



Security Summit

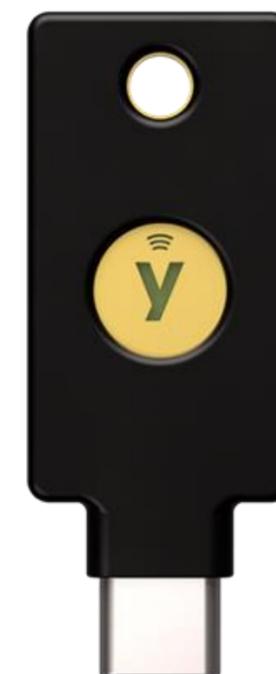
Milano 17-18-19 marzo 2026



Sessione

Yubico: Oltre le password – come MAIRE è passata al livello successivo

Gianni Fiumara | Ignition Presales System Engineer
Andrea Sgarlata | Gruppo MAIRE Identity Manager



Speakers



Gianni Fiumara

Ignition



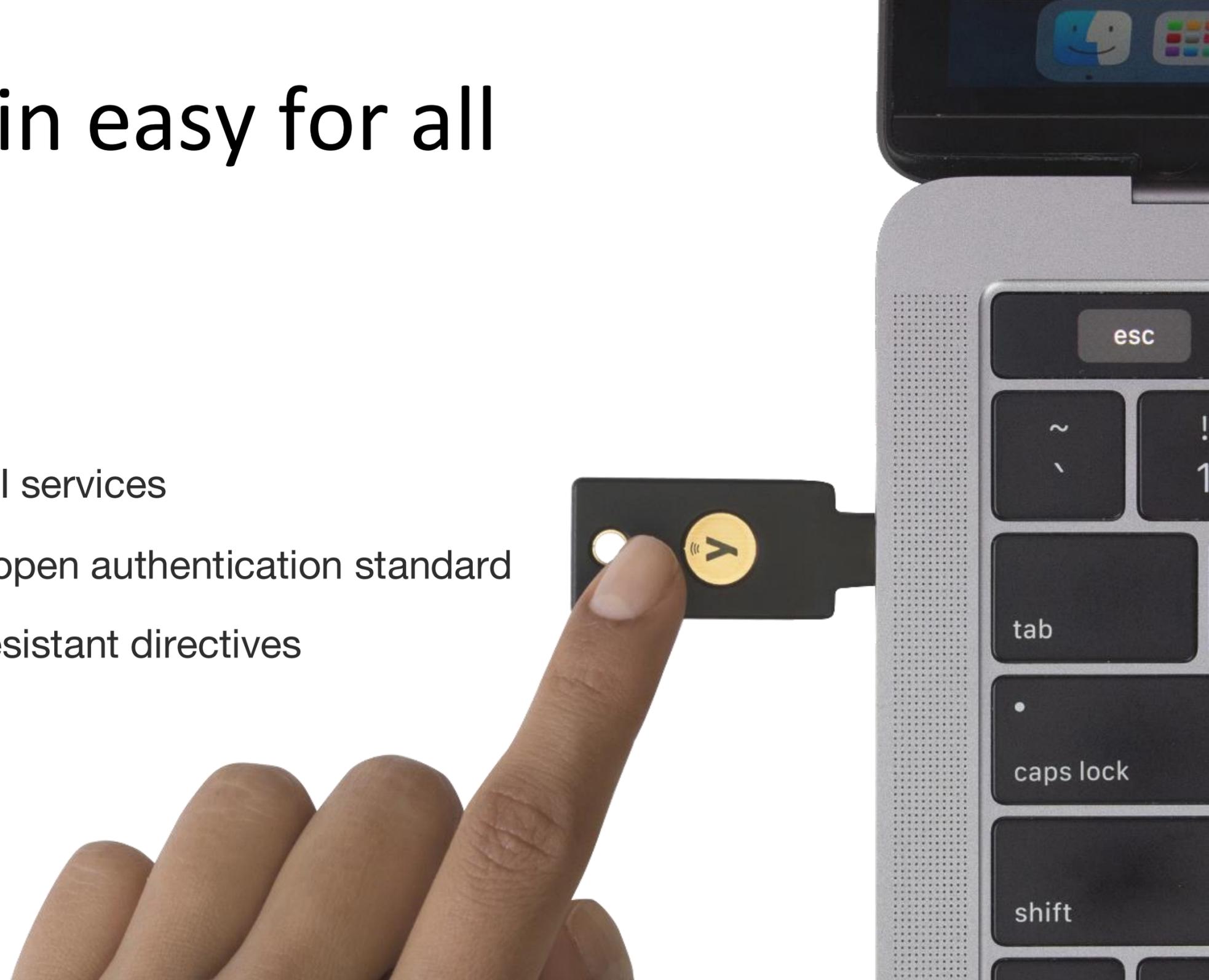
Andrea Sgarlata

Gruppo MAIRE

Making secure login easy for all

- Yubico was founded 2007
