yubico

Google Defends Against Account Takeovers and Reduces IT Costs

YubiKeys protect Google employees since 2009

Case Study

Google

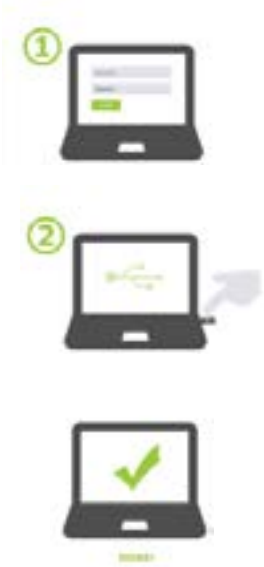
Industry
Technology

Protocols
U2F

Products
All YubiKey Form Factors

Deployment
Employees

U2F for USB



About Google

In 1998, Google was founded with one mission: organize the world's information and make it universally accessible and useful. Since then, the company has focused on developing services to significantly improve the lives of as many people as possible, and today, Google is a global Fortune 50 company considered to be one of the leading internet companies in the world. For an innovative technology company, such as Google, the need to ensure that online access to confidential information is restricted to approved employees and contractors is critical to the company's success.

Overcoming Account Takeovers

In 2009 Google was the target of sophisticated cyber attacks capable of circumventing traditional security controls. With a lack of viable two-factor authentication (2FA) options to effectively prevent these attacks and account takeovers, Google began working closely with Yubico to extend the capabilities of the YubiKey two factor authentication technology to also include public key cryptography. Through this collaboration, Yubico and Google co-created a strong authentication protocol based on the concept of a single phishing-resistant key to secure all services. It is this work that later became an open standard adopted by the FIDO alliance called the FIDO Universal 2nd Factor (U2F) standard.

One single YubiKey can secure a multitude of online services with no user information or private keys shared between the service providers. There is no reliance or requirement for mobile connectivity, cellular devices, mobile apps or manual code entry.

Results

After a two-year evaluation of one-time passwords (OTPs), TLS certificates, smart cards and other authentication methods, Google confirmed that FIDO U2F Security Keys were best suited to deliver on the company's security and usability needs. Shortly thereafter, Google expanded its deployment of the YubiKey to all staff and contractors for secure computer and server login, reaching more than 50,000 employees to date.

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

Heightened Security: Internal accounts protected solely with a YubiKey and FIDO U2F have experienced a significant increase in the level of security.

Accelerated Employee Productivity: Employees saw a significant reduction—by nearly 50 percent—of the time to authenticate using a YubiKey compared with using a one-time password (OTP) via SMS. Logins were nearly four times faster when comparing the YubiKey to Google Authenticator. The time saving is primarily due to the one-touch YubiKey authentication that executes in milliseconds.

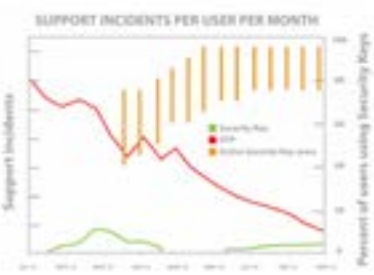
Case Study

Industry
Technology

Protocols
U2F

Products
All YubiKey Form Factors

Deployment
Employees



Reduced support: Compared to using a phone for authentication, YubiKeys were found to be easy to use, robust in design, waterproof and did not easily break. The YubiKey also allowed for issuing multiple backups to each employee, including one YubiKey nano designed to sit inside the user's laptop and one YubiKey designed for a keychain. Google found support calls dropped, with 92% reduction in support incidents, saving thousands of hours per year in support costs. Furthermore, authentication failures are estimated at zero.

Lowered Cost of Ownership: The combined security, usability, and workflow efficiencies of the YubiKey, allowed Google to give each employee multiple YubiKeys and still realize overall cost reductions.

Protecting Employees and Customers with Strong 2FA

Today, Google not only protects employees with the YubiKey but has also integrated support for the YubiKey and FIDO U2F security keys into the available security protections for all Google users. Any user with a Google account can now protect themselves from advanced phsihing and benefit from the strong authentication provided by the YubiKey.

The Strongest Defense against Phishing

Most recently in October 2017, Google launched its Advanced Protection Program (GAPP) for those users at highest risk including journalists, business leaders and political campaign teams. The GAPP program further tightens up security for Google account users by requiring the use of hardware-backed FIDO U2F security keys for secure login versus making them optional. To provide the strongest defense against phishing, Advanced Protection goes beyond traditional 2-Step Verification. Participants in GAPP are required to sign into your account with a password and a physical security key ie the YubiKey. Other authentication factors, including codes sent via SMS or the Google Authenticator app, will no longer work, since these forms of 2FA have been shown to be phishable.

Protecting Adwords Customers

Google has also highlighted the benefits of protecting Adwords accounts with the YubiKey, In 2016, Google published a blog highlighting how two digital marketing agencies, Jellyfish and iProspect, protect their AdWords accounts, customers, and revenue using the YubiKey.

Modern Authentication at Scale

Google is a leading technology company with innovation and invention at its core. Working in collaboration with Yubico, Google was critical in defining the open standard for strong authentication now known as the FIDO U2F standard. Today, Yubico and Google, offer over one billion Gmail users and more than 50,000 Google employees, strong phishing-resistant two-factor authentication to protect personal data and secure access to the Internet. Security keys have led to no confirmed account takeovers and greater user satisfaction since deployment at scale.

Mayank Upadhyay, Director of Security Engineering, Google Inc.

"We believe that by using this token we've raised the standard of security for our employees beyond what was commercially available. The device works with Google's Web browser Chrome, and works very seamlessly for people in their day-to-day workflow here at Google."

Yubico AB
Olof Palmes gata 11
6th floor
SE-111 37 Stockholm
Sweden

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