BeyondTrust

Habilite e Proteja sua Força de Trabalho Remota

Mantenha os Colaboradores Remotos Produtivos sem Prejudicar a Segurança

INTRODUÇÃO

Os departamentos de TI estão sob uma grande pressão para manter a produtividade da força de trabalho remota que, de repente, cresceu exponencialmente em poucas semanas.

Como muitas equipes de TI estão preocupadas em acomodar os funcionários para trabalhar em casa, a manutenção das práticas e da conformidade de segurança deixa de ser uma prioridade nesse momento. **E é ai que os atacantes se aproveitam para se beneficiar das atuais circunstâncias.**

Embora a tarefa de habilitar uma força de trabalho remota seja uma prática comum, **algumas questões urgentes e únicas estão sendo consideradas** pelas empresas e seus funcionários durante a crise do coronavírus.

Os atacantes são, em grande parte, oportunistas:
Os hackers procuram explorar empresas com grandes superfícies de ataque em virtude das políticas de segurança desatualizadas ou da pouca adesão às práticas de segurança durante esta crise.

As grandes não são os únicos alvos:
Pequenas e médias empresas (SMBs) e entidades governamentais estaduais e municipais, como escolas, foram os mais atingidos por surtos de malware e ataques de ransomware nos últimos anos.

ÍNDICE

IMPACTOS DA COVID-19

Quais são os principais desafios para habilitar uma força de trabalho remota segura?

Muitas empresas foram forçadas a "operar remotamente" em pouco tempo. Algumas conseguiram fornecer aos funcionários computadores que são gerenciados. Mas esse geralmente não é o caso.

As seguintes práticas relacionadas ao trabalho remoto oferecem riscos:

Práticas que Oferecem Riscos:

- Liberar a política de BYOD (bring your own device)
- Usar computadores da empresa para benefício próprio, como homeschooling (educação em casa)
- Usar ferramentas de acesso remoto pouco seguras ou desatualizadas para conectar-se à rede
- Usar "VPNs sempre ativas" para todas as conexões de usuários, mesmo quando alguns usuários precisam apenas acessar aplicativos e dados baseados na nuvem
- Abrir e-mails de phishing, que estão aumentando em função da pandemia
- Descarregar softwares maliciosos, e introduzir malware no ambiente corporativo desde casa

Recentemente, o Gartner elaborou um estudo, "Solving the Challenges of Modern Remote Access,"* para orientar os líderes de segurança e risco sobre os desafios de escalar rapidamente o acesso remoto moderno em larga escala. O estudo aponta que a **maioria das empresas possui apenas capacidade e licenças para lidar com um pequeno número de usuários, e não está preparada para permitir que todos os colaboradores trabalhem remotamente** durante eventos críticos de longo prazo, como nesse momento da COVID-19. Além disso, as companhias não possuem a largura de banda necessária para oferecer suporte a todos os usuários que trabalham remotamente, de maneira simultânea.

