

yubico

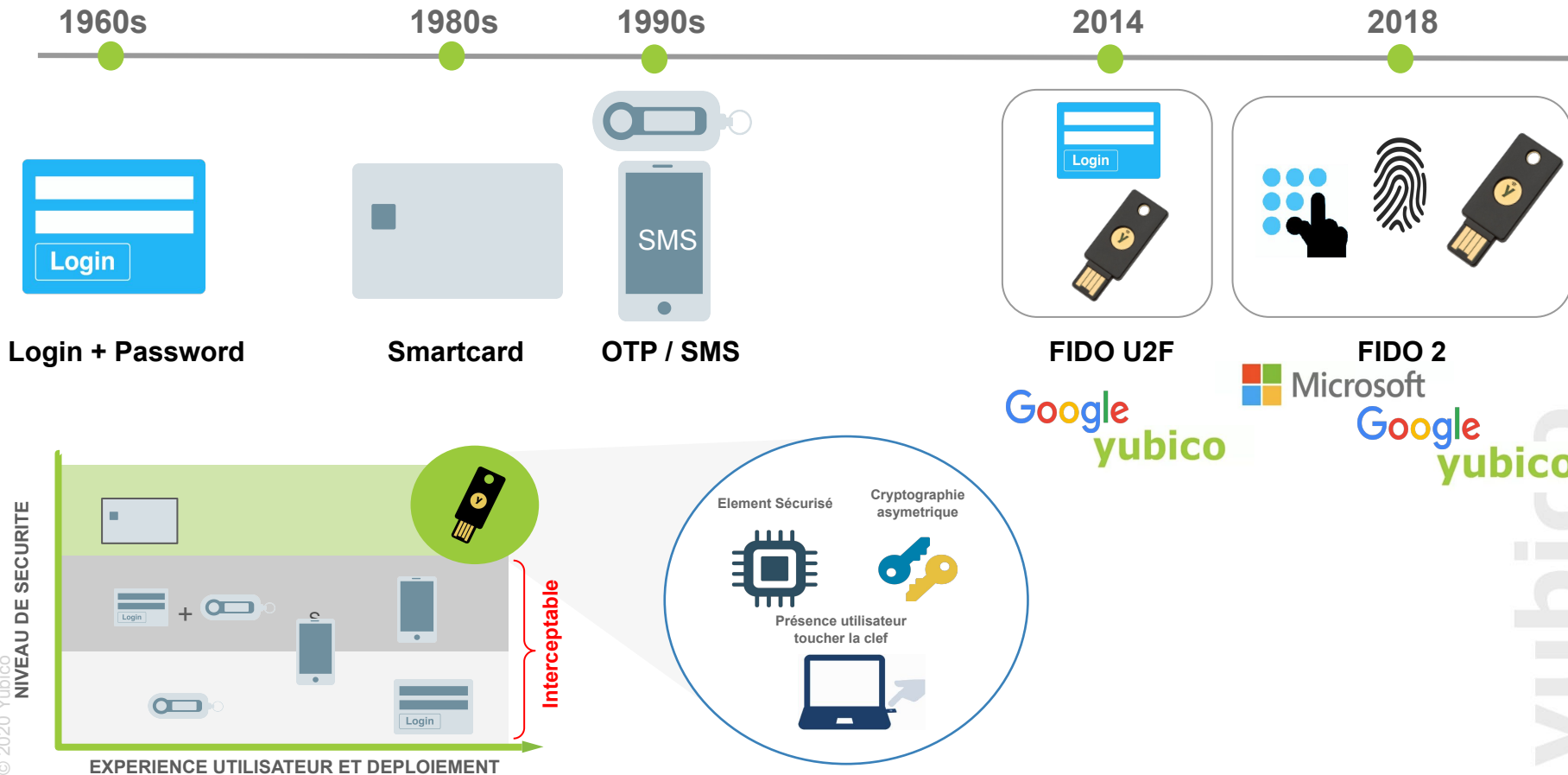
La simplicité au service de
l'authentification



Partenariat CERTA

- **Activité pédagogique :** Équiper les classes/étudiants public ou privés sous contrat proposant le BTS Cybersécurité et Services Informatiques aux Organisations de YUBIKEYS pour réaliser des tests.
 - Réseau CERTA (<https://www.reseaucerta.org>)
 - Former les futurs administrateurs, RSSI, DSI
- **Population cible :** Étudiants et enseignants de 250 sections de BTS SIO réparties sur l'ensemble du territoire français et des DOM-TOM (lycées publics et privés sous contrat).
- **Session:** 4 sessions Webinaires + démos
- **Type de clés concernées:** YUBIKEYS 5C NFC (USBC) OU 5 NFC (USBA)
- Bénéficiaire de tarifs spécifiques « Education » via INMAC
<https://www.inmac-wstore.com/>

