Secure Remote Access for Employees and Vendors

Modern network security is a complex problem. Organizations need to provide secure access to a variety of users—including IT administrators, data center teams, employees, contractors, and third-party vendors—without hindering productivity.

However, the rise of cloud computing, bring-your-own-device (BYOD) policies, remote work, and the widespread adoption of SaaS applications across corporate IT stacks means traditional perimeter-based security is no longer sufficient. With so many users and devices connecting to a network from different locations, organizations need to verify identity and grant access to the right resources on a more granular level.

This is especially difficult when working with third-party suppliers because they often need privileged access. The issue is that organizations often have little control over third party devices and mandating Endpoint Detection and Response (EDR) or Mobile Device Management (MDM) solutions for those devices is often out of the question.

So how can your organization confidently secure the most sensitive and privileged access to your data and resources?

How to solve

Your security plan needs to implement granular control over your endpoints and user access through continuous authentication of both identity and device, using phishing-resistant MFA and least privilege access controls for all remote access.

Traditional solutions, like VPNs, provide broad access to resources. If an attacker accesses one resource, they have access to all of your data and resources. Additionally, VPNs often depend on legacy MFA for identity validation, which relies on shared secrets and weak factors like passwords, SMS push, OTPs and other perishable factors..

Even if you can securely authenticate your remote users, the devices they are using to access the network may not meet corporate security posture which presents vulnerabilities. This is especially true for the third-party vendors accessing your environment.

Continuous authentication of user and device using strong phishing-resistant factors and security policies is the key to securing your data and resources.

The solution

Deploying Beyond Identity with BeyondTrust will allow your organization to implement a zero trust architecture through comprehensive, remote access security and reliable authentication for every endpoint.

Beyond Identity's frictionless authentication solution seamlessly integrates with BeyondTrust to enable organizations to build more secure access policies with less hassle. And if Beyond Identity's continuous authentication detects that one of your devices has fallen out of device security compliance, BeyondTrust is notified and is able to disconnect that device. The integration effectively allows you to control what devices are entering your environment without the use of MDM or EDR.

Features

- **Centrally manage and secure remote access** for service desks, IT admins, and vendors.
- **Secure identity authentication** with phishing-resistant, passwordless, MFA so you always know who is remotely accessing your applications.
- **Secure device authentication** by defining device security posture thresholds for both internal users and third-party vendors.
- **Ensure devices are sanitized and compliant with corporate policy** from session inception to termination through continuous monitoring. If a device falls out of compliance, Beyond Identity automatically terminates the session.
- **Prove compliance with detailed session data** that combines BeyondTrust native monitoring with Beyond Identity's immutable audit record of every user, device, and resource being accessed, critical for forensic and compliance.
- **Manage unattended access to thousands of systems** as your infrastructure grows.
- **Securely access any remote device** on any platform located anywhere in the world.

Key benefits

Password elimination: Leverage the technology built into modern devices to provide secure authentication through biometrics and the Trusted Platform Module.

Phishing-resistant authentication: Lack of one-time passwords (OTP), security questions, and interceptable push notifications means no potential for compromise through phishing attacks.

Zero trust foundation: Establish zero trust by combining phishing-resistant, frictionless MFA that cryptographically binds identity to the device with privileged access controls that enforce least privilege across users and devices.

Secure vendor access: Take control of vendor access to critical systems by combining role-based access with fine-grained device security posture policies without requiring an MDM or VPN.

Frictionless insider access: Give remote workers and service desk employees seamless access to the systems needed to do their jobs with secure, phishing-resistant MFA.

Continuous monitoring: Continuously enforce granular, risk-based access policies throughout a session, disconnecting devices that fall out of compliance in real time.

Immutable audit and enforceable compliance: Audit privileged user activity with an immutable audit record and enforce compliance requirements continuously.

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.