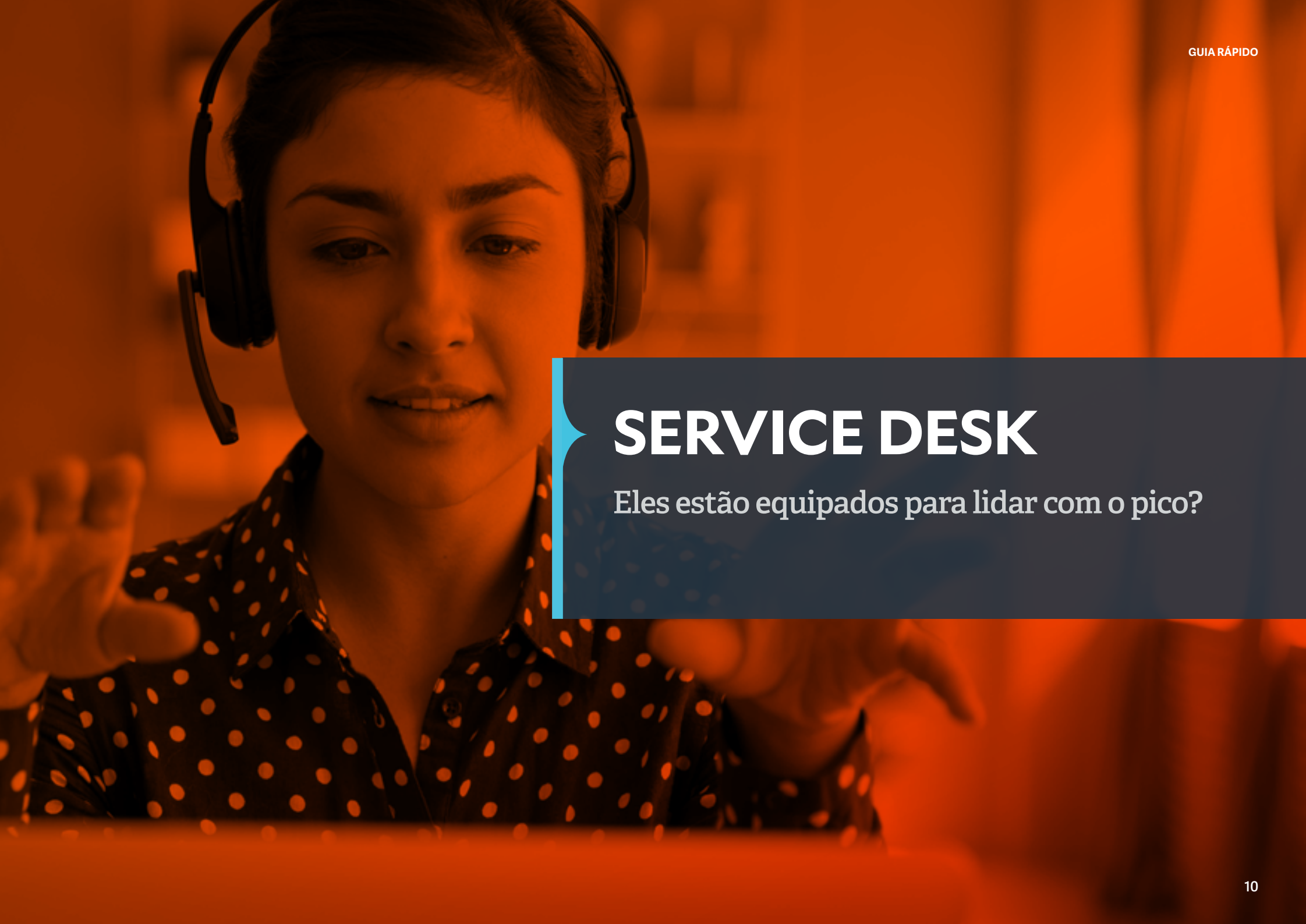
Gartner, "Solving the Challenges of Modern Remote Access," Rob Smith, Steve Riley, Nathan Hill, Jeremy D'Hoinne, 25 de Março de 2020

Práticas inadequadas de higiene de segurança cibernética podem colocar sua empresa em risco, incluindo:

- Uso de conexões de redes Wi-Fi pouco seguras
- Uso ou compartilhamento de senhas
- Compartilhamento de dispositivos
- Abertura de emails que contêm ransomware
- Armazenamento de senhas em locais não seguros, ou anotadas em um papel
- Download de softwares que podem conter malware

?

Como as empresas podem oferecer aos colaboradores ferramentas seguras para garantir a continuidade dos negócios e evitar ataques cibernéticos?



SERVICE DESK

Eles estão equipados para lidar com o pico?

A PRESSÃO NO SERVICE DESK

O trabalho remoto está demandando muito da infraestrutura e dos sistemas de TI. Isso tem um grande impacto nas equipes de service desk, que estão tentando habilitar e oferecer suporte aos colaboradores remotos enquanto eles mesmos trabalham de casa.

Ferramentas eficazes de suporte remoto impactam diretamente no sucesso do trabalho remoto. Essas soluções devem ser dimensionadas e adaptadas para atender a rigorosos requisitos de segurança, além de aumentar a produtividade do técnico.

Além disso, a solução deve ser:

POTENCIAIS CASOS DE USO

As empresas precisam de uma solução de acesso remoto seguro que possa cobrir uma lista abrangente de casos de uso, enquanto torna toda a experiência do service desk mais eficiente e segura. Alguns casos de uso comuns incluem:

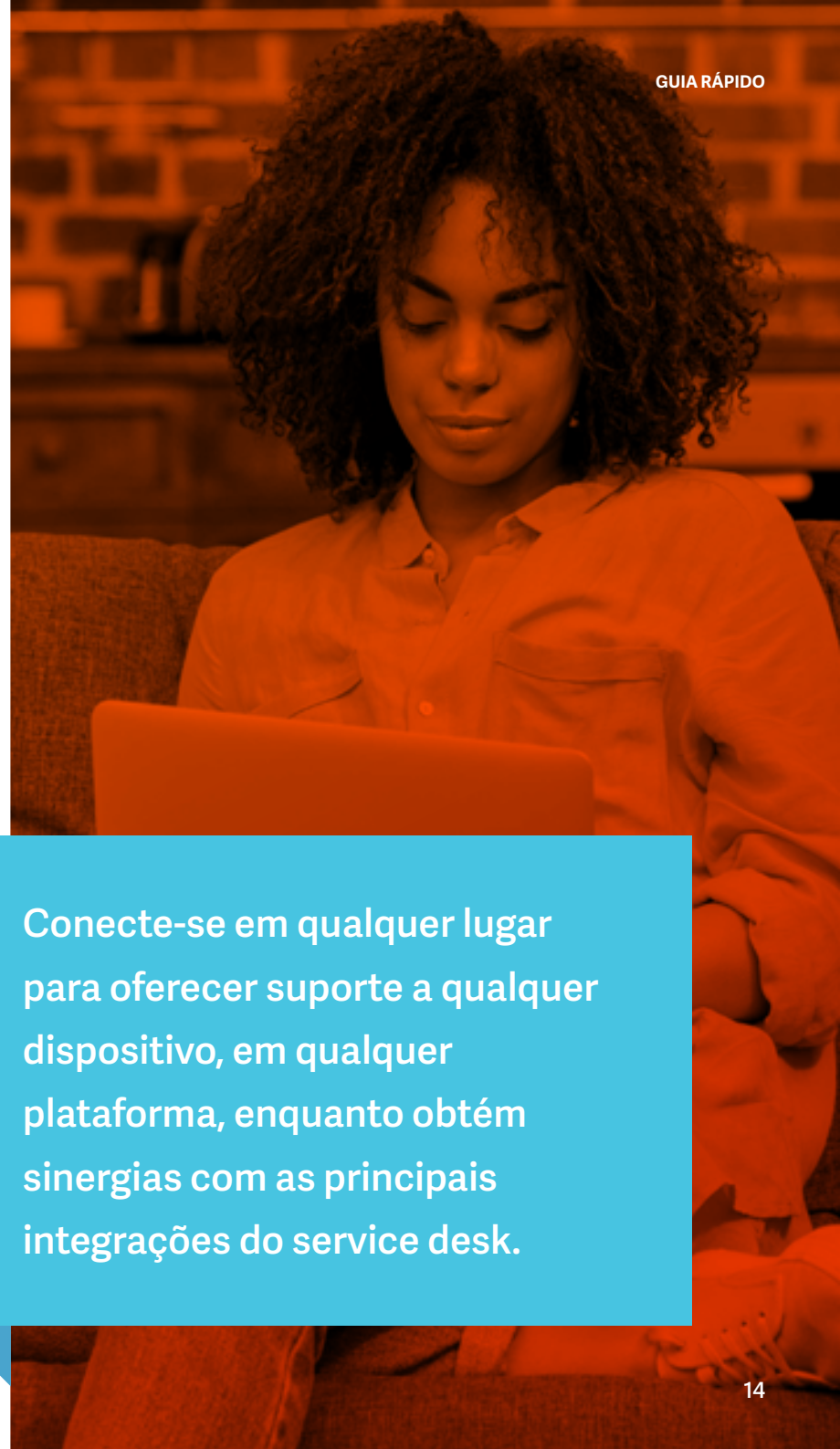
Durante esses tempos difíceis, a escolha da solução de suporte remoto correta é fundamental para a produtividade e a segurança de seu service desk

OFERECER SUPORTE A QUALQUER DISPOSITIVO OU SISTEMA, EM QUALQUER LUGAR

BeyondTrust Remote Support

Ative o suporte remoto seguro e confiável para colaboradores dentro e fora da sua rede. Tenha acesso à tela, converse, eleve privilégios e acesse a câmera do dispositivo móvel para solucionar problemas. Ofereça suporte para dispositivos Windows, Mac, Linux, iOS, Android e de dispositivos de rede com uma única solução.

O Remote Support foi desenvolvido para que o service desk funcione melhor. Nossa solução abrange a mais ampla variedade de casos de uso de suporte remoto, oferecendo segurança robusta. A BeyondTrust possui a única solução de suporte remoto que atende aos requisitos rigorosos do FIPS Nível 2.



Conecte-se em qualquer lugar para oferecer suporte a qualquer dispositivo, em qualquer plataforma, enquanto obtém sinergias com as principais integrações do service desk.

VPNs

Quem está na sua rede e o que está fazendo?

AS DEFICIÊNCIAS DAS CONEXÕES VPN.

As empresas precisam oferecer algum tipo de suporte remoto aos colaboradores, invariavelmente. Os funcionários precisam acessar seus sistemas fora do firewall. No entanto, o acesso remoto, por sua própria natureza, cria exposição a riscos. Para estabelecer conexões remotas para funcionários, as organizações geralmente usam algum tipo de rede virtual privada (VPN), permitindo assim que os usuários interajam com seus sistemas. As VPNs funcionam bem quando os funcionários trabalham com seus laptops corporativos em casa. Porém, para os que precisam acessar o desktop ou servidor corporativo a partir de um laptop ou dispositivo pessoal, ou para terceiros e fornecedores que estão se conectando aos seus sistemas, gerenciar e proteger VPNs representa um desafio.

