BeyondTrust

OFEREÇA ACESSO. NÃO UMA VPN

A solução de gerenciamento de acessos privilegiados da BeyondTrust permite que os profissionais de segurança controlem, monitorem e gerenciem os acessos de usuários privilegiados e terceiros aos sistemas críticos da empresa. Com a BeyondTrust, você pode:

- Eliminar a base que os atacantes podem ganhar em seu ambiente
- Manter o controle granular do acesso à sua rede
- Monitorar e auditar sessões de acesso em tempo real
- Registrar os dados de segurança de sessões diretamente na sua ferramenta SIEM
- Atenuar ataques de personificação
- Diminuir o tempo de resposta a incidentes
- Realizar investigações forenses eficazes
- Atender aos requisitos de auditoria e compliance

beyondtrust.com

Você sabia?

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 pivot para alcançar seu objetivo final. Eles costumam ter como alvo os terceiros que utilizam métodos de acesso legados, como VPN e RDP, sabendo que são mais fáceis de ser comprometidos. A BeyondTrust oferece acesso aos sistemas sem precisar de uma VPN.

Em média, é o tempo que uma empresa leva para perceber que sofreu uma violação. No caso de o acesso de um fornecedor ser comprometido, qualquer atividade mal-intencionada é interrompida quando a sessão da BeyondTrust atinge o tempo limite, em comparação com uma VPN, na qual o hacker tem liberdade até que seja detectado.

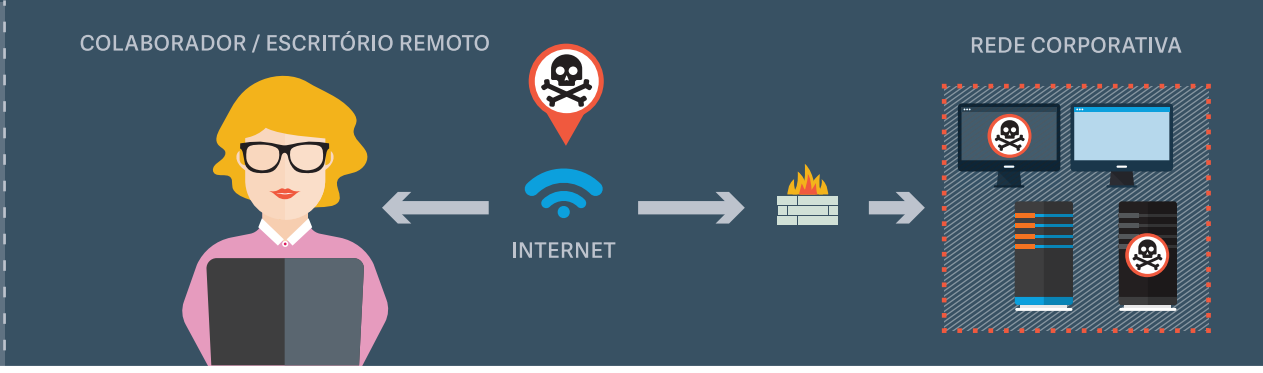
80% das violações envolvem uma conta privilegiada explorada. Para um hacker, os terceiros geralmente são a maneira mais fácil de ataque à sua rede.

62%

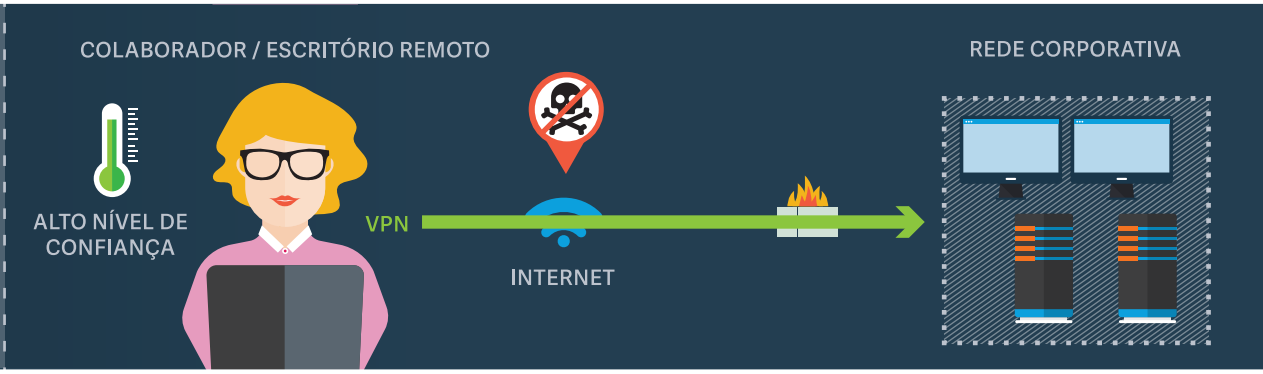
62% Quase dois terços das empresas acredita que gerenciar os direitos de identidade e acessos é uma tarefa complexa. Em média, as organizações têm 1.200 solicitações de acessos por mês. A BeyondTrust aborda essa complexidade, permitindo que os administradores gerenciem, monitorem e auditem os acessos sem interromper os processos.