- Inspired by the word 'ubiquity'
- One simple security key to protect all services
- Leading inventor of FIDO / Passkey open authentication standard
- Driver of US government phishing-resistant directives

fidoTM



How the YubiKey Works



Strongest security with the fastest user experience for authentication



Enter PIN (or password)

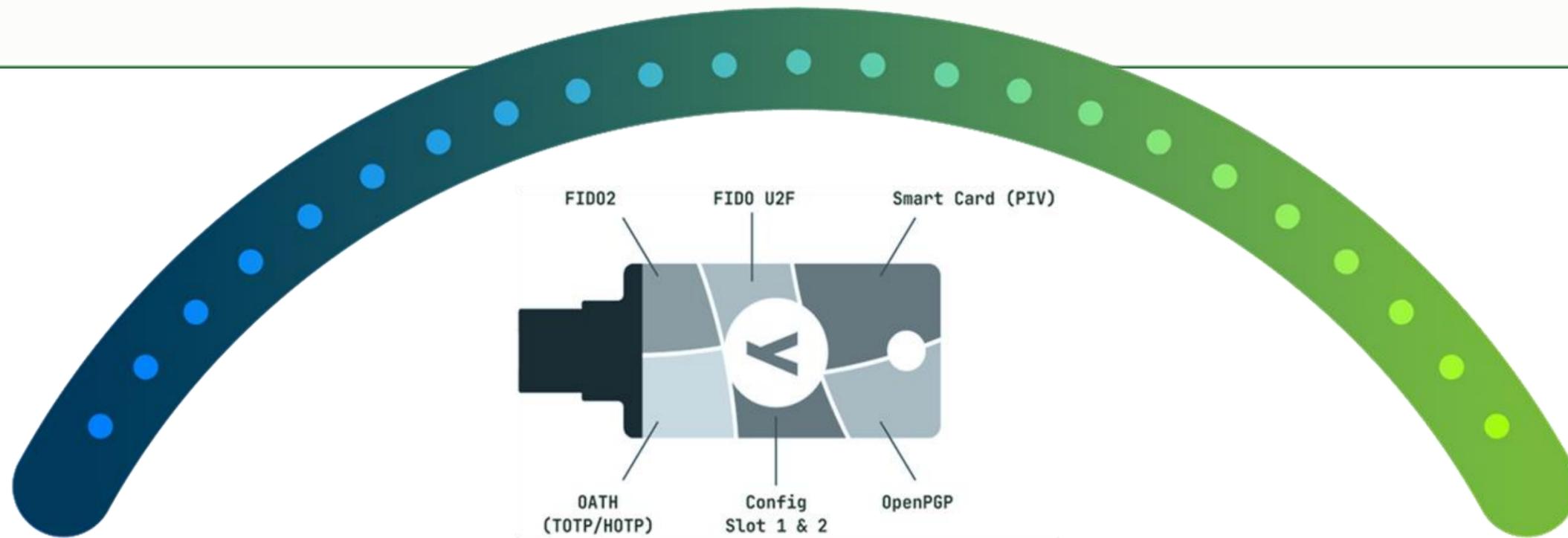
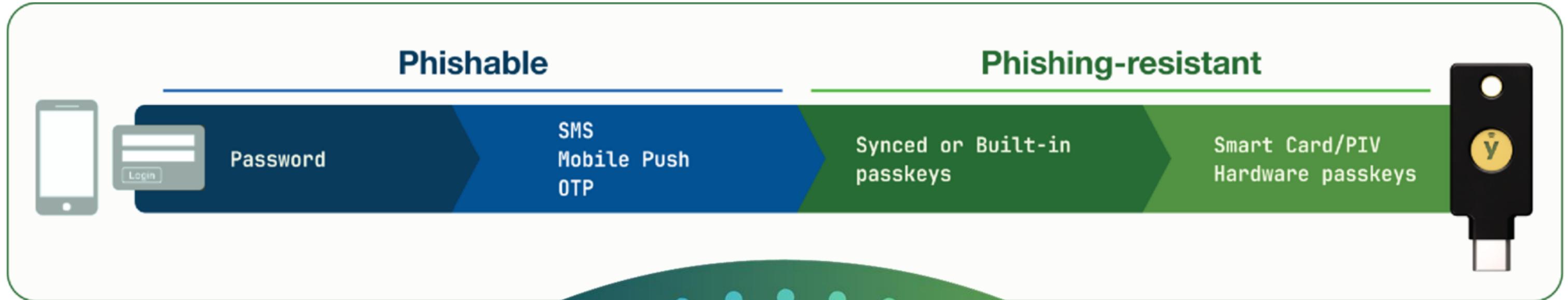


