas um mês. A migração repentina dos utilizadores dos escritórios da empresa para os domésticos fez com que várias empresas tivessem dificuldade em fornecer licenças de VPN aos seus funcionários. Existe o risco de que, sem uma conectividade por VPN, os utilizadores não tenham acesso aos recursos necessários ou usem ligações inseguras para aceder a estes.

Os utilizadores precisam de segurança agora que estão fora da rede. No entanto, também é importante garantir que o malware e outras ameaças não surjam quando esses utilizadores se voltarem a ligar à rede, seja por VPN ou quando regressarem fisicamente ao escritório. A ampliação da proteção a redes por VPN proporciona um elevado nível de segurança. No entanto, a natureza dos cibercrimes dos dias de hoje exige mais do que apenas isso.

Quando uma VPN é usada de forma isolada, é atribuído um nível de segurança totalmente desadequado ao Endpoint, e isso pode causar a disseminação de malware para a rede mais ampla. As empresas devem perceber, cada vez mais, que os seus colaboradores são a linha da frente da defesa da organização contra as ciberameaças e também o seu elo mais fraco.

Por esse motivo, as equipas de TI devem começar a tratar as redes domésticas dos funcionários como uma potencial ameaça, em que:

- Basta um único endpoint comprometido ou uma credencial roubada para que seja possível invadir a sua empresa;
- Quase dois terços das ameaças escondem-se em tráfego encriptado;
- Alguns ataques são altamente direcionados, sendo outros oportunistas, sem alvos específicos. É preciso proteção contra ambos.
- Os utilizadores são a linha da frente da defesa e precisam de recursos para identificar, evitar e denunciar ameaças.

O uso de VPNs cresceu drasticamente, com um **aumento de 50% no tráfego só numa semana.** Só nos Estados Unidos, espera-se que **o uso de VPNs cresça 150% por mês.**

IMPLEMENTAÇÃO DE REDES ZERO TRUST

A sua empresa já tem uma estratégia de segurança de confiança zero? As redes tradicionais são construídas com base na ideia de uma confiança inerente. Já as estruturas "zero trust" pressupõem que cada dispositivo e utilizador, dentro ou fora da rede, representa um risco à segurança. Em termos de conceito, "zero trust" pode ser interpretado como uma abordagem de segurança que recomenda "nunca confiar, sempre verificar" e usa múltiplos níveis de proteção para prevenir ameaças, bloquear movimentos laterais e reforçar controlos granulares de acesso do utilizador.

A estrutura "zero trust" baseia-se em três princípios:

1. Identificação de utilizadores e dispositivos: limite as permissões de acesso de dispositivos a sistemas e aplicações críticos.

As empresas têm uma grande parte das suas equipas a operar remotamente. Por isso, garantir acesso às ferramentas internas representa um grande desafio. Ao mesmo tempo, os cibercriminosos estão a utilizar uma variedade de técnicas para obter nomes de utilizadores e passwords (como spear phishing, engenharia social e compra de credenciais roubadas na dark web) com o objetivo de ter acesso à rede e roubar dados valiosos de empresas e clientes. Os serviços de autenticação multifatorial (MFA) baseados na cloud permitem a mitigação de roubo de credenciais, fraude e ataques de phishing.

2. Disponibilização de acesso seguro: saiba sempre quem e o quê está ligado à rede da empresa.

Na estrutura "zero trust", o objetivo da gestão de acessos é proporcionar uma forma de gerir centralmente os acessos em todos os sistemas de TI comuns e, ao mesmo tempo, limitar o acesso a utilizadores, dispositivos e aplicações específicos. As decisões sobre acessos devem ser feitas em tempo-real com base em políticas definidas pela empresa em questão e no contexto da solicitação de acesso. As tecnologias de login único (SSO), combinadas com MFA, podem melhorar a segurança de acessos e minimizar o inconveniente da definição de passwords para os utilizadores.