ERA UMA VEZ...

o maior risco de segurança eram os ataques MItM (Man in the Middle) em uma conexão remota à sua rede.

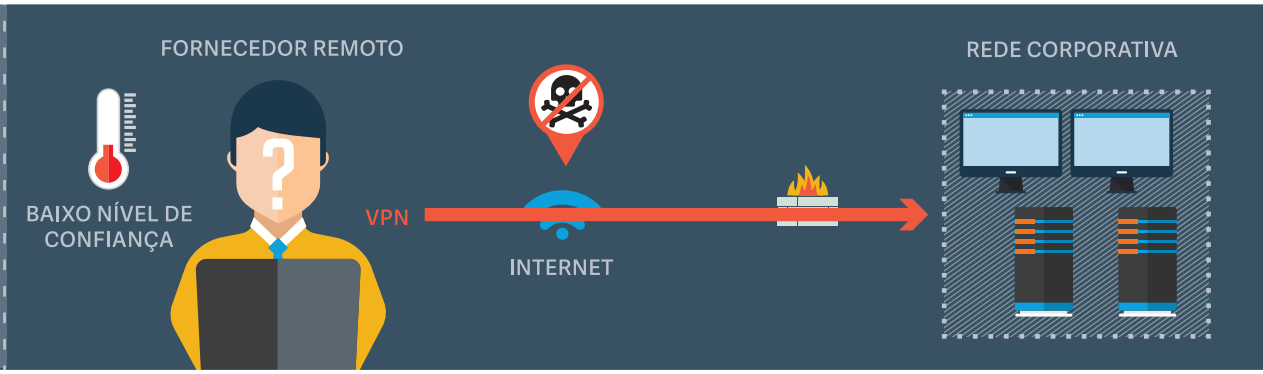


As empresas começaram a implementar VPNs para fornecer um túnel criptografado para funcionários e escritórios remotos acessarem a rede, interrompendo os ataques do tipo MitM.

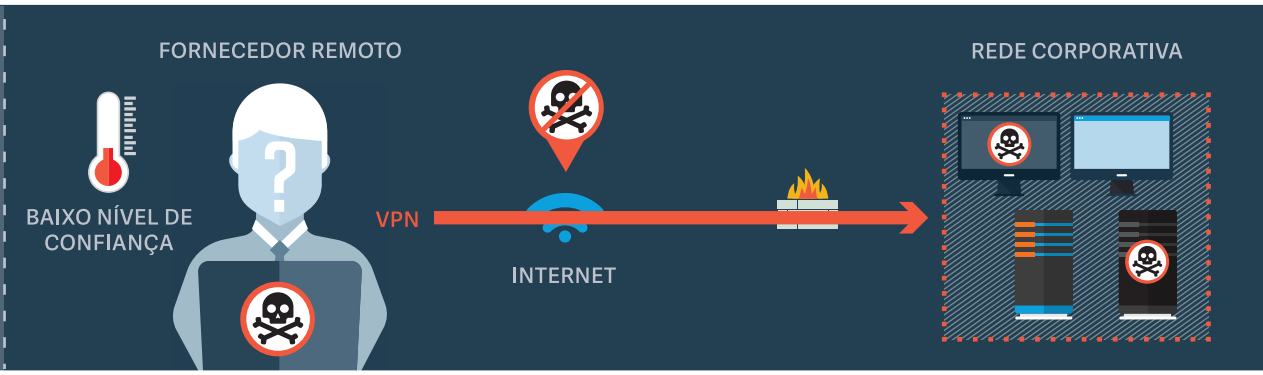


MISSÃO SECRETA!

Como terceiros e fornecedores começaram a exigir acesso privilegiado às redes, as empresas concederam acesso a eles usando a melhor ferramenta disponível – VPNs.



No entanto, os ciber-criminosos descobriram que um fornecedor com uma conexão VPN é alvo perfeito para eles conseguirem entrar em uma rede segura. Com essa base na VPN, eles têm acesso e tempo para encontrar e atacar sistemas sensíveis.



OFEREÇA ACESSO SEM UTILIZAR VPNS!

A solução de gerenciamento de acessos privilegiados da BeyondTrust permite que você ofereça aos usuários externos acesso à sua rede sem precisar de uma conexão VPN, e sem conectar diretamente aos seus sistemas internos de maior valor, que são o que eles mais almejam.

Ainda evitamos os ataques MitM

A solução da BeyondTrust permite que você aplique permissões de acesso granular ou exija aprovações para acesso a fornecedores. Ela também captura trilhas de auditoria e gravações de vídeo de todas as atividades do usuário externo.

Nenhuma modificação do firewall. O usuário remoto é conectado por meio de uma conexão ao appliance da BeyondTrust, NÃO ao sistema de destino.

Com a BeyondTrust, você pode definir quais sistemas podem ser acessados por usuários externos, além de quando e por quanto tempo eles podem permanecer em sua rede.