yubico | boxcryptor

Keep attackers out with strong authentication

In many business environments, attackers can guess common passwords, reuse them from site breaches, and phish credentials. They occasionally have to tweak their tactics to deal with password managers, SMS authentication, or mobile push applications, but their playbook is still mostly the same unless stronger mitigations are used.

Authentication methods: What's the difference?

In 2019, Black Hat USA asked attendees what cybersecurity technologies have been most effective for data security and privacy online. Multi-factor authentication (MFA) was the highest ranked security tool for protecting enterprise data, with 82% of respondents citing it as effective[1].

Enabling MFA is like building a fortress around critical assets—it provides an extra layer of protection for devices, systems, and accounts, and helps secure data against external threats. There are a variety of authentication methods available today, each offering different levels of security and convenience. It's important to ask yourself: is the method you're using enough?

Robert Freudenreich, CTO, Secomba GmbH | Boxcryptor:

"The protection of sensitive data has top priority in our company. One important aspect for us is, therefore, the authentication of Boxcryptor users. Only authenticated users should be provided access to protected data."

80% attack penetration rate

Username and password

Having only a username and password to protect your account has known usability and security gaps, and is the most susceptible to external threats. It's also expensive.

Because stealing someone's password is relatively easy to do from afar, it's become one of the most common attacks in the world. Some common ways attackers obtain and misuse passwords include weak password guessing and password reuse abuse.

10-50% attack penetration rate

Time-based OTP via SMS, email, mobile push

Basic authentication methods, such as SMS, email, and mobile are stronger than a username and password, yet remain vulnerable to network and software attacks including man-in-the-middle (MitM), account recovery exploitation, and credential phishing.

Attackers can hijack time-based one-time passwords (TOTP) and push notifications during the brief window they are valid, and the attack is all but invisible for the user. Additionally, waiting for and manually typing in these codes creates user fatigue and decreases workforce productivity.

0% attack penetration rate

Security keys, smart cards, biometrics

Utilizing stronger authentication methods, such as security keys, biometrics, and smart cards raises the bar for security.

Hardware security keys strengthen existing security solutions by requiring a physical key as the authentication controlling factor.

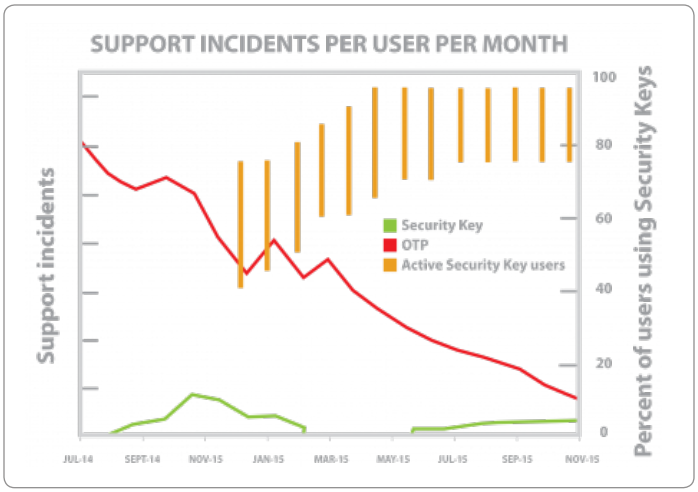
Similarly, storing certificates in smart cards makes use of strong public/private-key cryptography to thwart remote attacks, while biometrics, when obtained and stored locally in the secure element, offer convenience and resistance to on-premise attacks.

Security keys: Trusted by the world's leading companies

Security keys have already proven their effectiveness. After a two-year evaluation[3] of one-time passwords (OTPs), TLS certificates, smart cards and other authentication methods, Google confirmed that FIDO-based security keys were best suited to deliver on the company's security and usability needs.

Google's study to measure the business impacts of hardware-based authentication highlighted several important benefits:

- Zero account takeovers
- 4x faster logins
- 92% fewer IT support calls



Additionally, within Microsoft, the YubiKey dramatically reduced the number one IT support cost—password resets—which Microsoft estimates costsover $12M per month[4].important to ask yourself: is the method you're using enough?

Stronger together: Boxcryptor enables strong hardware-backed authentication with YubiKeys

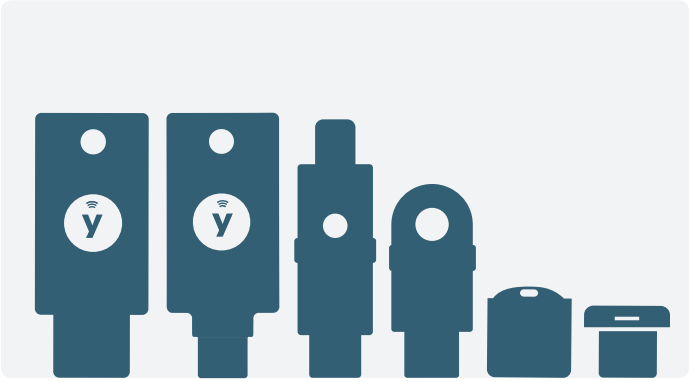
Yubico's YubiKey is purpose-built for security, and provides a modern authentication solution to prevent account takeovers and security breaches. The YubiKey provides physical proof that the user is present at the time of login when they touch the key to authenticate, and offers a user experience that's four times faster than manually typing codes.

The YubiKey supports multiple authentication protocols including FIDO/WebAuthn, OTP, PIV-compatible smart card, and challenge-response, so users can secure access to computers, networks, mobile devices, and a multitude of apps and services with a single key. They also don't require batteries or connectivity to work, and are always available and ready for authentication.

"In order to provide secure access to users, multi-factor authentication is the preferred go-to solution. Apart from software-based solutions (like authenticator apps), a hardware-based solution like YubiKey offers a high level of security and convenience which we at Boxcryptor want to provide to our users."

Boxcryptor and YubiKey:

Sensitive data must be well protected. With Boxcryptor users can encrypt data before they store it in the cloud. And to support the security that is offered through the Boxcryptor software doorkeeper "password" we recommend a physical key (like YubiKey) so that nobody gets unauthorized access.



Get started with Boxcryptor:
https://www.boxcryptor.com/

Get started with Yubico:
https://www.yubico.com/support/contact/

[1] Consumers in the Crosshairs, 2019
[2] 2019 State of Password and Authentication Security Behaviors Report, 2019
[3] Security Keys: Practical Cryptographic Second Factors for the Modern Web, 2016
[4] Saying Goodbye to Passwords, Alex Simons, Manini Roy, Microsoft Ignite 2017

About Secomba: Secomba GmbH is a German company developing Boxcryptor, a cloud-optimized encryption solution for businesses as well as private users all over the world.

Learn more about Boxcryptor: www.boxcryptor.com

About Yubico Yubico sets new global standards for simple 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.

Discover why nine of the top 10 internet brands trust the YubiKey: yubico.com