KEEPER
Cybersecurity Starts Here™

Password Management in a BYOD World

Table of Contents

Bring Your Own Device 3

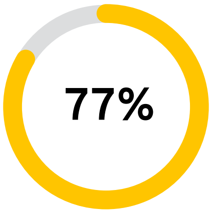
Bring Your Own Device Brings Its Own Risks 3

Mitigate BYOD Risk 4

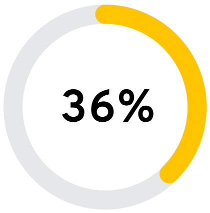
Constant Vigilance 7

About Keeper Security 7

Contacts 8



Americans own smartphones[1]



adoption rates for BYOD trends in North American for early 2017[3]

in annual savings per employee with a comprehensive BYOD policy[4]

Bring Your Own Device

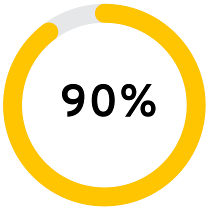
The vast majority of Americans – 95% – now own a cellphone of some kind. The share of Americans that own smartphones is now 77%, up from just 35% in Pew Research Center's first survey of smartphone ownership conducted in 2011.[1] As researchers at MIT noted, "the only technology that moved as quickly to the U.S. mainstream was television between 1950 and 1953."[2] And now consumers watch television on their smartphones and tablets. Given the pace of the IT consumerization, it makes sense that employers would want to accommodate workers' desire for convenience and mobility. The number of organizations that allow their employees to use personal devices for work-related reasons (bring your own device or BYOD) is one of the fastest trends in business today. A survey by MarketsandMarkets found that North American adoption rates were at 36 percent at the start of 2017 and are projected to be almost 50 percent by the start of 2018.[3]

Employers clearly appreciate the cost-savings associated with BYOD policies. When implemented correctly, a basic BYOD policy on average saves a company about $350 per employee per year, according to a Cisco analysis. A more comprehensive BYOD policy can yield upwards of $1,300 in annual savings per employee.
When it comes to BYOD, we're moving from what started as a convenience to something that will be mandatory.

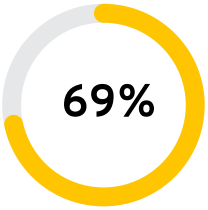
Bring Your Own Device Brings Its Own Risks

BYOD has a dark underside. The rise of greater choice and mobility in the workforce correlates strongly with the rise of cybercrime, whose sheer scale is mind-boggling. The British insurance company Lloyd's estimates that cybercrime costs businesses $600 billion every year.[5] In a ZDNet.com survey of 400 IT professionals, 96% said that security was extremely or somewhat important to IT departments over the next three years, by far the top response. Just beneath it at 89%, was mobile device management, which is an issue created by BYOD.

It doesn't help that even those consumers probably choose easily hackable passwords. According to Entrepreneur magazine, 90% of employee passwords can be hacked in six hours. Moreover, 69% of U.S. adults use the same password for multiple accounts.



of employee passwords can be hacked in six hours[6]



of U.S. adults use the same password for multiple accounts[6]

Which is why it's surprising how ill-prepared most companies are when it comes to cybersecurity and BYOD policies. Part of the problem is that many organizations' BYOD developed organically. What first might have started as employees simply checking their work email at home or on their smartphones turned into permission to access a company's otherwise secure enterprise system remotely (even if it's inside the office). Organizations whose BYOD practices have evolved over time probably haven't properly assessed the risks and likely don't understand how exposed their systems really are. The larger the organization, the bigger the problem an evolving BYOD policy is.

Mitigate BYOD Risk

The best strategy for a safe and effective BYOD policy is to remove as much of the security decision-making from employees as possible. We hasten to add that this shouldn't be seen as a negative decision, but rather a decision that allows a business – executives, managers and employees – to get the most out of a BYOD model that seeks to maximize employee performance, happiness and organization security.

There are three major aspects to consider:

1. Eliminate the trade-off between security and convenience. Security and convenience are generally opposing forces. Employees wanting to get their jobs done eventually suffer security fatigue and try to defeat security controls or fall back poor security habits.

2. Provide admins needed visibility and control into employee access so they can course correct. You can't fix what you can't measure.