Touch or tap YubiKey



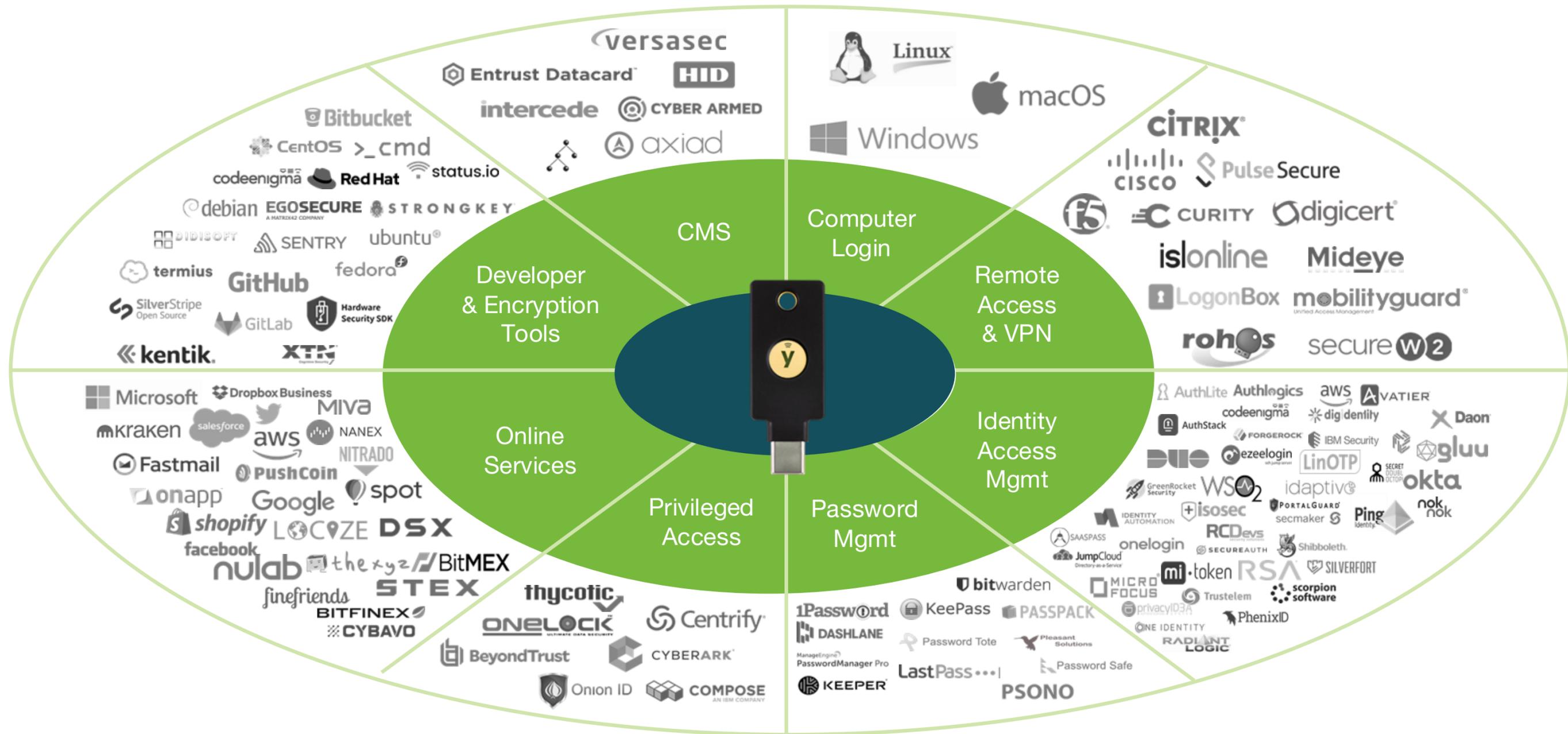
Use once

Strongest MFA & Bridge to Passwordless



Secure today, future proof for tomorrow.

