BYOD Security Risks:

Why Passwords and Traditional MFA Leave Gaps

BEYOND IDENTITY

BEYOND IDENTITY

CONTENTS

BEYOND IDENTITY

BYOD Security Risks

Why Passwords and Traditional Multi-Factor Authentication Leave Gaps

Bring your own device (BYOD) policies can greatly improve business productivity, especially when employees work from home, but this advantage also increases security risks from potential malware attacks (e.g. ransomware) to compromised email accounts.

Controlling internal machines is hard enough for administrators, but securing personal devices is a different and more difficult challenge. Not only must administrators ensure that devices are secure, but they must also differentiate between devices that should be legitimately authorized on the network versus blocking shadow IT machines used for malicious purposes. Shadow IT devices aren't always malicious, but shadow IT devices can be connected to the network without authorization and can cause compliance and security concerns and expand your attack surface.

Does multi-factor authentication solve BYOD security challenges?

The introduction of multi-factor authentication (MFA) was geared toward eliminating risks of weak passwords, poor BYOD management, credential theft from phishing, and sophisticated brute-force attacks. While MFA helps, it's not a complete solution and often gives administrators and users a false sense of security. Security experts will tell you that risk can never be reduced 100%, but MFA has long been advertised as the destroyer of unauthorized network access from compromised credentials. Even though it does not reduce risk entirely, MFA has always been the de facto answer to poor password security.

When new security is introduced, attackers will change their strategies to overcome the new cybersecurity technology and bypass defenses. They find a way to overcome any new cybersecurity methods. MFA is no different, and several bypass strategies are currently available and leave typical authentication procedures ineffective. Some bypasses are well known while others are more sophisticated and difficult to detect.

The biggest vulnerability in MFA is the human element. Verizon research into common human errors indicated that 57% of data breaches come from insider threats. A 2020 Verizon report showed that 80% of data breaches are from lost or stolen credentials. These threats aren't always intentional or malicious, but employees don't always understand cyberattacks and can therefore become components in accidental mistakes, leading to a compromise from lack of cybersecurity knowledge.

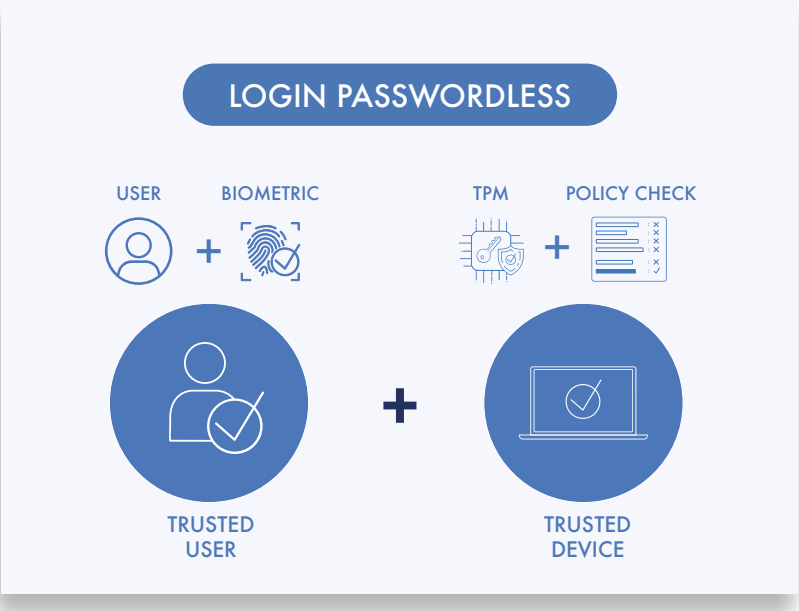
57% of data breaches come from insider threats

80% of data breaches are from lost or stolen credentials

Bypassing MFA is one concern, but the biggest disadvantage of standard MFA strategies is their inability to validate security on user devices. MFA could work perfectly, but a user device could still contain vulnerabilities. For example, the user could successfully authenticate into the environment but nothing ensures the security of their device using MFA. The user is the legitimate owner of the device, but the device itself could be an attack vector used to bypass authorization controls.

With BYOD, a user is free to install any application, and these applications could contain rootkits, ransomware, keyloggers, and any other malicious applications. When the user authenticates into the network using the compromised device, malware could potentially steal data, install ransomware on the network, or unleash payloads opening backdoors for other attacks. After the network is compromised, advanced persistent threats can remain hidden in the environment for months, leaving a large window of opportunity for data exfiltration.

All these attacks are possible even with an effective MFA system in place, which means organizations need a better way to authenticate users, while also ensuring the security of their devices.