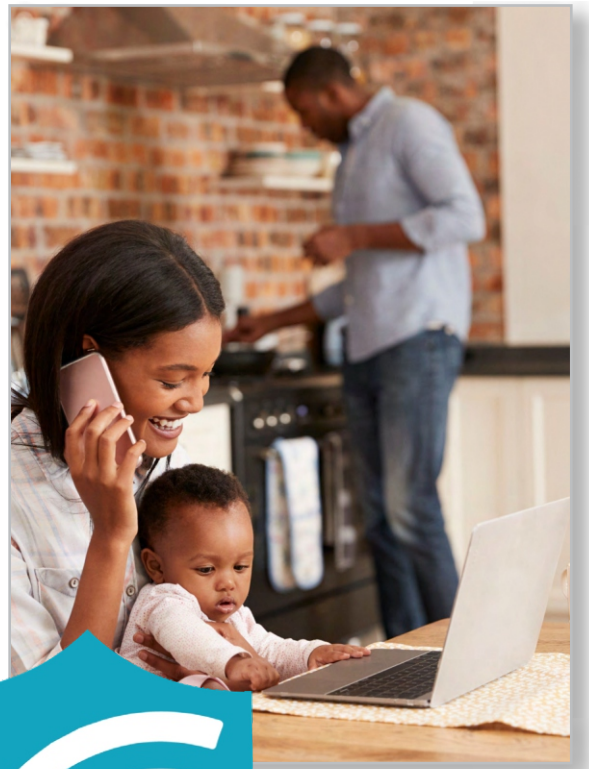
3. Monitorização contínua: monitorize a integridade e a postura de segurança da rede de todos os endpoints geridos.

Com o coronavírus, as ameaças de malware e ransomware intensificaram-se significativamente. O risco de infeção está mais alto do que nunca, uma vez que os utilizadores já não podem contar com a proteção de uma firewall enquanto estão em teletrabalho. E oferecer proteção a utilizadores que navegam na Internet torna-se algo ainda mais desafiador quando estes se ligam de fora da rede.

Com a obrigatoriedade de trabalhar a partir de casa, é bem possível que os portáteis da empresa sejam intensamente utilizados pelos funcionários para navegar na web e ler e-mails pessoais. Ter controlo sobre as ameaças requer uma segurança avançada persistente que vá muito para além do antivírus tradicional.

CRIAÇÃO DE UM AMBIENTE WIRELESS DE CONFIANÇA

O trabalho remoto também pode levantar questões de segurança relacionadas com o Wi-Fi. Por todo o mundo, os locais fechados devido à pandemia da COVID-19 estão a planear a sua reabertura. Enquanto isso, os administradores de rede preparam-se para ter trabalho extra quando as pessoas regressarem ao escritório. Já imaginou quantos portáteis da empresa poderão ter sido infetados por ransomware enquanto usaram uma rede Wi-Fi doméstica?



Com um Ambiente Wireless de Confiança, é possível fazer o seguinte:

- Automatizar a deteção e a análise das principais causas de falhas e anomalias.
- Detetar automaticamente em tempo-real os casos em que clientes de Wi-Fi não conseguem ligar-se e identificar a causa principal desse problema (seja relacionada com a rede Wi-Fi, com o serviço de rede ou com o dispositivo e/ou aplicação).
- Importar facilmente ficheiros de imagem standard com as plantas de cada localização. Uma vez adicionados, basta clicar com o botão direito no access point para ver todas as funções de gestão e resolução de problemas de cada AP. Os mapas de calor mostram a cobertura do access point, a velocidade de ligação e a cobertura do canal.

Vai Voltar para o Escritório? A rede Wi-Fi Pode Ajudar a Garantir o Distanciamento Social

Promova um ambiente de trabalho seguro com a monitorização automatizada do distanciamento social via gestão do Wi-Fi Cloud. Os access points de Wi-Fi podem proporcionar medições em tempo-real de densidade de utilizadores, bem como alertas e notificações se os limites da capacidade forem violados ou chegarem perto disso.

