1Password

How to securely embrace BYOD

BYOD: risks and rewards

Bring-your-own-device policies have been popular since the 2010's, and they became even more common during the pandemic work-from-home boom. Employers like BYOD because it saves them the cost of purchasing devices (especially cell phones) for their workforce. Employees like them because they get to work on the devices they're comfortable with. But BYOD comes with some tradeoffs.

Usually, BYO-devices are considered unmanaged, because they're not enrolled in a company's MDM, and are therefore outside of the control of IT and security teams.

Unmanaged BYOD presents serious security risks, including:

- Data leakage: IT can't monitor downloads or data transfers
- Malware: These devices may not be properly patched and lack basic antivirus protection
- Onboarding/Offboarding: IT lacks the ability to remotely configure or wipe these devices
- Credential-based attacks: Bad actors can use stolen employee credentials to log in from unknown devices

To maintain a safe BYOD policy, you must address (or at least acknowledge) these risks.

Steps to creating a secure BYOD policy

1 Define scope

Some BYOD policies only allow for certain types of devices, like mobile phones vs laptops and tablets. Others are reserved for certain roles, like full-time employees vs contractors. Which types of unmanaged devices you tolerate will depend on both your risk appetite and the technical limitations of your security stack. You generally can't put MDM on contractor devices or Linux endpoints, for instance.

You may have contractual and compliance obligations to prevent sensitive data from going onto unmanaged devices, so your BYOD policy may only apply to certain applications that you consider low-risk, such as allowing email and Slack on personal phones.

Questions to consider:

- Is our goal to allow unmanaged devices or require MDM? If the latter, how will we make enrollment a requirement?
- How do we separate corporate from personal data on BYO-devices?
- What happens if employees or contractors refuse to install monitoring software on their personal devices?

2 Establish minimum device requirements

Even with a permissive BYOD policy, you don't want devices accessing your systems unless they meet certain baseline security requirements. You also need a way to associate devices with user identities, so bad actors can't authenticate to your systems using totally unknown devices. Again, your legal and contractual obligations will help you identify these baselines for device health, but you will still need tools to enforce these policies.

Common device requirements:

- Updated OS
- Disk Encryption
- Firewall on
- Screenlock enabled

3 Enforce policies with device trust

A device trust solution can ensure that no device accesses sensitive resources unless it is both known (associated with the user) and in a secure, healthy state. In the case of 1Password Extended Access Management, the Device Trust agent acts as a possession factor during authentication, so devices can't access any application protected by your IdP unless they are both known and pass their compliance checks. This lighter touch form of management can't automate compliance like MDM, so you'll need the cooperation of your end-users.

Requirements for a device trust solution:

- Comprehensive library of posture checks
- Ability to write custom checks
- Ability to block authentication to failing devices
- Remediation path for end-users to minimize disruption

4 Communicate policies to end-users

Users can be understandably reluctant to install management software on their personal devices. To get buy-in, explain how these tools will impact their privacy and be clear about both what they can and can't do. For instance, make it clear that these tools can't remotely wipe their personal phone or laptop, so their family photos are safe. 1Password Extended Access Management helps with such messaging, both during the initial rollout, and every time users interact with the solution.

Employee communication best practices:

- Provide clear guidance on a tool's capabilities and limitations prior to initial roll-out
- Anticipate privacy concerns, document all data collection, and make it easily available to users
- If a user is blocked, provide clear remediation instructions, including support channels they can use even if blocked from apps on their device

How 1Password Extended Access Management helps secure your BYOD environment

1Password Extended Access Management is one of the only solutions capable of securing a BYOD environment, because it can provide visibility and security on all devices, whether or not they're enrolled in MDM.

- Our device trust solution ensures that devices meet your security standards. Choose from our library of hundreds of pre-built posture checks or build your own custom checks that can assess virtually any device property. If a device fails a check or is missing the device trust agent, it is blocked from authenticating to company apps until the user resolves the problem.
- Our app insights feature detects unapproved Shadow IT apps on BYO-devices, which IT admins can then choose to either prohibit or bring under management.
- Our enterprise password manager encourages users to practice good password hygiene instead of leaving plaintext credentials stored on their personal devices.

1Password Extended Access Management can accomplish all these things because it is minimally invasive and respects user privacy, so employees can feel good about having it on their device. Whether you choose to embrace BYOD or to prevent personal devices from accessing your resources, our solution can help you accomplish your goals.

Learn more about 1Password Extended Access Management

1Password