Managing BYOD security using passwordless authentication

Device security and authorization are necessary, but the challenge organizations face is giving users the ability to use their own devices to connect to the network, while also finding ways to ensure that device security is validated. MFA is traditionally used as a security layer to ensure that the organization is protected against a hacker using compromised credentials, and it often gives users and administrators a false sense of security. This strategy works well for basic authentication security, but it still leaves the organization vulnerable to sophisticated device-level attacks.

Although personal devices need valid security to connect to the network, they still belong to the employee, not the company. A corporate device can have any number of applications and configurations installed, but personal devices must be secured without being too intrusive. Corporations can't fully control personal devices, but they must be able to put the right security in place to ensure compliance regulations are followed and devices are protected from malware. Remote wiping capabilities are possible with corporate devices, but these programs are too intrusive for a user's personal device.

Operations people and security administrators attempt to wrestle with many risks on an internal network. Antivirus and anti-malware is installed on all network devices. Monitoring systems detect suspicious activity and user behaviors. Scanning systems find vulnerabilities on the network and alert administrators for necessary intervention to remediate issues. Those steps are necessary and possible on internal network devices, but personal devices are much more difficult to control and protect.

Technically, passwordless authentication is also multi-factor authentication, but it adds security without friction for the end user. A key challenge for administrators is differentiating between a shadow IT device, a malicious device making authentication requests, and a valid user device making requests to access network resources when they work from home or travel. With passwordless authentication, cryptographically secure keys tie a user's identity to the device and incorporate biometrics to ensure the person currently on the device is a valid user.

Biometrics are used less often as a factor within MFA but are a very secure alternative factor that can be used. Many organizations, however, make the mistake of storing those values in the cloud. The cloud is often touted as a safer alternative to storing sensitive data on-premises, but it can also be an attacker's opportunity to compromise a system if resources are not configured properly. The solution to that problem, and the many other credential-based authentication systems, is to eliminate magic links, text messages, push notifications, and server-side stored biometrics and replace them with proven public key infrastructure (PKI) and hardware security.

Beyond Identity introduced a patented, effective way to eliminate passwords and solve the challenges administrators battle every day with MFA weaknesses. It binds security to the device, so any user device is validated instead of potentially stolen or compromised credentials being validated.

Old Virtual Private Network (VPN) systems are no longer a valid way to authorize user access for BYOD devices, and Beyond Identity's passwordless platform can replace VPNs and instead authenticate users using private keys stored in the Trusted Platform Module (TPM), binding a user's identity to a device. That system solves challenges with VPN and the maintenance and removes the security risks that comes with using VPNs.

On an additional note, Beyond Identity solves the problems of user frustrations and the constant struggles administrators face to enforce traditional password authentication and cybersecurity policies. Users often complain of how cybersecurity controls make the entire authentication and authorization process inconvenient. It's for that reason that users are compelled to find ways to disable cybersecurity controls, including MFA systems. Beyond Identity also addresses privacy concerns, because the platform can ensure a device is secure without giving an employer full access to that device or ability to wipe the device, unlike a mobile device management product. It's a win for security and for employee privacy.

Beyond Identity seamlessly integrates with user devices so that they can continually authenticate and authorize access in a frictionless way behind the scenes and without frustrating traditional interfaces. The Beyond Identity solution performs all necessary authentication and authorization without using any insecure and friction-filled factors like one-time codes, magic links, or passwords.

BEYOND IDENTITY

Remove passwords and avoid common BYOD security pitfalls

Instead of relying on users and very weak factors like passwords and SMS text messages, Beyond Identity uses the strongest authentication factors possible—biometrics, device-level validation, and cryptographic keys. BYOD adds risk to your security, but you can reduce that risk by using Beyond Identity's convenient, frictionless, and effective passwordless solution. Our solution keeps your organization compliant, sets the foundation for zero trust, and improves security posture across your organization.

To get started with next-level advancements in security, get a demo.

ABOUT BEYOND IDENTITY

Beyond Identity provides the most secure authentication platform in the world. Breaking down barriers between cybersecurity, identity, and device management, Beyond Identity fundamentally changes the way the world logs in–eliminating passwords and providing users with a frictionless multi-factor login experience. Beyond passwordless, the company provides the zero-trust access needed to secure hybrid work environments, where tightly controlling which users and which devices are accessing critical cloud resources has become essential. The advanced platform collects dozens of user and device risk signals during each login - enabling customers to enforce continuous, risk-based access control. The innovative architecture replaces passwords with the proven asymmetric cryptography that underpins TLS and protects trillions of dollars of transactions daily. Customers turn to Beyond Identity to stop cyberattacks, protect their most critical data, and meet compliance requirements.