yubico

How to best protect your mobile-restricted environment

What is a mobile-restricted environment and what unique requirements does it have?

“Mobile-restricted” describes any sensitive environment where mobile devices are not allowed, are not reliable or must be limited because of security concerns. Nearly every organization has a use case where using mobile devices is either not permitted or not possible. And, the steady stream of cybercrimes covered in the news recently have pushed security teams to think more strategically about how to protect these sensitive workspaces.

Mobile-restricted environments can be found across a wide range of sectors and industries that host these environments and where cell phones are restricted as a security concern. These environments can be found across industries such as Financial services, Manufacturing, Retail, and Hospitality, as well as specific work environments that exist in every industry such as Call Centers. The concept of “mobile-restricted” might also apply to any environment where connectivity issues might hamper collaboration or productivity, such as in an industry like Energy and Natural Resources where work may be taking place in very remote locations without cellular connectivity. For all of these scenarios, authenticating users using legacy multi-factor authentication (MFA) such as mobile authentication is simply not a viable option. Organizations therefore need to look for modern and effective ways to securely authenticate users before giving them access to sensitive resources.

Key considerations in choosing the ideal MFA solution

Any authentication solution that serves a mobile-restricted environment must balance the two poles of security and usability. Where this balance rests will depend on conditions on the ground, user access needs and particular industry requirements and standards. But a good rule of thumb is to ask how much “hassle-factor” your users can withstand before they begin not complying with procedures or start looking for shortcuts.

Use the following as a checklist to see if the authentication solution you’re considering can meet the critical requirements of a mobile-restricted scenario.

Adaptable for shared workstations

Mobile-restricted environments often include shared workstations, and those stations may have special login and logout requirements. In the past companies have relied on physical security procedures in these environments, but for more robust security, physical protocols should be supplemented with phishing-resistant authentication on workstations as well.

Offer ruggedized devices that don’t require cellular connectivity

As outdoor or remote work sites security devices will need to be able to withstand physical shocks and weather conditions. Even the average office may not be so easy on devices as users can drop them, or inadvertently pour beverages on them. Ruggedized devices need to be ones that can operate in any condition, without cellular connectivity, and secure a range of computers and other endpoints that are either working offline, or on the network.

Deliver an easy user experience

Users often get overlooked in a search for a solution. Make sure you have gone over user survey feedback and find a good writer and communicator on your internal rollout team to prepare users for the change well ahead of time. Making this a usable system has to be just as important as making it a secure system, as one can’t be realized without the other.

YubiKeys deployed in:

9 of the top 10 global technology companies

4 of the top 10 U.S. banks

2 of the top 3 global retailers

Support complex environments

There is no one-size-fits-all solution for most sites. Different protocols must be considered if the solution is to be easily adapted to what already exists. Organizations looking to modernize security for their mobile-restricted environments that are using primarily on-premises infrastructure could opt for a smart card-based security approach, whereas those using a primarily cloud-based environment can consider a FIDO-based approach. If organizations are looking to move to passwordless authentication, they should opt for a solution that can support both smartcard passwordless or FIDO passwordless scenarios as a future proofed security strategy.

Deliver strong security

The solution must ensure high trust for the authentication mechanism itself. High trust comes from ensuring that the vendor has a secure supply chain and manufacturing process. If your vendor's security team can demonstrate strong security across their supply chain and follows proper code-signing protocols, you can rest a bit easier. In addition, it is important to enable safety nets against increased sophistication as attackers are growing increasingly bold and devising systems that capitalize on human errors. A solution should stay ahead of malicious innovation, employing anti-phishing policies or authentication to provide a backstop against any ransomware or malware attacks.

Able to support future compliance and regulations

Future compliance requirements are always something leaders should keep a close watch on. Looking into the future, increasing compliance regulations will dictate that organizations move towards phishing-resistant MFA approaches, in all environments, including mobile-restricted environments. There will be a move away from OTP-based approaches which are vulnerable to phishing, in favor of PIV (smart cards) and FIDO2/WebAuthn-based MFA approaches which are highly phishing-resistant.

YubiKeys have protected Google employees since 2009

0	**92%**	**4x**	**0**
account takeovers	fewer support incidents	faster to login	account lockouts[1]

Why YubiKeys are an ideal solution for the mobile-restricted environment

YubiKeys do not require client software to be installed and they require no batteries. So someone working in a mobile-restricted environment can just plug it into a USB port and touch the button, or tap-n-go using NFC for secure authentication. YubiKeys have no breakable screens, don't need a cellular connection, and are water- and crush-resistant (IP68 rated). All of these qualities are useful in a mobile-restricted environment that might have some physical hazards (for example, a factory workfloor or outdoor location).

By supporting multiple authentication protocols on a single YubiKey, such as OTP, OpenPGP, and strong authentication protocols such as smart card, FIDO U2F and FIDO2/WebAuthn, the YubiKey offers organizations the flexibility to deploy strong authentication using a single key across a variety of legacy and modern infrastructures to support organizations no matter where they are on their passwordless journey.

When mobile authentication is not even an option, the YubiKey's versatility allows it to work seamlessly across a wide range of sensitive and remote work environments where always-on authentication is a must.

The YubiKey provides the convenience needed to support today's modern in-person, hybrid, and remote employees. It is convenient for use in both mobile-restricted and non-restricted areas, providing a consistent, strong, phishing-resistant MFA approach across all environments.

Summary

To strike the right balance in a mobile-restricted space Yubico recommends first understanding the unique needs of that space, setting up a broad-based internal team to review requirements (as well as user experience and feedback), then working with a trusted vendor to install a solution that optimizes on both poles, productivity and security.

It's well known that legacy MFA methods like OTP and digital tokens have noticeable gaps where attacks can be launched. Mobile authentication is not a superior solution in any environment, mobile-restricted or not. Hardware-based security keys may offer the best solution in a mobile-restricted environment.

[1] Yubico, Google defends against account takeovers and reduces IT costs, https://www.yubico.com/resources/reference-customers/google/

About Yubico Yubico sets new global standards for easy and secure access to computers, servers, and Internet accounts. Founded in 2007, Yubico is privately held with offices in Australia, Germany, Singapore, Sweden, UK, and USA. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at **www.yubico.com.**

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088