



YubiKey 5 FIPS Series

Chứng nhận FIPS 140-2 bảo mật mạnh mẽ và đáp ứng quy định an toàn

Rủi ro khi dựa vào tên đăng nhập và mật khẩu

Các sự cố an ninh nghiêm trọng xảy ra thường xuyên. Dự kiến, chi phí do tội phạm mạng toàn cầu gây ra sẽ tăng 15% mỗi năm và đạt mức 10.5 nghìn tỷ USD/năm vào năm 2025¹.

Trong đó, 60% các vụ vi phạm do sử dụng mật khẩu yếu hoặc bị đánh cắp². Do đó, bộ phận IT không thể chỉ dựa vào mật khẩu để bảo vệ dữ liệu công ty mà cần áp dụng phương thức xác thực mạnh hơn cho nhân viên và đối tác – nếu không muốn trở thành nạn nhân tiếp theo.

YubiKey 5 FIPS Series xác thực đa lớp chống lừa đảo mạnh mẽ

Dòng YubiKey 5 FIPS giúp triển khai xác thực mạnh mẽ và mở rộng dễ dàng, loại bỏ nguy cơ chiếm đoạt tài khoản do tấn công lừa đảo. YubiKey là thiết bị phần cứng với các khả năng:

- Cung cấp nhiều giao thức xác thực và mã hóa như FIDO2/WebAuthn, FIDO U2F, Smart Card (PIV), OpenPGP, Yubico OTP để bảo vệ quyền truy cập của nhân viên vào máy tính, mạng và dịch vụ trực tuyến chỉ bằng một lần chạm
- Hỗ trợ đăng nhập không mật khẩu qua FIDO2/WebAuthn và thẻ thông minh.
- Tương thích với Windows, macOS, Android, Linux và các trình duyệt phổ biến.
- 6 mẫu thiết bị sử dụng các kết nối USB-A, USB-C, NFC và Lightning.

¹ Cybersecurity Ventures, *Cybercrime To Cost The World \$10.5 Trillion Annually By 2025*

² Verizon, *2025 Data Breach Investigations Report*

³ Google Research, *Security Keys: Practical Cryptographic Second Factors for the Modern Web*



YubiKey 5 FIPS là dòng sản phẩm xác thực đa giao thức FIDO2/WebAuthn đầu tiên được FIPS xác thực. Từ trái sang phải: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS và YubiKey 5C Nano FIPS.

YubiKeys đã bảo vệ nhân viên Google từ năm 2010

0	92%	4x	0
tài khoản bị chiếm đoạt	ít sự cố hỗ trợ hơn	đăng nhập nhanh hơn	tài khoản bị khóa

YubiKey là lựa chọn tin cậy của Google, Meta và Salesforce từ năm 2012

Cung cấp xác thực đa yếu tố mạnh mẽ

YubiKey kết hợp xác thực phần cứng và mã hóa khóa công khai để đảm bảo xác thực mạnh và ngăn chặn chiếm đoạt tài khoản. Khả năng bao gồm FIDO2/WebAuthn và FIDO U2F, các tiêu chuẩn xác thực mở hỗ trợ bởi Liên minh FIDO, cùng với chức năng thẻ thông minh Smart Card dựa trên chuẩn PIV được quy định trong NIST SP 800-73.

Giảm chi phí IT

Dựa trên dữ liệu từ việc triển khai YubiKey, Google nhận thấy rằng khóa để sử dụng và ổn định đã giúp giảm 92% số sự cố hỗ trợ liên quan đến mật khẩu. Điều này giúp công ty tiết kiệm hàng ngàn giờ hỗ trợ mỗi năm.³

Cung cấp bảo mật dễ sử dụng, nhanh chóng và đáng tin cậy cho nhân viên

YubiKey là thiết bị phần cứng đáng tin cậy vì không cần pin hay kết nối mạng, nên luôn sẵn sàng hoạt động. Việc xác thực nhanh chóng chỉ bằng một lần chạm, nhanh hơn gấp 4 lần so với phương thức xác thực hai yếu tố qua SMS hoặc thiết bị di động.



YubiKey được tin dùng bởi:

9/10 công ty công nghệ lớn nhất thế giới

4/10 ngân hàng lớn nhất nước Mỹ

5/10 tập đoàn bán lẻ lớn nhất thế giới

YubiKey: Giải pháp bảo mật mạnh mẽ được tin dùng bởi các công ty hàng đầu thế giới