Com a monitorização de multidões baseada em Wi-Fi, as empresas podem:

- Gerir agrupamentos de colaboradores e fluxos de reunião;
- Analisar visitantes, incluindo o movimento de saída e entrada;

  Assegurar o cumprimento de regras, com restrições de grupos de pessoas;
- Melhorar as operações comerciais, o planeamento, o impacto económico e a valorização de ativos com dados acionáveis;
- Manter anonimato total, em conformidade com as políticas de privacidade e o RGPD.

GUIA ZERO TRUST DE SEGURANÇA WATCHGUARD

A adoção de uma estratégia "zero trust" pode ajudar a sua empresas a desenvolver uma abordagem muito mais moderna de cibersegurança. A boa notícia é que não está sozinho nessa missão. Se o seu departamento de TI for muito pequeno, ou se não tiver um, os prestadores de serviço geridos são a solução de que as empresas necessitam para confiar numa infraestrutura sólida que permita aos utilizadores móveis trabalhar a partir de qualquer dispositivo e lugar, além de fornecer acesso a serviços de cloud públicos, garantindo a segurança da empresa.

Como a WatchGuard Oferece Segurança "Zero Trust"

1. Identidade do utilizador e proteção de dispositivos adaptadas exclusivamente a ambientes "zero trust":

- **100% Gerido na Cloud.** A WatchGuard Cloud permite-lhe gerir e gerar relatórios sobre os seus serviços de segurança a partir de uma só plataforma poderosa. Quer tenha como objetivo reduzir ou eliminar custos de infraestrutura, acelerar a sua configuração, implementar sites remotos em qualquer nível, simplificar as suas ferramentas de gestão de segurança ou obter mais visibilidade sobre a sua rede, a WatchGuard Cloud pode ajudar.

- **DNA de Dispositivos Móveis.** As ameaças sofisticadas conseguem clonar dispositivos móveis e usar o aparelho falso para fazer autenticação em sistemas, contornando os mecanismos de MFA. O recurso exclusivo Mobile DNA da WatchGuard tira uma impressão digital das características únicas de cada dispositivo móvel. Sempre que um utilizador fizer login, a aplicação AuthPoint recriará o DNA do dispositivo móvel, incluindo-o numa password de uso único (OTP), garantindo que apenas o aparelho original possa realizar a autenticação.

- **Integrações de Terceiros.** O ecossistema da WatchGuard inclui muitas integrações de terceiros com o AuthPoint. Isto permite que as empresas autorizem utilizadores a passar pelo processo de autenticação antes de aceder a aplicações na cloud, VPNs e redes confidenciais. Além disso, o AuthPoint oferece suporte ao standard Security Assertion Markup Language (SAML), permitindo que os utilizadores façam login uma vez para aceder a todas as aplicações e serviços.

2. Acesso seguro simplificado em todas as áreas:

- **Integração do AuthPoint com as Principais Plataformas de IAM.** As empresas estão a implementar soluções de gestão de identidades e acessos (IAM) para dar aos utilizadores controlo completo e facilidade de acesso a todas as aplicações da empresa. O WatchGuard AuthPoint faz a integração diretamente com as principais plataformas de IAM no mercado, incluindo CyberArk, Akamai, Oracle, entre outras.

- **Portal de Acesso e WatchGuard Firebox.** O Portal de Acesso é uma solução de VPN sem cliente incluída por definição em todos os sistemas Firebox e permite acesso remoto seguro a utilizadores. Com o Portal de Acesso, os utilizadores apenas precisam de um browser web para se ligarem a aplicações web de terceiros, aplicações internas e serviços do Microsoft Exchange, bem como criar sessões de RDP e SSH a recursos locais.

