BeyondTrust

GIVE THEM ACCESS. NOT A VPN

BeyondTrust's Privileged Access Management Platform enables security professionals to control, monitor, and manage access to critical systems by privileged users, including third-party vendors. With BeyondTrust, you can:

- Eliminate the foothold attackers can gain inside your environment
- Maintain granular control of access to your network
- Monitor and audit access sessions in real-time
- Log session security data directly to your SIEM tool
- Mitigate impersonation attacks
- Decrease incident response times
- Run effective forensic investigations
- Satisfy audit and compliance mandates

beyondtrust.com

did you know?

Hackers typically need days and weeks to find what they are after. If they obtain VPN access from an exploited system to an internal network, they can often move around undetected and use pivoting techniques to find their ultimate target. Hackers regularly target third-party vendors with legacy access methods like VPN and RDP to a secure network knowing they're easier to compromise. BeyondTrust gives vendors access to the systems they need with no VPN, eliminating the threat of hacked vendor VPNs.

On average, that's how long it takes an organization to realize they've been breached. In the case that a vendor's access was compromised, any malicious activity would be stopped once a BeyondTrust session times out versus with a VPN where the hacker has free reign until they are detected.

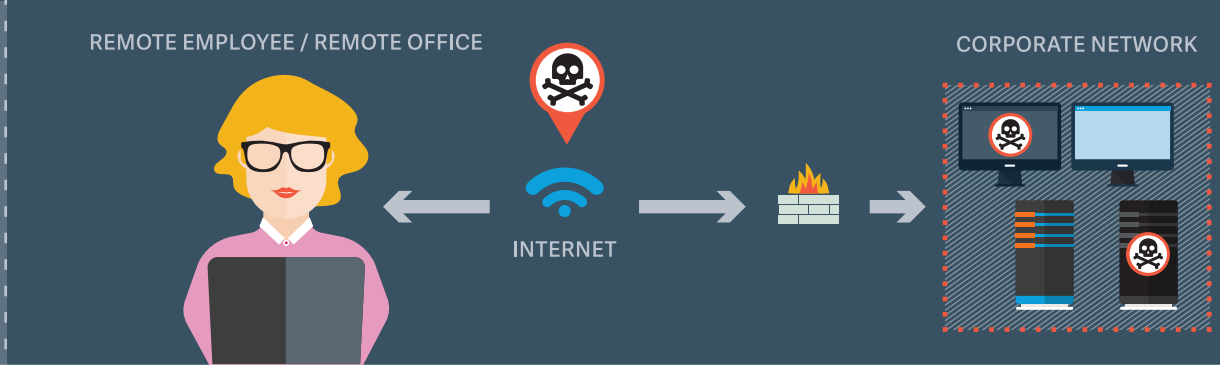
80% of breaches involve a privileged account being exploited. The security posture of your vendors may vary significantly. Hackers know this and can view your vendors as an easier way to attack your network.

62%

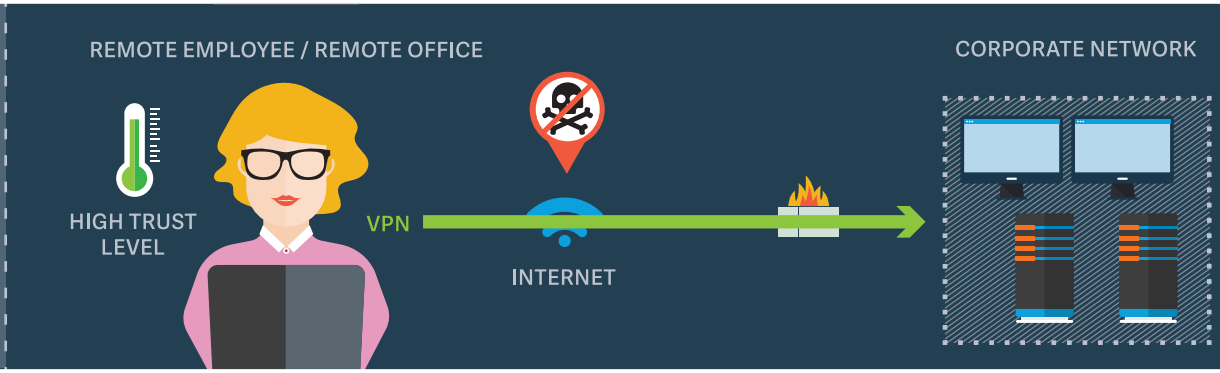
Close to two-thirds of organizations believe that managing identity and access rights in their organization is too difficult. On average, organizations have 1,200 access requests per month. BeyondTrust addresses this complexity by enabling admins to centrally manage, monitor, and audit access without disrupting processes.