3. Tools that rapidly deploy remotely and integrate with existing services. IT teams cannot be required to physically touch every BYOD device.

Security vs. Convenience

Biometrics are a great example of boosting security through convenience. In one of the most common use-cases, Touch ID (fingerprint scan) on iPhones is used to unlock the PIN, which in-turn is used to unlock the phone. The phone can still be opened with the PIN. Therefore, the Touch ID feature technically does nothing to make the phone more secure, but it is more convenient. This in-turn may prevent users from trying to defeat phone locking in the first place, making the end result more secure.

The most obvious risk with BYOD is what happens when an employee's device is stolen. When three out of ten smartphone owners don't use passwords to access their device , the problem for businesses becomes acute. An unprotected smartphone with access to a company's systems is a disaster waiting to happen. In a BYOD world a single stolen smartphone is a major inconvenience for the consumer; it can be catastrophic for a company. Keeper requires a separate login from the device, so even if the user has defeated the device login, the passwords are still secure. Admins can even set the auto-logout timer according to company policy.

Employees use weak passwords, reuse them across accounts and forget them. Keeper will generate strong, random passwords and automatically fill them for users. This saves them time, frustration and eliminates the need for them to reuse and remember passwords. Employees must choose a strong master password that meets enforced password guidelines, but otherwise they won't have to remember another password for any company needs, reducing the password-reset requests that often plague IT departments.

By putting the Keeper vault at the user's fingertips from any device, they will be encouraged to use it rather than spreadsheets and sticky notes. Keeper is available in native applications for iOS, Android, Windows, Mac and Linux. Browser Extensions for Chrome, Safari, Firefox, Edge and IE are also supported. All devices are backed-up and synchronized via the Keeper Cloud Security Vault™.

Many Keeper customers also provide personal vaults for employees. It reinforces employee behavior for them to use the same tool for all passwords. This further encourages strong passwords and not reusing them across work and personal accounts. Keeper makes ability to switch accounts easy.

Right now, employees are emailing or IMing passwords to each other. Sharing passwords is inevitable, but losing control of them is not. With Keeper, each user has a 2048-bit RSA key pair that is used for sharing password records and messages between users. Shared information is encrypted with the recipient's public key. Keeper's record sharing methodology is easy to use, secure and intuitive.

Beyond passwords, Keeper works with any PIN, digital certificate, encryption key, SSH key, API key or access key. By setting habits with passwords, employees will naturally look to use Keeper for all their credential needs.

Visibility and Control

Most businesses have limited visibility into the password practices of their employees which greatly increases cyber risk. Password hygiene cannot be improved without critical information regarding password usage and compliance. Keeper solves this by providing comprehensive password reporting, auditing, analytics and notifications through the Admin Console.

From the Keeper security report in the admin console, security pros can see at-a-glance employee password strength, password reuse and two-factor authentication status.

The ability to enforce policy controls, define access roles and restrict sharing is critical for safe enterprise password management. Limiting employee access to need-to-know (aka least privilege) ensures that employees only have company resources and logins that they need at the times that they need it, greatly reducing the risk from careless or disgruntled employees. Assigning a delegated admin that is regularly monitoring, provisioning and deprovisioning access to users based on their role in the company is highly recommended.

Here is a sample of the role-based access control Keeper enforces:

- Master Password Complexity
- Master Password Expiration
- Biometrics
- 2FA enforcement – type and platform
- Platforms Allowed
- Password Sharing and Exporting
- IP whitelisting
- Logout Timers Across Platforms

Every cybersecurity framework from NIST to ISO and PCI to HIPAA requires access tracking, least privilege controls and audit logs. Keeper enables role-based controls and visibility into shared credentials. Access logs to Keeper vaults can be audited for compliance or forensics.

Rapid Provisioning and Integration

With BYOD, the last thing the IT department needs is to have to physically touch every device. Tracking people down, scheduling times for them to come in and having resources available is a nightmare. Fortunately, Keeper provides enterprise-grade tools for rapid user provisioning and access controls.

Keeper AD Bridge™ synchronizes to Microsoft Active Directory or Open LDAP. This enables rapid user provisioning and automatically adds Nodes (organizational units), Users, Roles and Teams. Keeper enables role-based access control and the ability to track roles as people move throughout the organization. This includes automatically locking vaults of employees that leave.