Riscos de segurança da VPN

- VPNs permitem acesso excessivo na camada de rede
- É difícil manter as VPNs e, geralmente, elas resultam em muitos acessos quando os hosts são removidos ou substituídos
- As VPNs permitem apenas o acesso "tudo ou nada", sem níveis granulares de acesso

MITIGANDO O RISCO DAS VPNS

Os hackers normalmente precisam de dias ou semanas para descobrir o que estão buscando. Se eles obtiverem acesso a uma rede interna a partir de um sistema comprometido, poderão passar despercebidos e usar técnicas de movimentação lateral para alcançar seu objetivo final. Eles costumam ter como alvo os terceiros que utilizam métodos legados de acesso, como VPN e RDP, sabendo que são mais fáceis de serem comprometidos.

182

Número médio de terceiros* que acessam suas redes internas semanalmente, segundo os profissionais de TI.

Muitos deles têm acesso privilegiado excessivo para executar suas funções.

*BeyondTrust, "Relatório de Ameaças de Acessos Privilegiados 2019"

BeyondTrust Privileged Remote Access

O Privileged Remote Access permite o gerenciamento seguro de sessões, com a capacidade de proxy de acesso aos hosts RDP, SSH e Windows / Unix / Linux, sem a necessidade de uma VPN. A atribuição dinâmica de privilégios just-in-time, através do Adaptive Workflow Control, permite que as empresas bloqueiem o acesso aos recursos com base no dia, data, hora e local. Por exemplo, se seus colaboradores remotos fazem login em sistemas específicos, você pode garantir que o acesso seja permitido apenas a partir de intervalos de endereços predefinidos. Da mesma forma, você pode estabelecer políticas para controlar quando as contas estão acessadas e criar alertas quando determinadas políticas de acesso são solicitadas.

O uso do Privileged Remote Access com sua VPN corporativa permite que sua empresa reduza a superfície de ataque e aumente a produtividade **das seguintes maneiras:**

1. Aplicando a política de restrição de privilégios, dando a determinados usuários o nível correto de acesso
2. Habilitando a responsabilidade individual para contas compartilhadas
3. Definindo quais endpoints os usuários podem acessar e quando colocar os aplicativos em listas brancas ou negras
4. Removendo a carga administrativa de configurar e instalar VPNs para fornecedores ou funcionários remotos usando dispositivos pessoais
5. Controlando e monitorando sessões por meio de um agente seguro ou usando protocolos padrão para conexões RDP, VNC, Web e SSH

CONSIDERAÇÕES ADICIONAIS

Desempenho da VPN

A maioria das VPNs corporativas não são projetadas para oferecer suporte a todos da empresa que trabalham remotamente. Habilitar determinados usuários, como terceiros ou funcionários utilizando seus próprios equipamentos para acessar sistemas através do Privileged Remote Access, pode ajudar a reduzir a sobrecarga da VPN e aumentar o desempenho.

Além de causar problemas de segurança no ambiente corporativo, a migração para VPNs em massa pode impactar o desempenho da rede.

Riscos de grande escala em VPNs

- As tecnologias VPN geralmente carecem de escalabilidade rápida e, quando um número significativo de colaboradores ou funcionários externos precisam de acesso repentinamente, a solução pode não funcionar em um nível aceitável
- As VPNs dependem muito da largura de banda disponível na casa do usuário que está conectando e da quantidade de largura de banda que o aplicativo requer
- As VPNs normalmente não são configuradas para permitir o acesso a todos os recursos disponíveis quando alguém está fisicamente aceesando uma rede

ACESSO REMOTO SIMPLIFICADO

Use qualquer plataforma ou dispositivo pessoal

FACILIDADE PARA OS USUÁRIOS

BeyondTrust Privileged Remote Access

Os funcionários que deixaram seus desktops ou laptops no escritório podem aproveitar o Privileged Remote Access para se conectar com segurança à sua estação de trabalho, usando apenas um navegador web.

Embora muitos funcionários remotos usem o laptop da empresa, há os que não tem equipamentos fornecidos pela empresa, mas podem usar qualquer dispositivos para conectar-se à sua rede:

A BeyondTrust oferece, aos usuários remotos, o acesso aos recursos necessários para continuarem sendo produtivos, usando dispositivos pessoais ou fornecidos pela empresa.

- Dispositivos pessoais dos funcionários
- Terceiros usando laptops pessoais ou da empresa

Embora os funcionários com dispositivos da empresa sejam considerados confiáveis, os que não possuem equipamentos corporativos representam risco de segurança para a empresa, se estiverem conectados à sua VPN. Esses dispositivos podem ser usados por hackers para se infiltrar na sua rede e estabelecer uma presença persistente.

