



ONLYKEY CLOSES THE ENTERPRISE GAP IN IDENTITY ACCESS MANAGEMENT SOLUTIONS



The password is dead. Long live the password.

The death of the password was first predicted almost two decades ago at the RSA Security Conference in 2004. This was 18 years ago. And, the passwordless future has been predicted at practically every security conference since.

With these predictions largely failing to materialize, is it safe to assume that passwords are here for the foreseeable future? If so, what can organizations do?

With the research presented here, we intend to answer these questions and identify how OnlyKey helps businesses fill the gaps in their IAM infrastructure.

THE CURRENT STATE OF AUTHENTICATION

One of the primary issues with replacing passwords is that passwords have a wide range of utilities. They are used for authentication in:



web browsers



local applications



physical devices
(Desktop/server
authentication)



virtual devices
(VMware,
VirtualBox, VDI)



remote
systems (Citrix,
Teamviewer,
RDP, VNC, AWS
Workspaces)

With no single solution to address all of a businesses' authentication needs, organizations are left with a fragmented IAM infrastructure. In the real world, businesses implement a patchwork of authentication solutions to cover required services, which may include custom-built applications and legacy systems involving the use of many passwords. There are also gaps between management's intended deployment of password solutions and the actual implementation. Such gaps may turn into a breach.

In a recent poll, the overwhelming majority of users reported that of the websites they use:



At least **90%** do not support passwordless authentication



At least **25%** do not support any kind of multi-factor authentication

This leaves quite a large gap where **strong and complex passwords are absolutely essential.**

AUTHENTICATION GAP CASE STUDY: OKTA BREACH

In 2022, Okta, a leader in the single sign-on and passwordless authentication space, fell victim to a breach <https://www.okta.com/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise/>.

Using this breach as a case study, we can make important observations about some of Okta's security policy and technology gaps and how they were exploited by an attacker:

“

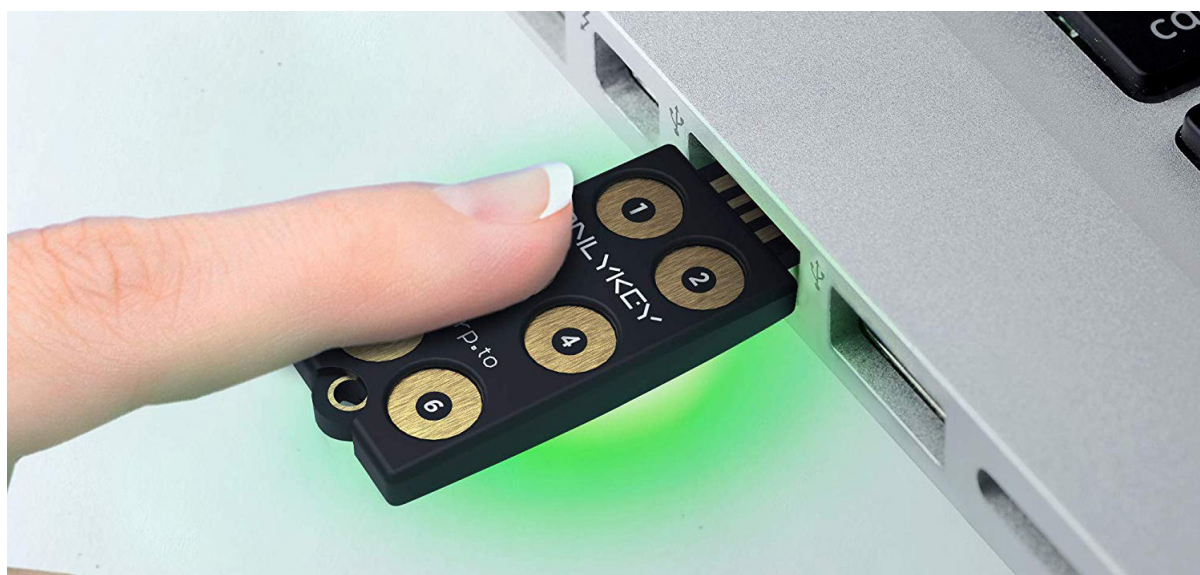
- The threat actor actively controlled a single workstation, used by a Sitel support engineer, with access to Okta resources.
- The threat actor was unable to authenticate directly to any Okta accounts.