Without question, SSO solutions are here to stay due to the reduced burden on users and enhanced security. However, SSO leaves many functional and security gaps. Most legacy, native and even many newer web-based applications don't support SAML. There are also many credentials to manage beyond passwords, such as encryption keys (RSA, AES, SSH, TLS), digital certificates and API keys. Keeper Enterprise Password Manager with Keeper SSO Connect™ transforms SSO into an essential, ubiquitous application. Keeper SSO Connect™ integrates with popular SSO IdP platforms such as Okta, AWS, Centrify, CAS, OneLogin, Ping Identity, F5 BIG-IP APM, G Suite, JumpCloud and Microsoft ADFS/Azure to provide businesses the utmost in authentication flexibility. Email auto-provisioning is completely unique to Keeper. Large organizations with distributed users such as universities, hospitals and retail and can provision Keeper vaults to thousands of users with a domain match on email addresses. With minimum administration, large scale deployment can be accomplished using an existing email channel or portal.

Keeper Commander™ SDK provides IT admins and developers with command-line tools and Python source code to perform password management, password rotation and vault functionality. Eliminate hard-coded or plaintext back-end passwords. Connectors include Unix, Windows and AD logins; Oracle, Microsoft SQL, MySQL, Postgres and Dynamo databases; and AWS password and API access keys.

Constant Vigilance

Password Management remains a critical step in any organization's BYOD policy. Before an employee receives their first company email, an organization can be confident that the employee's mobile device is safe for use. Keep in mind that registering, managing and tracking the dozens, hundreds or even thousands of devices that come with a BYOD policy can frustrate even the savviest of IT departments. A password management solution helps streamline the process, secure organization data and remove most employee carelessness or maliciousness from the equation. And yet an organization can still reap the cost-savings and convenience that come with a BYOD policy.

About Keeper Security

Keeper is a Zero-Knowledge Password Management solution. This means all information that is stored in Keeper is only accessible by the end-user. All encryption and decryption is done on-the-fly in the client's device using a PBKDF2 derivation of the master password. The user must enter the master password because it is not stored on the device. The data is encrypted both in-transit (TLS) and at rest on Keeper's Infrastructure (AES-256.) The plaintext version of the data is never available to Keeper Security employees nor any outside party. Keeper is fanatical about protecting customer data, but in the unlikely event Keeper was hacked, the attackers could only possibly access the worthless ciphertext.

Keeper Security is transforming the way businesses and individuals protect their passwords and sensitive digital assets to significantly reduce cyber theft. As the leading password manager and digital vault, Keeper helps millions of people and thousands of businesses substantially mitigate the risk of a data breach. Keeper is SOC 2 Certified and utilizes best-in-class encryption to safeguard its customers. Keeper protects industry-leading companies including Sony, Chipotle and The University of Alabama at Birmingham. Keeper partners with global OEMs and mobile operators to preload Keeper on smartphones and tablets.

Sources:

1 - https://www.pewinternet.org/fact-sheet/mobile/
2 - https://www.technologyreview.com/s/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/
3 - https://mobilebusinessinsights.com/2017/08/the-latest-byod-trends-and-predictions-from-mobile-focus-to-endpoint-management/
4 - https://www.insight.com/en_US/learn/content/2017/01-16-2017-workplace-mobility-statistics-show-improved-productivity.html
5 - https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html
6 - https://www.statista.com/statistics/763091/us-use-of-same-online-passwords/
7 - https://www.pewresearch.org/fact-tank/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/

Business Sales

Americas & APAC
+1 312 829 2680

United Kingdom
+44 20 3405 8853

Germany & DACH
+49 89 143772993

Ireland
+353 21 229 6020

EMEA
+353 21 229 6011

Netherlands
+31 20 262 0932

Iberia & Italy
+34 919 01 65 13

Sweden & Nordics
+46 8 403 049 28

Support

Consumer
+1 312 971 5702

Business (Americas & APAC)
+1 312 226 4782

Business (EMEA)
+353 21 229 6019

keepersecurity.com sales@keepersecurity.com