Para todos esses cenários, a **BeyondTrust permite que as equipes de TI:**

- Concedam acesso remoto granular, baseado em função, com autenticação multifator
- Forneçam uma trilha simples para os usuários remotos acessarem com segurança os recursos de rede, incluindo computadores deixados no trabalho, usando uma console da web HTML5 sem a necessidade de configurações especiais
- Forneçam e restrinjam privilégios de usuário para funcionários remotos que se conectam aos sistemas críticos

HIGIENE CIBERNÉTICA

Senhas são como germes - não as compartilhe!

O PAPEL DO GERENCIAMENTO DE SENHAS

Os funcionários remotos precisam aprender a não compartilhar senhas, uma vez que, se não gerenciadas ou controladas adequadamente, elas podem representar um grande risco de segurança para as empresas. Em geral, os usuários têm muitas senhas; como resultado, muitos funcionários geralmente compartilham, reutilizam ou armazenam senhas de maneira pouco responsável. Esses hábitos deixam seus sistemas vulneráveis a ataques.

Quando os colaboradores não lembram as senhas, geralmente costumam:

Ao considerar soluções de acesso remoto, a integração com um cofre de senhas é outro fator importante.

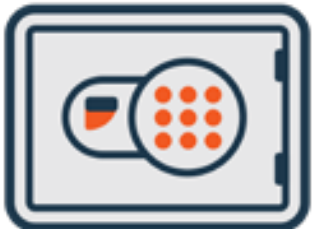
Maus Hábitos que Geram Risco

- Escrever senhas em papel
- Esquecer senhas
- Escolher senhas muito fáceis ou reutilizar senhas antigas

PROTEGER CREDENCIAIS PRIVILEGIADAS

BeyondTrust Vault

Incluído nas soluções Privileged Remote Access e Remote Support, o BeyondTrust Vault unifica o gerenciamento de sessões e o armazenamento de credenciais essenciais para usuários privilegiados internos e terceiros com uma solução simples e rápida baseada na nuvem.



BeyondTrust Password Safe

Para funcionalidades mais avançadas de gerenciamento de senhas, o Password Safe combina o gerenciamento de senhas e de sessões para descobrir, gerenciar e auditar todas as atividades de credenciais privilegiadas. O Password Safe ajuda a proteger contas privilegiadas de usuário, aplicativos, chaves SSH, contas de administrador na nuvem, contas RPA e muito mais, com uma trilha de auditoria pesquisável para conformidade e forense.

Obtenha flexibilidade para proteger e controlar o gerenciamento de credenciais privilegiadas e o monitoramento de sessões com modelos que se adaptam às suas necessidades específicas.

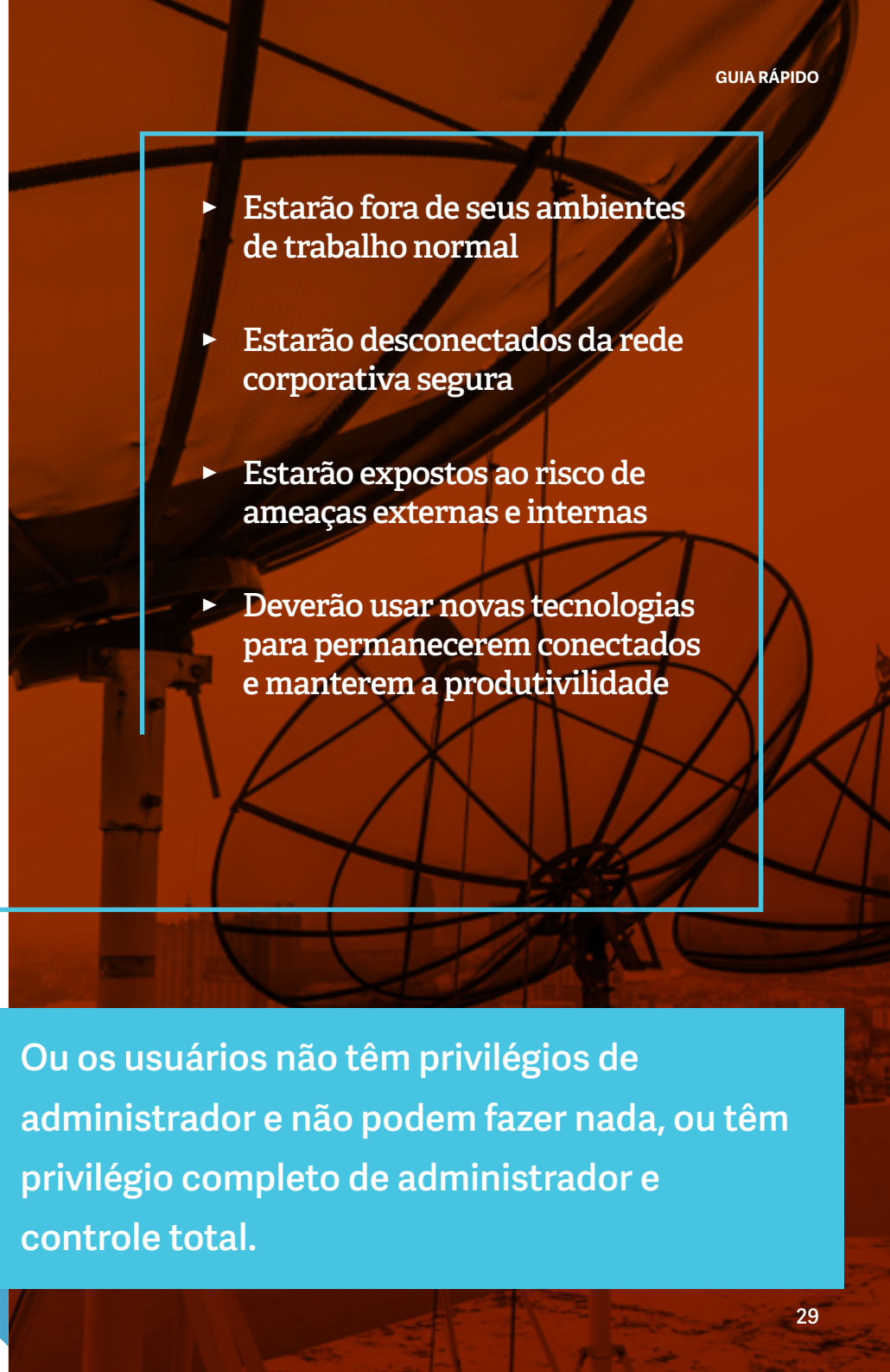
GERENCIAMENTO DE PRIVILÉGIOS NOS ENDPOINTS