- **Verificação de VPN Segura e Isolamento do Host**. A nossa plataforma de Deteção e Resposta a Ameaças (TDR) unifica a segurança da rede e recursos de segurança de endpoint para impedir máquinas potencialmente infetadas de transportar malware para a rede mais ampla. Com o TDR, é possível exigir um sensor de host ativo em cada dispositivo que faça uma tentativa de ligação à rede diretamente ou via VPN. Além disso, o sensor de host monitorizará a integridade do dispositivo e isolará o mesmo se este se tornar um risco.

3. Redes, endpoints e utilizadores estão seguros, independentemente de onde as pessoas se liguem:

- **Filtragem de DNS com o DNSWatch e o DNSWatchGO.** A filtragem de DNS baseada na cloud possibilita o bloqueio de ligações e a limitação do acesso a áreas perigosas da Internet, sem o reencaminhamento do tráfego de volta à rede. Os cliques em links maliciosos e as tentativas de ligação a domínios relacionados com phishing e malware são bloqueadas automaticamente.

- **Deteção e Resposta a Endpoints do AD360.** Para detetar um malware avançado, é preciso usar técnicas avançadas. O AD360 combina vários métodos de deteção, como a análise comportamental, heurística e sandboxing numa única plataforma. Os recursos de IA do AD360 permitem prever e bloquear automaticamente as ameaças antes que comecem a causar danos, assim como descobrir anomalias que os analistas humanos podem deixar escapar.

- **Total Security Suite e WatchGuard Firebox.** Implementado no centro da rede, uma WatchGuard Firebox oferece segurança de classe empresarial em camadas que protege contra as mais recentes ameaças.

- **Deteção e Resposta a Ameaças (TDR).** Com o TDR, a WatchGuard integra telemetria de rede e endpoint na cloud, correlacionando dados de segurança para detetar e responder a ameaças que não seriam detetadas isoladamente.

- **Núcleo de Automatização.** As soluções da WatchGuard são altamente automatizadas, o que permite poupar muito tempo em processos manuais e replicados. A automatização simplifica tudo, das atualizações em antivírus e gestão de patches à deteção de anomalias e alertas. Além disso, os processos de segurança podem ser facilmente integrados com ferramentas de PSA. Uma integração sólida com ferramentas RMM permite obter respostas mais rápidas a solicitações de suporte.

COMECE A PLANEAR UMA ABORDAGEM "ZERO TRUST" PARA A SUA EMPRESA

Embora a crise pandémica tenha apanhado toda a gente desprevenida, o advento do teletrabalho em massa é particularmente um território desconhecido para muitas empresas. Com a maioria dos utilizadores a trabalhar remotamente, contar com uma estratégia "zero trust" pode ajudar a manter a continuidade e a segurança das empresas.

Os parceiros da WatchGuard podem desempenhar um papel fundamental, ao trazer as competências e recursos necessários para uma implementação eficaz de redes zero-trust na sua organização.

Aceda a https://watchguardsupport.secure.force.com/PartnerFinder/ para saber mais sobre os Parceiros WatchGuard e o portfólio de produtos de cada um.

PONTUAL
software solutions

A Pontual dedica-se ao desenvolvimento e implementação de soluções tecnológicas que geram crescimento nas organizações. No nosso portefólio de atividades constam software de gestão ERP, engenharia de software, desenvolvimento web e de lojas online, hardware e managed services.

Criamos valor para as empresas com soluções que promovem agilidade, desempenho operacional e melhor gestão, contando com equipas certificadas, motivadas, orientadas para resultados e com vontade de fazer a diferença.

https://www.pontualsoftware.com/

Santa Maria da Feira | Porto | Lisboa | Viseu | Fundão | Vila Real

Uma equipa pronta a ajudar a criar as empresas do futuro

WatchGuard

 Vendas na América do Norte: 55.11.98586-8814 • Vendas no Brasil (Norte/Centro Oeste/Sul): 55.11.99272-7257 • Web: www.watchguard.com