Residência protegida como uma extensão da rede corporativa

Índice

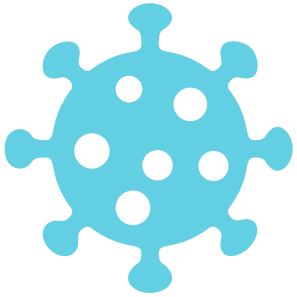
Resumo executivo

O trabalho em casa (work from home — WFH) não é um conceito novo, mas vimos sua evolução e aceleração nos últimos dois anos durante a pandemia.

Antes da COVID, o trabalho em casa era operado em uma escala muito menor do que é exigido para a força de trabalho de qualquer lugar de hoje. Segundo o Fórum Econômico Mundial, por exemplo, nos Estados Unidos, antes cerca de 7% dos trabalhadores tinham a opção de trabalhar regularmente em casa.[1] Trabalhar remotamente às vezes era visto como um luxo apenas para executivos, gerentes de alto nível e trabalhadores do conhecimento. Para a maioria dos funcionários, WFH significava ler os e-mails ou revisar um documento rapidamente em casa fora do horário de trabalho.

A pandemia forçou muitas empresas a habilitar rapidamente o WFH para seus funcionários em grande escala para a continuidade dos negócios. De acordo com o Pulse of Remote Work: Before & After COVID-19 realizado pela Pipefy, no início de 2021, 66% dos trabalhadores estavam trabalhando remotamente pela primeira vez após a paralisação causada pela COVID.[2] Muitas organizações tiveram que rapidamente reunir soluções WFH, como videoconferência, compartilhamento de dados e colaboração em equipe para seus funcionários em casa, para que pudessem realizar suas funções básicas de trabalho. Essas soluções foram apressadas, feitas em um prazo curto, não otimizadas ou não totalmente seguras na maioria das vezes.

Dois anos de pandemia e WFH agora é o novo normal. Muitas empresas percebem que, embora tenham sido forçadas a entrar no modo de operação WFH involuntariamente, tiveram algum sucesso. E certamente houve benefícios para a eficiência operacional e a felicidade dos funcionários. Mas, para manter o WFH sustentável e benéfico no futuro, as empresas agora buscam soluções de infraestrutura de longo prazo para oferecer melhor suporte às suas forças de trabalho remotas e otimização para obter melhor desempenho e produtividade.



A pandemia da COVID-19 não apenas levou a transição rápida e em larga escala para o trabalho remoto, mas também apresentou uma oportunidade de imaginar o trabalho de maneira diferente.

Avaliação das soluções WFH atuais

As empresas estão superando a mera necessidade de conexões e acesso à Internet para funcionários trabalhando em casa e buscando experiências digitais mais consistentes, melhor produtividade e desempenho otimizado. Para melhorar as experiências digitais, as organizações devem avaliar o estado atual das infraestruturas de rede e a forma como suas soluções WFH podem ser otimizadas. Também devem avaliar as deficiências e desafios e reavaliar suas soluções a partir do que se apressaram em implementar no início da pandemia.

Muitas das atuais soluções improvisadas de WFH são, na melhor das hipóteses, fragmentadas. No início da pandemia, em resposta à necessidade do mercado e à escassez de soluções WFH, as organizações implementaram uma variedade de pacotes de hardware e software diferentes de diversos fornecedores de rede, segurança e colaboração. Por exemplo, muitos pontos de acesso (access points — APs) sem fio de classe empresarial foram promovidos como conectividade sem fio segura para a rede corporativa. No entanto, com uma análise mais detalhada desses APs corporativos, pode-se ver que eles são alimentados principalmente por Power-over-Ethernet (PoE), que não é uma fonte de energia comum em casa. Essa configuração requer um grande injetor de energia entre a conexão Ethernet e o AP.

