How to Manage Secure Access for Contractors and Third-Parties

Companies increasingly rely on third-party vendors, including contractors and consultants. From hiring freelancers to outsourcing entire business functions, these critical members of the workforce help businesses scale faster and stay competitive. But as the number of people with access to corporate resources grows, so does the risk of security breaches. Fortunately, you don't have to choose between growing your business and protecting it.

Scale securely to avoid growing pains

$4.35 million Average cost of a data breach in 2022

Remote access to your network and data is often a necessity for contractors and third-party vendors to fulfill their roles. However, as your company grows, so does your attack surface and the common threats of intrusion, phishing, and malware.

While you may have robust systems and processes to protect your internal network from attacks, a lack of visibility and control over your vendors' endpoints means you still have holes in your security.

And as more and more companies turn to third-party vendors and contractors to support their business, the problem is only set to grow. With the average cost of a data breach reaching an all-time high of $4.35 million in 2022, it's vital to close the loop on remote access vulnerabilities, whether it's an employee using BYOD or a third party contractor or consultant on an unmanaged device.

Don't use old methods to manage modern threats

Traditionally, companies have managed access to their networks and data using tools like virtual private networks (VPNs), mobile device management (MDM) software, and privileged access management (PAM) solutions. However, given that your goal is to ensure only authorized users can access your network and cloud resources on a secure device, these methods aren't up to the task.

In particular:

They have security flaws: Malicious actors can exploit weak VPN protocols to gain access to your network. As VPNs grant full access to the network, once a hacker is in, they can do unmitigated damage.

They're unpopular with users: Many people don't want to implement these solutions on their personal devices. MDM software, especially, is rife with privacy concerns, and while you can insist employees adopt it, you may not have the same level of influence over contractors or consultants.

They're inefficient: Each method is expensive and difficult to scale, and managing them can tie up your IT team in unproductive admin work.

Implement stronger security

The key to enabling vendor access without compromising your company's security is adopting a combination of practices that address modern attack vectors.

Passwordless MFA: With stolen credentials at the root of 86% of web application breaches, employing passwordless multi-factor authentication is essential. By eliminating inherently insecure passwords in favor of immutable credentials backed by private keys, you can strengthen your security posture significantly. Passwordless means no passwords at all. Some cybersecurity companies promise passwordless MFA, but store a backup password in a database for account retrieval. This allows the same risk for data breach that password-based MFA does.

Risk-based authentication: For stronger access controls, risk-based authentication lets you automatically analyze a variety of risk signals from the device, user, and application every time a user requests access to your resources. Depending on your risk tolerance, you can customize your risk policy and the attributes you examine.

Zero trust authentication: Zero trust security works by never trusting a user and always verifying them during their session. Zero authentication should continuously authenticate the user as they access different resources and lay the foundation for a zero trust architecture. For example, even though a user gains network or application access, their risk level may change and they are denied access to a service.

Although you can't control the security policies of your third-party vendors like contractors and consultants, you can implement each of these best practices. Beyond Identity can help you secure remote workers using BYOD and unmanaged devices to truly protect your organization.

Make it simple to comply with your security standards

By making your security measures frictionless and unobtrusive for third-party vendors, everyone wins. With our passwordless MFA, you control who's accessing your corporate resources and verify their device security posture—wherever they're logging in—without making it arduous for the user.

Book a demo today and find out how easy it is to effectively close the loop on your remote access vulnerabilities.

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 use Beyond Identity, check out www.beyondidentity.com.