In this case, it was not necessary to log into an Okta SSO account to achieve the data breach. This is often the case as compromising a password on a single workstation can give an attacker all they need.

81% of the total number of breaches leveraged stolen or weak passwords. – 2020 Verizon Data Breach Investigations Report

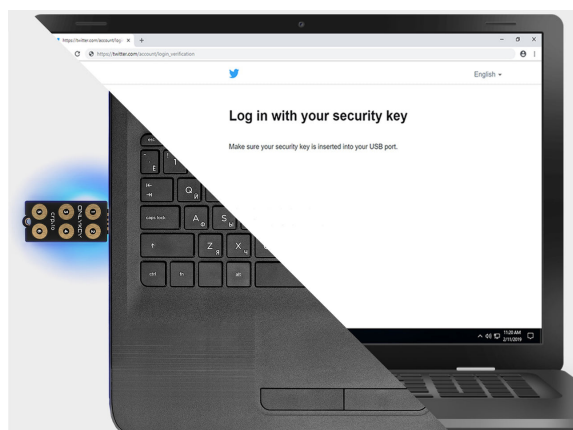
SOLVE WORKSTATION & SERVER AUTHENTICATION GAPS

OnlyKey can be used to authenticate to physical devices like a workstation or server using a variety of protocols, such as FIDO2 authentication for Azure AD. It also works seamlessly with MFA provider Authlite to provide local Windows Enterprise authentication that even works securely offline.



SOLVE LOCAL APPLICATION AUTHENTICATION GAPS

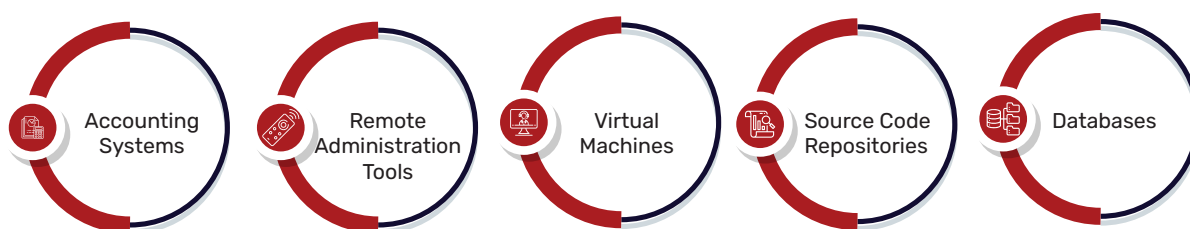
Another common security gap is that of local application authentication, whereby an attacker in the Okta breach accessed local applications providing access to sensitive client data:



“

- The threat actor accessed two active customer tenants within the SuperUser application (whom we have separately notified), and viewed limited additional information in certain other applications

With so many applications each supporting their own methods of authentication, most organizations struggle to manage them all. Local applications are often business critical and may only support password authentication. For example:



OnlyKey fills the gaps left by other enterprise authentication solutions and will work with practically any off-the-shelf or custom service or application. OnlyKey functions as a hardware security key for applications that support MFA, or by securely storing and outputting strong/complex/random passwords (up to 56 characters long) on behalf of users.

Forcing Users to Remember Long Complex Passwords = Unhappy Users

When users are overwhelmed by complex password requirements, they will either reuse passwords or resort to sticky notes, notepads, or digital documents to store their complex passwords. People simply can't memorize long, complex passwords for all the systems they need access to. Using OnlyKey allows users to be more productive and secure without having to remember and type long, complex passwords.

WHY ONLYKEY?

Faster Secure Logins - The modern day employee wastes an average of 24 hours per year logging into workstations. With OnlyKey, a 56-character password can be typed in 1 second. Improve workforce productivity by reducing valuable time wasted typing in long, complex passwords.

A recent poll of OnlyKey users found that the majority experience faster, secure logins with OnlyKey.