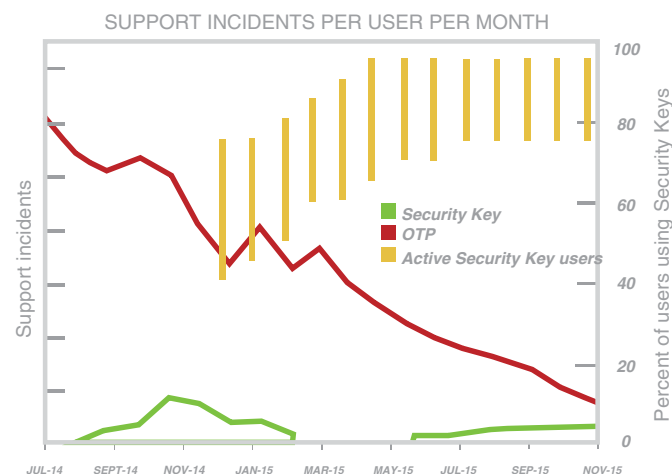
Xác thực chống lừa đảo cho doanh nghiệp

YubiKey lưu trữ thông tin bí mật xác thực trên chip phần cứng bảo mật. Thông tin này không bao giờ được truyền đi nên không thể bị sao chép hoặc đánh cắp.

Giảm chi phí IT

YubiKey giảm đáng kể chi phí hỗ trợ phòng ban IT – việc đặt lại mật khẩu – vốn tiêu tốn của Microsoft hơn 12 triệu USD mỗi tháng.⁴

Bằng cách chuyển từ OTP di động sang YubiKeys, Google đã giảm 92% các sự cố hỗ trợ mật khẩu vì YubiKeys đáng tin cậy hơn, nhanh hơn và dễ sử dụng hơn



This graph illustrates how quickly Google reduced password support incidents after switching from OTP to YubiKey.⁵

Dễ sử dụng, nhanh và đáng tin cậy

Không cần cài đặt gì – khách hàng hoặc nhân viên chỉ cần đăng ký YubiKey, nhập tên đăng nhập và mật khẩu như bình thường, sau đó cắm và chạm YubiKey khi được yêu cầu.

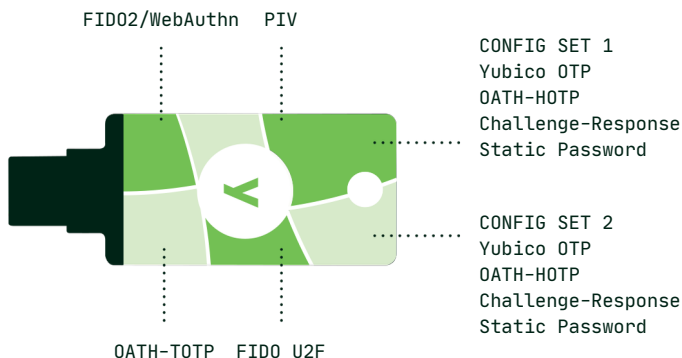
YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS và YubiKey 5C FIPS có thể dễ dàng gắn vào móc khóa, trong khi YubiKey 5 Nano FIPS và YubiKey 5C Nano FIPS được thiết kế để gắn cố định trong cổng USB. Điều này giúp người dùng luôn dễ dàng sử dụng và có cùng mức độ bảo mật cao. Các mẫu YubiKey 5 NFC FIPS và 5 Nano FIPS có khả năng chống va đập và chống nước.

⁴ "Saying Goodbye to Passwords," Alex Simons, Manini Roy, Microsoft Ignite 2017

⁵ Google Research, Security Keys: Practical Cryptographic Second Factors for the Modern Web

Triển khai dễ dàng

Phòng IT có thể triển khai YubiKey chỉ trong vài ngày. Một khóa duy nhất có thể tích hợp cả những hệ thống mới và cũ, loại bỏ nhu cầu sử dụng nhiều khóa hoặc tích hợp thêm.



Khả năng của YubiKey: Các chức năng này được bao gồm trong các khóa bảo mật YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS và YubiKey 5C Nano FIPS. Thông số kỹ thuật chi tiết có trên digibit.vn.

Công ty hàng đầu trong lĩnh vực xác thực

Yubico là nhà phát minh chính của tiêu chuẩn xác thực FIDO2/WebAuthn và U2F, và là công ty đầu tiên sản xuất khóa bảo mật U2F cũng như thiết bị xác thực đa giao thức FIDO2/WebAuthn.

YubiKey được sản xuất tại Mỹ và Thụy Điển, đảm bảo an toàn và kiểm soát chất lượng nghiêm ngặt.

Chứng nhận FIPS 140-2

Bảo vệ tổ chức của bạn bằng giải pháp xác thực đa yếu tố YubiKey tốt nhất được chứng nhận FIPS 140-2 Overall Levels 1 và 2, Physical Security Level 3. Dòng YubiKey 5 FIPS cho phép các cơ quan chính phủ và các bộ ban ngành được quản lý đáp ứng các yêu cầu cấp độ đảm bảo xác thực cao nhất 3 (AAL3) theo tiêu chuẩn NIST SP800-63B mới.



Liên hệ
digibit.vn



Tìm hiểu thêm
yubi.co/fips