Proteja Endpoints Remotos contra Ataques e Malwares

A mudança abrupta e em larga escala para o trabalho remoto não apenas interrompeu os fluxos de trabalho e processos normais dos usuários finais, como também causou estragos nos processos e políticas de segurança. Muitas organizações não estão preparadas para oferecer suporte a forças de trabalho totalmente remotas, mas a continuidade dos negócios exige que eles encontrem uma maneira de fazê-lo funcionar.

Colaboradores que se encontram repentinamente - muitas vezes pela primeira vez - forçados a trabalhar remotamente, podem enfrentar estes desafios:

Os funcionários estão pressionando o service desk para fazer mais. Porém, se eles não forem atendidos na velocidade que esperam, irão instalar ferramentas e aplicativos por eles mesmos, criando ainda mais riscos à segurança.



- Estarão fora de seus ambientes de trabalho normal
- Estarão desconectados da rede corporativa segura
- Estarão expostos ao risco de ameaças externas e internas
- Deverão usar novas tecnologias para permanecerem conectados e manterem a produtividade

Ou os usuários não têm privilégios de administrador e não podem fazer nada, ou têm privilégio completo de administrador e controle total.

GARANTA SEGURANÇA E PRODUTIVIDADE

Com o aumento de ataques cibernéticos contra funcionários remotos, é imperativo que as empresas protejam as máquinas dos usuários e evitem malware e ransomware em seu ambiente corporativo.

As soluções de gerenciamento de privilégios nos endpoints da BeyondTrust reforçam a restrição de privilégios em todos os desktops e servidores, permitindo o nível exato de acesso privilegiado que os usuários precisam - enquanto evitam que malwares e ransomwares entrem na rede corporativa. Isso permite que os usuários realizem atividades do dia a dia, como instalar e atualizar aplicativos e impressoras, câmeras, etc., sem conceder privilégios de administrador completos e sem sobrecarregar o service desk.

Ponemon Institute, "The Third Annual Study on the State of Endpoint Security Risk", Janeiro de 2020