Works Seamlessly to Manage Remote Systems - MSPs and system administrators have access to manage remote systems. Using a software password manager through remote systems can be difficult.

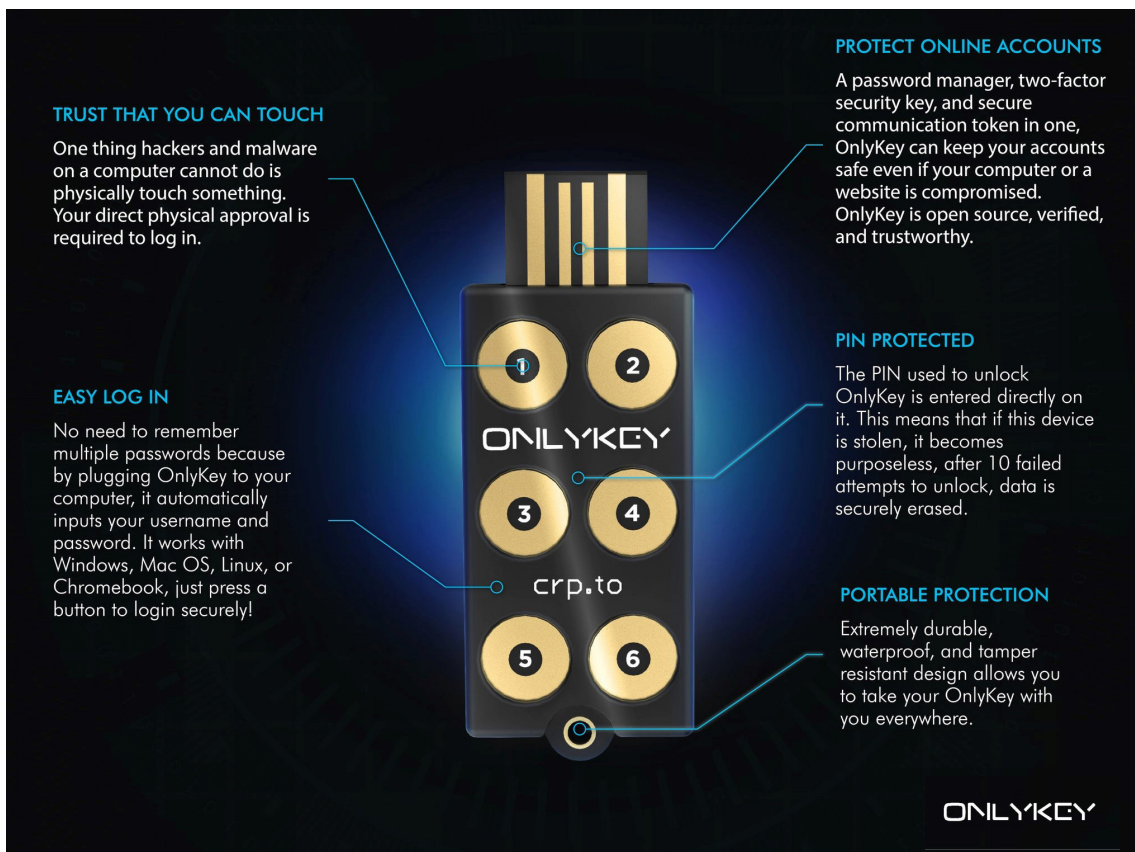
OnlyKey's hardware password manager supports all types of remote administration tools and even works in virtual machines.

Simple Integration - There is no need for rip and replace. OnlyKey integrates with your existing IAM infrastructure, desktop authentication, and local application authentication.

We asked OnlyKey users, and 100% of respondents reported that they have had NO ACCOUNTS COMPROMISED that are protected by OnlyKey.

OnlyKey is available in two portable and durable form factors:

- **OnlyKey:** on-device PIN protection provides maximum security, supports USB-A (USB-C and Lighting with available adapters)



TRUST THAT YOU CAN TOUCH
One thing hackers and malware on a computer cannot do is physically touch something. Your direct physical approval is required to log in.