YubiKey works with 1000+ applications

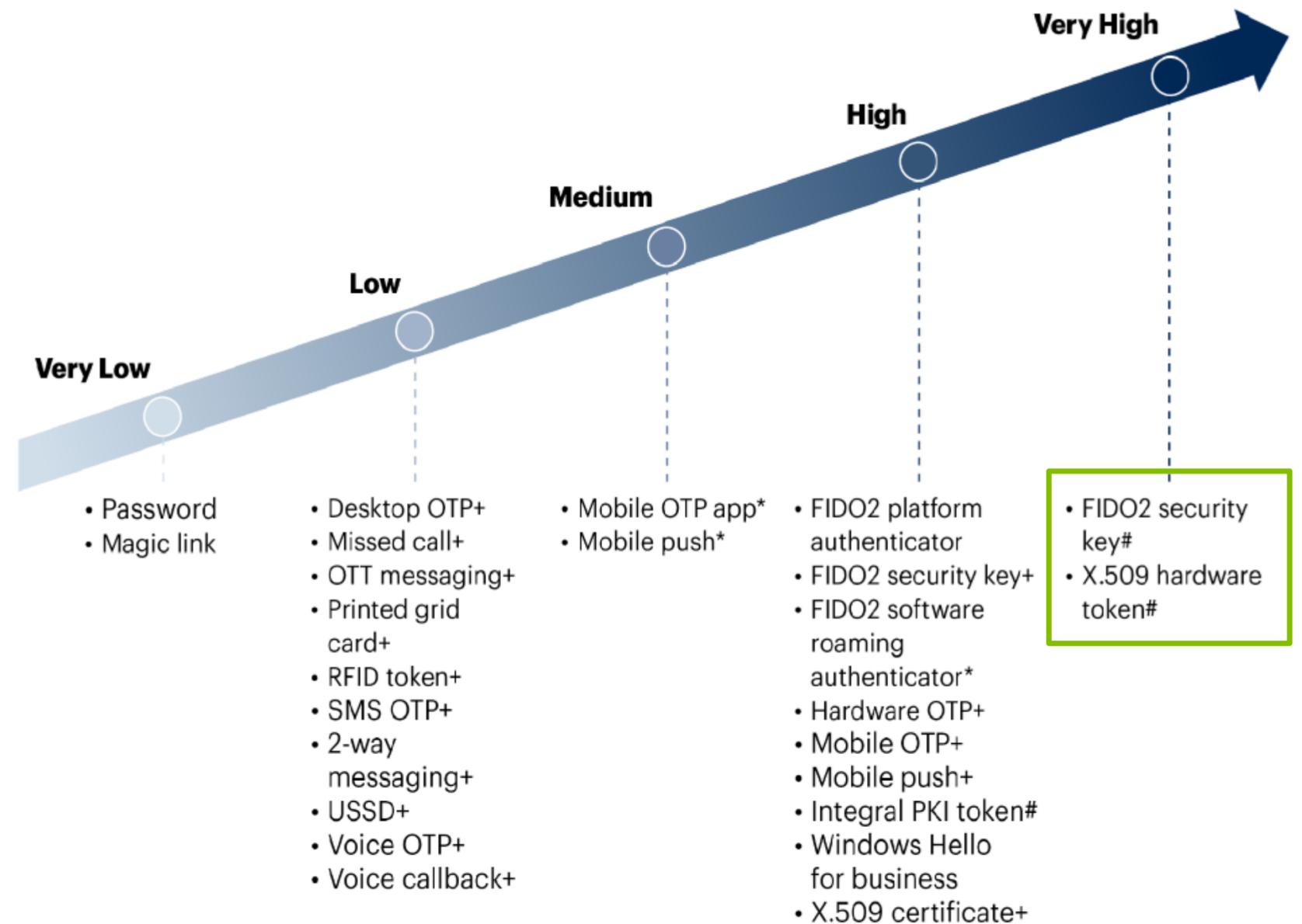


YubiKeys Offers The Highest Level of Security

Gartner Report: The Must-Have IAM Requirements for Enterprise Applications 6.5.25

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. Not for redistribution

The Gartner Trust Scale for Authentication



+ = with a password as a second factor; * = with local authentication; # = with biometric or PIN

Source: Gartner

782650_C

Gartner

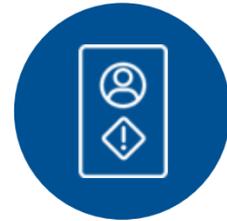
Protecting all users in the enterprise

Customer business scenarios



Privileged Access

Secure privileged account users



Mobile Restricted

Secure call centers for mobile restricted users



Shared Workstation

Protect shared workstation users



Remote Workforce

Enable remote workforce



Office Workers

Improve UX and security for office workers



3rd Party Access

Protect corporate system access by 3rd parties



End Customers

Safeguard Yubico's customers' end-customers

Start by addressing key user populations

Expand to broader set of stakeholders

Trusted Brands Trust Yubico



Introducing...