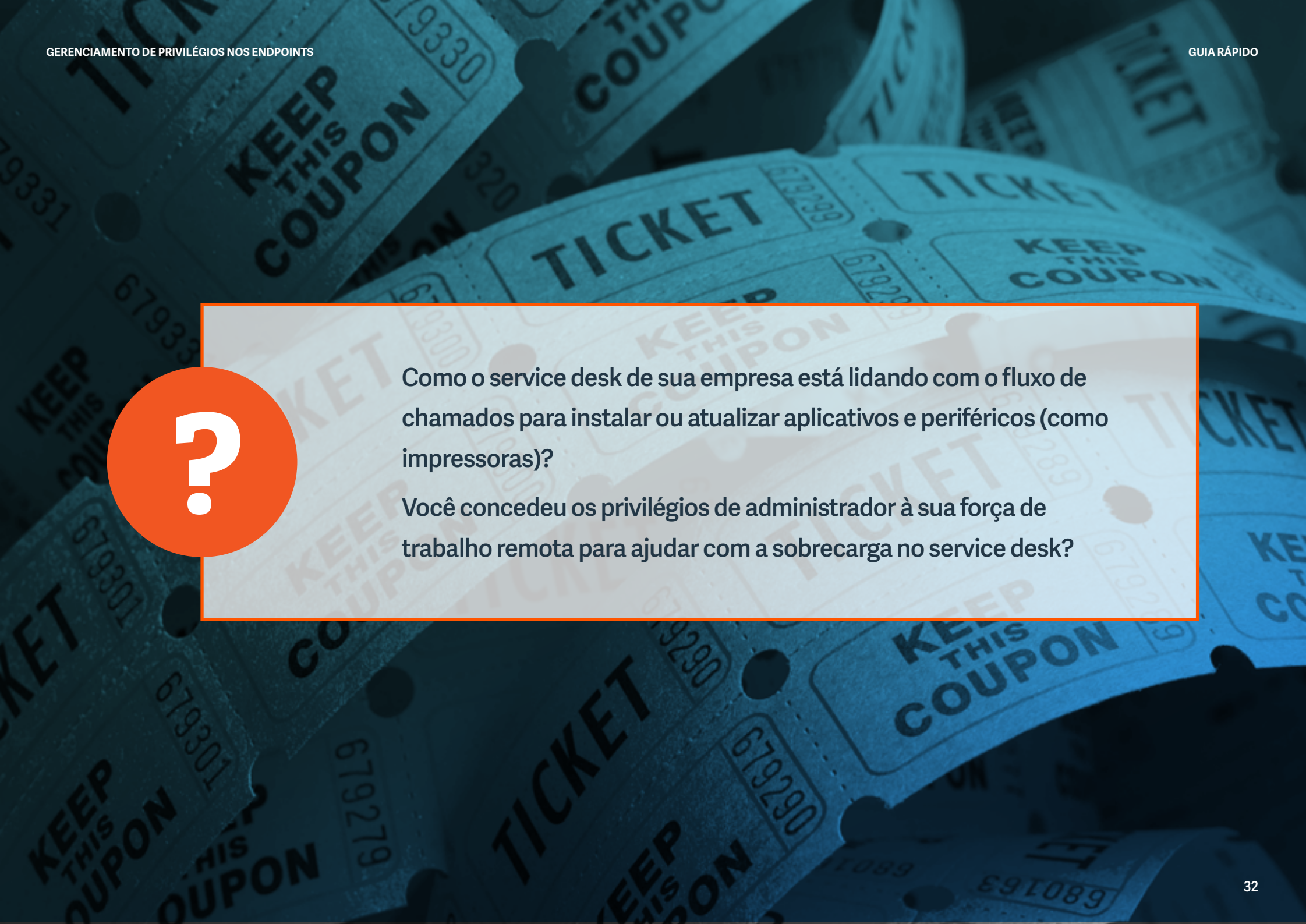
Evite os ataques não detectados pelos softwares antivírus, removendo os privilégios de administrador, implementando a restrição de privilégios, permitindo a elevação de privilégios e protegendo os aplicativos.

Com o Endpoint Privilege Management, as empresas podem implementar políticas para todos os usuários ou grupos de usuários. Além disso, nossas políticas exclusivas de Início rápido, que aproveitam os dados de milhares de implantações, permitem que os administradores de TI implementem modelos de regras flexíveis e operacionalizem rapidamente.

Com implantações globais que abrangem mais de 50 milhões de endpoints em uma infinidade de setores, nossa experiência ajudou a criar uma abordagem testada e comprovada, proporcionando um tempo-valor inigualável em todo o setor.

> “Meus clientes tiveram uma **redução de 75%** na quantidade chamados no service desk após eliminar os privilégios de administrador.”
>
> *- Sami Laiho, MVP da Microsoft e hacker ético**

**BeyondTrust, "Relatório de Vulnerabilidades da Microsoft 2020"*



?

Como o service desk de sua empresa está lidando com o fluxo de chamados para instalar ou atualizar aplicativos e periféricos (como impressoras)?

Você concedeu os privilégios de administrador à sua força de trabalho remota para ajudar com a sobrecarga no service desk?

REDUZA A CARGA DO SERVICE DESK

BeyondTrust Privilege Management for Windows & Mac

Elimine privilégios desnecessários e eleve direitos para usuários de Windows e Mac sem prejudicar a produtividade. Combinamos as melhores soluções de gerenciamento de privilégios e controle de aplicativos, simplificando a remoção de direitos de administrador para garantir conformidade, segurança e eficiência.

Recursos e benefícios incluem:

- Reduzir chamados do service desk e capacitar os usuários a instalar e executar seus próprios aplicativos pré-aprovados, com políticas prontas para uso
- Conceder aos usuários direitos de elevação ad hoc para instalar apenas aplicativos aprovados / seguros
- Promover a integração com o ServiceNow e outras ferramentas de ITSM para automatizar o envio de um ticket ao service desk, para que eles possam tomar uma decisão informada e rápida sobre a solicitação do usuário para executar um aplicativo, instalação, script ou tarefa
- Corrigir rapidamente um problema - para todos os usuários - através de amplas atualizações de políticas
- Capacitar os usuários a auto-instalar impressoras e outros periféricos

?