EASY LOG IN
No need to remember multiple passwords because by plugging OnlyKey to your computer, it automatically inputs your username and password. It works with Windows, Mac OS, Linux, or Chromebook, just press a button to login securely!

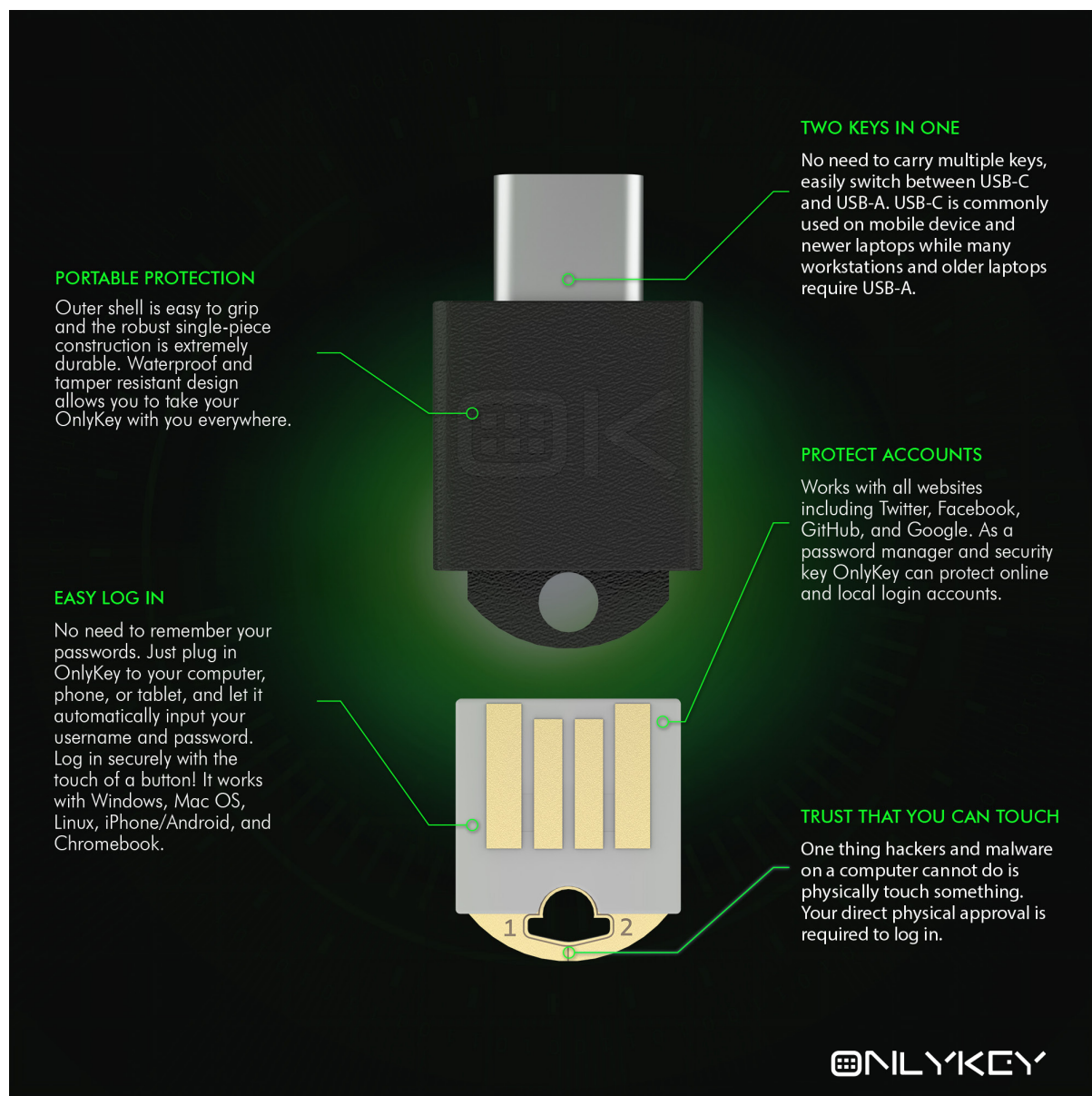
PROTECT ONLINE ACCOUNTS
A password manager, two-factor security key, and secure communication token in one, OnlyKey can keep your accounts safe even if your computer or a website is compromised. OnlyKey is open source, verified, and trustworthy.