Introducing Maire



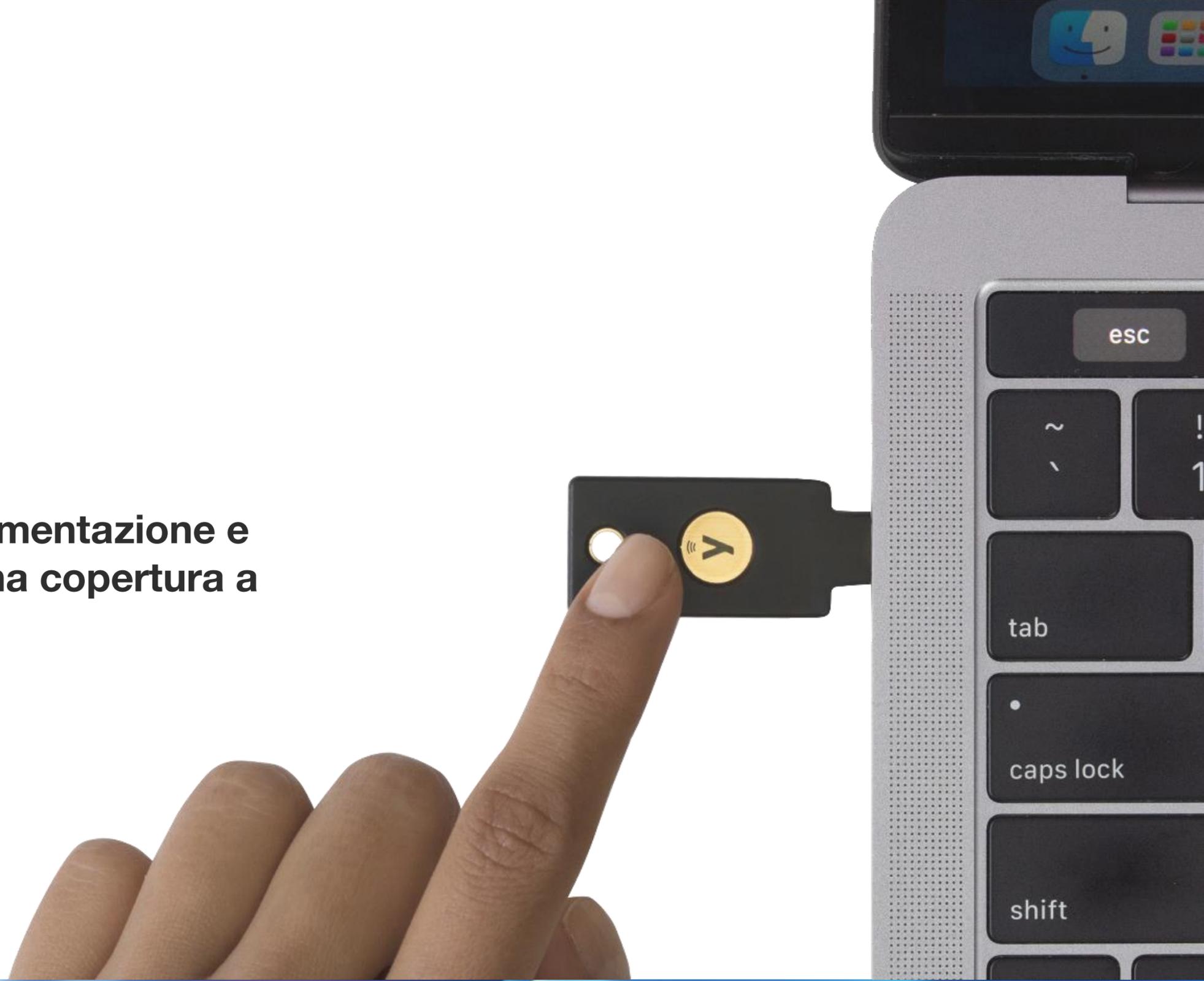
Andrea Sgarlata is an Identity Manager at the MAIRE Group, where he leads Cyber Risk Operation Center initiatives focused on identity protection. He coordinated the adoption of passwordless authentication using YubiKey for both digital and physical use cases. With over ten years of experience in Identity Management and Zero Trust, he is a frequent speaker at international events such as SailPoint Navigate and Microsoft Security events.

Andrea Sgarlata

Gruppo MAIRE

Q&A

- **Perché Yubico?**
- **Qual è stata la prima idea di implementazione e come si è evoluta sino ad avere una copertura a 360 gradi e worldwide?**



Passwordless Strategy



Deploy password replacement option

- ✓ Identify and provide alternative to the users (Fido2/PIV security Keys). Password coexistence is accepted
- ✓ Identify test users as representative organization target
- ✓ Perform systems change and setup for allowing passwordless authentication
- ✓ Perform systems change and setup for allowing passwordless authentication
- ✓ Validate passwordless authentication



Transition into a passwordless deployment

- ✓ Awareness campaign, positively promote the change to the users
- ✓ Gradually include remaining user
- ✓ Password scrambling and rotation



Reduce user-visible password surface area

- ✓ Minimize password prompts
- ✓ Survey test users for password usage and plan password mitigations. Users know their own password but should never be used



Eliminate passwords from the identity directory

- ✓ Remove password usage for administrators
- ✓ Remove passwords from the identity directory, IT and administrators have no longer access to users passwords
- ✓ Enforce robust authentication methods leveraging on passwordless authentication
- ✓ Continuous improvement, remain informed about advancements in passwordless technologies and adjust your strategy accordingly

Q&A

- Quali sono i prossimi step?



yubico

The Key to Trust