ONCE UPON A TIME...

The biggest security risk was a MitM (Man in the Middle) attack on a remote connection to your network.

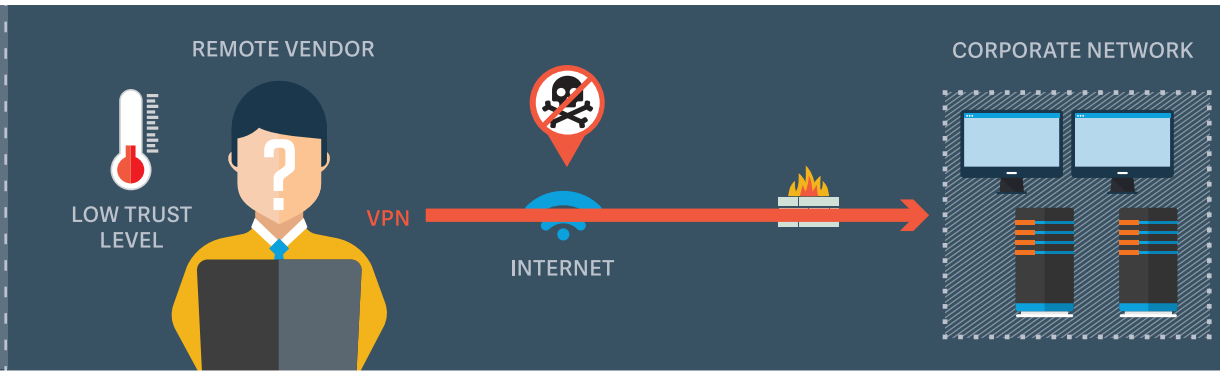


Companies began implementing VPNs to provide an encrypted tunnel for trusted roaming employees and remote offices to access the network, stopping the MitM attacks.

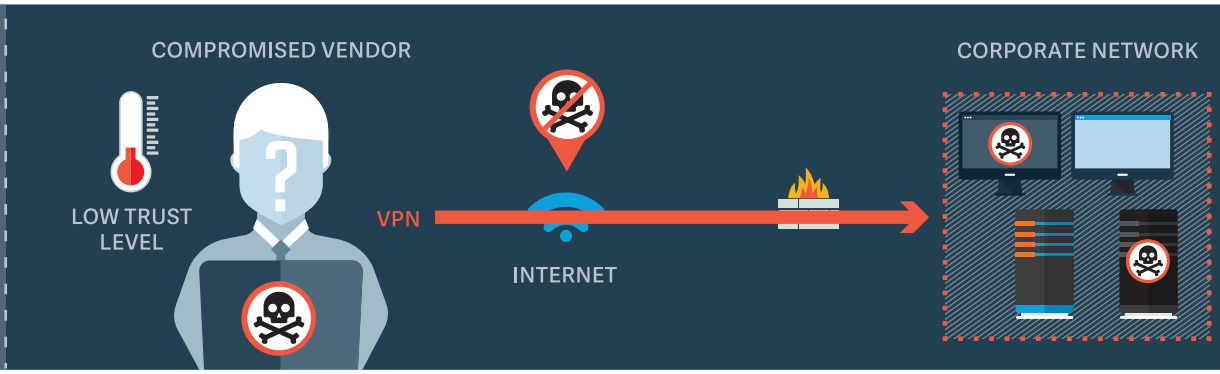


MISSION CREEP!

As 3rd parties and vendors began requiring privileged access to their networks, companies gave them access using the best tool available – VPNs.



Cybercriminals learned that a vendor with a VPN connection is the perfect target for gaining access to a secure network; with that VPN foothold, they have the access and time to find and attack sensitive systems.



GIVE VENDORS ACCESS WITHOUT VPNS!

BeyondTrust's Privileged Access Management solution allows you to give vendors access to your network without a VPN connection and without connecting directly to your highest-value internal systems.

We still prevent the MitM attacks

BeyondTrust allows you to apply granular access permissions or require approvals for vendor access, and captures a searchable audit trail and video recording of all vendor activity

No firewall modifications needed; remote vendors connect through an outbound-only connection to the BeyondTrust appliance, NOT the target system

With BeyondTrust you can set which systems vendors can access, when, and for how long so they can't pivot around or linger in your network.

V2019_03_ENG