PIN PROTECTED
The PIN used to unlock OnlyKey is entered directly on it. This means that if this device is stolen, it becomes purposeless, after 10 failed attempts to unlock, data is securely erased.

PORTABLE PROTECTION
Extremely durable, waterproof, and tamper resistant design allows you to take your OnlyKey with you everywhere.

ONLYKEY

- **OnlyKey DUO:** smaller form factor for maximum portability, supports easily switching between USB-A and USB-C without an adapter.



THE SECURITY KEY LOVED BY PROFESSIONALS

Professionals such as system administrators, database administrators, developers, and power users like accounting staff, have to securely manage multiple systems/customers and need a more secure way of storing passwords. OnlyKey closes gaps left by other enterprise authentication solutions and is particularly useful for:

MSPs - Remote access to multiple tenants and clients systems.

System Administrators - Access to workstations and servers and also require using custom applications.

IT and Security - Access to security assessment software, license management systems, software update applications, etc.

Database Administrators - Access to

companies' most sensitive data and also require using custom applications.

Developers - Need to manage lots of passwords, API keys, and Git repositories that contain an organization's valuable and often proprietary source code.

Power Users - Other trusted users within an organization that have access to various other systems such as SCADA, facilities, and office management applications with authentication gaps to fill.

TAKE ACTION TO SOLVE AUTHENTICATION GAPS

Step 1

Easily add hardware MFA to your existing important business accounts

- Many services already support hardware MFA, and, for compliance, some accounts are required to utilize hardware MFA.



CIS Benchmark 1.14 Ensure Hardware MFA is Enabled for the Root Account

- Root accounts may be on local workstations or in the cloud, such as the Amazon AWS root account.

Use OnlyKey hardware MFA to solve your authentication gap and achieve compliance.

Step 2

Easily add hardware password protection for business critical passwords

- Organizations store business critical passwords in a variety of locations such as:
 - Management software such as IT Glue
 - Online software password managers such as LastPass
 - IT teams may store passwords in their own password management solutions such as KeePass or Pass

Use OnlyKey hardware password manager to solve your authentication gap and achieve compliance.

OnlyKey securely stores existing passwords in hardware, thereby adding extra protection for critical accounts. At the same time, those passwords become portable and easy to use in any application. Additionally, OnlyKey integrates with and is supported by popular solutions for IT teams, such as KeePassXC and Pass.

Step 3

Easily add hardware key protection for business critical key management

- Organizations store business critical authentication and encryption keys in a variety of locations such as:
 - System administrators may use local SSH keys to remotely access systems
 - Software developers may sign Git commits for critical software with local SSH or GnuPG/OpenPGP keys.
 - Security personnel may use OpenPGP for encryption.

Use OnlyKey hardware key management to solve your authentication gap and achieve compliance.

With OnlyKey, we engineered a proven security device that is trusted by thousands of users in various industries deployed across at least 60 countries. Today, OnlyKey is the leading hardware password management solution and a FIDO2 certified MFA solution. With OnlyKey, businesses are finally able to close critical gaps in IAM infrastructure.

OnlyKey has been highlighted by:

- [ZDNet "OnlyKey: The ultimate security key for professionals"](#)
- [TechRadar Pro "Best security key in 2022"](#)
- [Best Offline Password Storage Devices](#)
- [How-To Geek "The Best Hardware Security Keys of 2022"](#)
- [Best Reviews "Best Security Keys"](#)
- [Tom's Guide "What is a USB security key, and how do you use it?"](#)
- [Security Gladiators "What Are the Best Security Keys for Online Protection?"](#)

ORDER ONLYKEY DIRECTLY ON:

AMAZON (OVER 450 AMAZON REVIEWS)

ORDER ONLYKEY ON ONLINE STORE:

[HTTPS://ONLYKEY.IO](https://onlykey.io) (SHIPS WORLD-WIDE)