A residência como um desafio de segurança único

Quando as empresas implantaram suas soluções iniciais de WFH, a segurança era secundária — a conectividade e o acesso eram uma preocupação maior e mais imperativa. Quando se trata de segurança, as soluções WFH implantadas com mais frequência incluíram segurança de endpoints por meio de rede privada virtual (VPN) do cliente e controle de acesso por meio de autenticação multifator. Essa solução seria satisfatória se os funcionários estivessem usando seus dispositivos corporativos apenas para WFH e não para uso pessoal. No entanto, cada vez mais funcionários usam dispositivos pessoais para trabalhar, verificar e-mails comerciais, acessar recursos da empresa e colaborar em projetos. Às vezes, eles também usam notebooks corporativos para navegação pessoal na Web, entre outros. Isso abriu portas e facilitou a vida dos invasores ao invadir os dispositivos pessoais ou corporativos em casa e obter acesso e lançar um ataque aos sistemas corporativos assim que entrassem.

A lição é que proteger dispositivos corporativos e proteger a rede de trabalho de sobreposição dedicada não é mais suficiente. Todo o ambiente de rede doméstica mista também precisa ser protegido, incluindo:

- ✓ **Diversos usuários:** membros da família, amigos, convidados, superusuários, usuários avançados
- ✓ **Vários dispositivos:** notebooks, telefones celulares, tablets, impressoras, leitores eletrônicos, smart TVs
- ✓ **Um número crescente de dispositivos domésticos inteligentes da Internet das Coisas (IoT):** termômetros, fechaduras de portas, câmeras IP, assistentes digitais, abridores de portas de garagem, babás eletrônicas, câmeras e sensores de segurança e muito mais
- ✓ **Diversas aplicações:** jogos online, redes sociais, ferramentas de colaboração em equipe, ferramentas de produtividade, streaming de mídia

A segurança da rede doméstica atualmente reside no roteador doméstico integrado com recursos sem fio. E esses roteadores são fornecidos por fornecedores de redes de consumo ou provedores de serviços de Internet (internet service providers — ISPs). No entanto, embora esses roteadores voltados ao consumidor afirmem que fornecem recursos de segurança e alguns até adicionam segurança como serviço em seu produto de hardware, as medidas de segurança não são de nível empresarial. Elas são muito menos eficazes em antivírus, malware, detecção e prevenção de ransomware, sem falar em recursos avançados adicionais, como filtragem de conteúdo da Web e bloqueio de anúncios.

Gerenciamento e escala para soluções WFH

A força de trabalho que trabalha de qualquer lugar aumentou imensamente a superfície de ataque, com funcionários criando grandes quantidades de endpoints com seus dispositivos e aplicações. No entanto, ao contrário das filiais distribuídas, onde as empresas podem usar ferramentas e monitorar a rede, elas não têm visibilidade das redes domésticas dos funcionários. Essas redes domésticas ficam fora do firewall corporativo e não podem ser monitoradas para detectar ameaças.

Como foram apressadas para implantação e ativação rápidas, muitas das soluções WFH atuais são sobreposições sobre a infraestrutura de rede original da organização. Essas soluções carecem de gerenciamento e visibilidade centralizados e tendem a exigir ferramentas e métodos separados da rede local e gerenciamento de segurança. Pode ser quase impossível integrá-los efetivamente com novas soluções.

Além disso, o sistema de sobreposição causa inconsistências na política de segurança e no gerenciamento de acesso porque não pode ser sincronizado o tempo todo. O mesmo vale para o uso de recursos e otimização de aplicações. Se houver dois sistemas separados para corporativo e WFH, não haverá uma visão geral da utilização de recursos. Portanto, os recursos não podem ser alocados de forma apropriada.

Além da falta de controle, visibilidade e consistência, outro desafio exclusivo do WFH é sua escala massiva. Seria um uso intensivo de recursos e seria quase impossível para as equipes de TI implantar soluções WFH para cada funcionário, configurá-las, gerenciar acesso e ajustes de política e solucionar um problema de cada vez. No futuro, serão necessárias ferramentas automatizadas e otimização orientada por inteligência artificial (IA) para respaldar as forças de trabalho do WFH.