Como você pode impedir que os usuários introduzam malwares e ransomwares em seu ambiente?

O BeyondTrust Privilege Management para Windows e Mac reduz a superfície de ataque das seguintes maneiras:

1. Restringindo privilégios no ambiente de desktop e nos servidores - mantendo a segurança, a produtividade do usuário e a eficiência operacional
2. Interrompendo ataques envolvendo aplicativos confiáveis, capturando scripts incorretos e anexos de email infectados em tempo real
3. Usando uma lista de permissões automatizada e tratamento de exceção para fornecer controle completo sobre o que os usuários podem instalar ou executar
4. Fornecendo uma única trilha de auditoria de todas as atividades do usuário para otimizar a análise forense e simplificar a conformidade
5. Correlacionando o comportamento do usuário com dados de vulnerabilidade de ativos e inteligência de segurança para avaliar o risco do usuário com análises avançadas de ameaças

AGORA É A HORA

Habilite os trabalhadores remotos já!

ENTRE EM OPERAÇÃO COM UMA IMPLANTAÇÃO SIMPLES E RÁPIDA

As soluções BeyondTrust estão disponíveis em várias opções de implantação, incluindo appliances virtuais e SaaS, que começam a funcionar rapidamente. Com as soluções de acesso remoto seguro da BeyondTrust, não são necessários downloads de agentes de desktop - os usuários podem efetuar login através de um console da Web a partir de qualquer navegador. Para o Endpoint Privilege Management (EPM), os agentes são implantados rapidamente nos endpoints, com políticas aplicadas - sem interrupção para os usuários.

A administração e os fluxos de trabalho simplificados ou automatizados também aliviam a carga das equipes de TI. A seguir, estão os benefícios do uso das soluções da BeyondTrust:

OS BENEFÍCIOS

Caminhos de Acesso Consolidados	Rastreando o Acesso	Aplicativos Móveis	Trilha de Auditoria	Políticas de Início Rápido (EPM)
Intermedie todas as conexões por um único caminho de acesso, reduzindo a superfície de ataque e fornecendo uma lista única de endpoints autorizados para cada usuário	Defina as preferências quando um fornecedor / usuário privilegiado estiver acessando sua rede / sistemas ou quando uma sessão iniciada por acesso remoto estiver ocorrendo	Os administradores podem usar seus dispositivos móveis para aprovar solicitações e monitorar o uso do acesso de qualquer lugar	Grave todas as sessões para atender aos requisitos de conformidade e para uso em análises forenses, entre outros	Mantenha a segurança, a produtividade do usuário e a eficiência operacional de TI, aplicando a restrição de privilégios no ambiente de desktop

A BeyondTrust permite que as organizações apliquem a restrição de privilégios e controles de auditoria robustos a todos os acessos remotos exigidos por funcionários, fornecedores e centrais de atendimento. Os usuários podem acessar de forma rápida e segura qualquer sistema remoto, executando qualquer plataforma, localizada em qualquer lugar e aproveitar um cofre de senhas integrado para descobrir, integrar e gerenciar credenciais privilegiadas.

Obtenha visibilidade e controle absolutos do acesso remoto interno e externo, conectividade segura aos ativos gerenciados e crie uma trilha de auditoria completa que garante a conformidade.

Além disso, impeça os usuários de baixarem softwares maliciosos e abrirem anexos de phishing perigosos que podem causar danos enormes no ambiente corporativo.

Tudo isso reduzindo o fluxo de tickets no service desk e continuando a cumprir os regulamentos de conformidade.

Nossa abordagem cria uma experiência tranquila para os usuários, permitindo o nível certo de acesso no momento certo.

BeyondTrust

SOBRE A BEYONDTRUST

A BeyondTrust é líder mundial no Gerenciamento de Acessos Privilegiados (PAM), capacitando as organizações a proteger e gerenciar todo o seu universo de privilégios. Nossos produtos e plataformas integrados oferecem a solução PAM mais avançada do setor, permitindo que as organizações reduzam rapidamente sua superfície de ataque nos ambientes tradicionais, em nuvem e híbridos.

A abordagem do Gerenciamento Universal de Privilégios da BeyondTrust protege privilégios em senhas, endpoints e acessos, oferecendo às organizações a visibilidade e o controle necessários para reduzir riscos, obter conformidade e aumentar o desempenho operacional. Mais de 20.000 clientes confiam na BeyondTrust, incluindo 70% das empresas da Fortune 500 e uma rede global de parceiros.

Saiba mais em beyondtrust.com/pt/remote-workers