A residência é um espaço pessoal

Como muitos fornecedores corporativos aderiram à tendência em resposta à crescente demanda por soluções WFH seguras, quase todos eles não perceberam que a solução seria instalada em casa, um ambiente totalmente diferente do escritório.

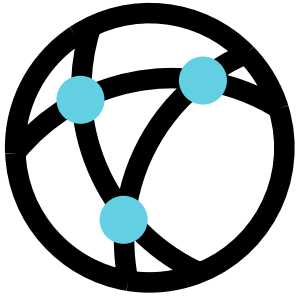
Para começar, precisa ser projetado pensando nos usuários domésticos e ser fácil de usar. A maioria das soluções corporativas é projetada para instalação e manutenção por profissionais de TI — os funcionários teriam dificuldade de instalar a solução corporativa por conta própria em casa.

Existem duas maneiras de implantar uma conexão de trabalho segura em casa. Os fornecedores de soluções WFH de hoje oferecem o uso de um ponto de acesso sem fio (wireless access point — WAP) empresarial de baixo custo e criam um túnel VPN dedicado para se conectar à rede corporativa. Essa conexão sem fio reside na rede doméstica, de modo que o trabalho do funcionário disputa a mesma largura de banda compartilhada com outros membros da família e suas diversas necessidades de conectividade.

Outra maneira pela qual muitos fornecedores focados no consumidor protegem o WFH é oferecendo recursos de segurança para cobrir e proteger toda a casa. No entanto, negligenciam essa propriedade do espaço doméstico. Se uma organização proteger toda a rede doméstica, será capaz de assumir o controle da rede doméstica do funcionário, o que equivale a uma total falta de controle de rede por parte do funcionário WFH e pode invadir a privacidade dele.

Outro problema vem do uso misto de trabalho e dispositivos pessoais. No mundo tecnológico de hoje, muitas organizações já têm algum tipo de política de BYOD (traga seu próprio dispositivo) em vigor. Embora o BYOD tenha muitos benefícios, apresenta alguns riscos de segurança para funcionários remotos. Dispositivos pessoais podem não ser protegidos por senha ou podem usar software antivírus desatualizado. Para esse fim, esses dispositivos podem facilmente se tornar backdoors para cibercriminosos acessarem ativos corporativos.

O desafio existe em como oferecer uma solução orientada para o usuário final, que proteja todo o ambiente de rede doméstica, priorize as aplicações de trabalho, mas que separe claramente o trabalho do uso pessoal, garantindo a privacidade doméstica e o controle pessoal.



As empresas correram para habilitar o WFH com uma mentalidade de “conectividade em primeiro lugar”. Essas soluções não são escaláveis nem seguras. Para dar continuidade, as organizações devem modernizar suas infraestruturas e criar uma solução de longo prazo que seja segura, integrada e otimizada.

Resumo

As soluções WFH modernas precisam ir além da conectividade básica e escalar para segurança, gerenciamento e otimização de desempenho robustos e abrangentes.

Para encontrar uma solução WFH de longo prazo, as empresas devem procurar três recursos essenciais: segurança de nível empresarial, gerenciamento centralizado e facilidade de uso.

Linksys HomeWRK for Business | Secured by Fortinet é a solução WFH de próxima geração oferecida por meio da parceria entre a Fortinet e a Linksys, combinando segurança de nível empresarial, a melhor conectividade doméstica da categoria e gerenciamento em nuvem simplificado. O Linksys HomeWRK permite que as organizações levem suas soluções WFH para o próximo nível na obtenção de otimização operacional e melhores experiências digitais para os funcionários.

Saiba mais sobre como proteger a força de trabalho WFH neste resumo informativo da solução.

[1] Drew DeSilver, "Working from home was a luxury for the relatively affluent before coronavirus - not any more," World Economic Forum, 21 de março de 2020.

[2] Team Pipefy, "Pulse of Remote Work: Before & After COVID-19," Pipefy, 6 de janeiro de 2021.

FORTINET®

www.fortinet.com/br

fevereiro 23, 2023

1410900-0-0-PT