Evolution des protocoles

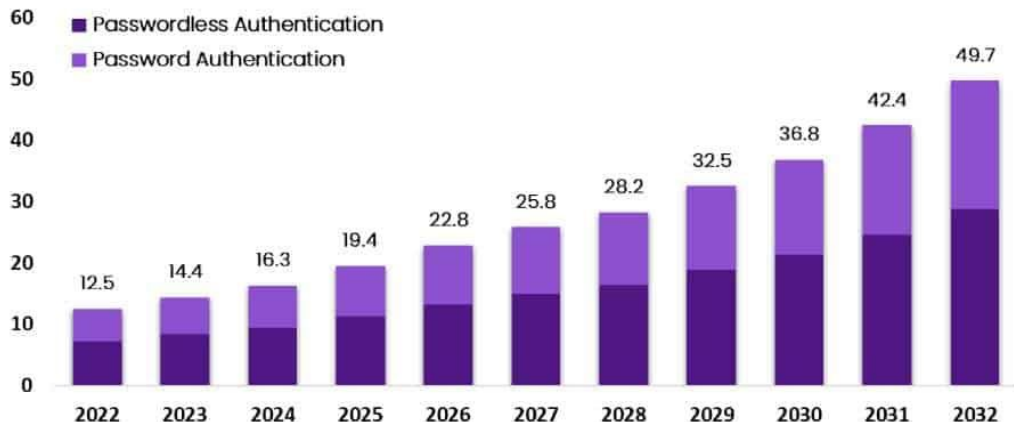


yubico

Le marché

Global Multi-Factor Authentication Market

Size, by Authentication Type, 2022-2032 (USD Billion)



The Market will Grow
At the CAGR of:

15.2%

The forecasted market
size for 2032 in USD:

\$49.7B



market.us
HOW MUCH DATA YOUR FIRM REPORTS



Zero Trust



yubico

“Les attaquants ne hackent plus, ils se connectent”

74%

Les attaques de passwords ont explosé : +74% en un an, et 921 attaques par seconde.¹

54%

Des personnes sondées ont partagé leur mot de passe dans les 12 derniers mois³

70\$

Le coût moyen du reset d'un mot de passe selon Gartner⁶

40 000

Attaques de MFA “fatigue” par mois²

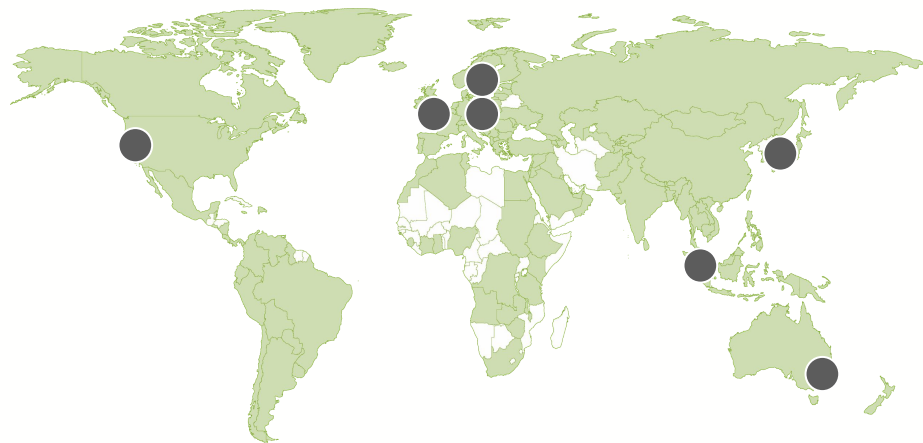
250%

Coût moyen d'augmentation des assurances cyber.⁵



1. Microsoft Digital Defense Report 2022
2. Azure Identity Protection
3. Enquête mondiale sur l'état de l'authentification des entreprises, Yubico
4. Statista 2021
5. Business Insurance, Hospitality sector steps up risk controls as cyber, other threats rise, February 2022
6. Forrester

Yubico - acteur majeur de l'authentification forte



■ Clients Yubico

● Bureaux Yubico

- Fondé en Suède en 2007
- 400 employés dans 10 pays
- 20M+ YubiKeys et + de 5000 entreprises équipées



La YubiKey



yubico

YubiKeys : les gammes

YubiKey 5 Series



Protocoles

FIDO 2

FIDO U2F

Smart Card

TOTP / HOTP

Slot 1&2

Open PGP

YubiKey Bio Series / Security Keys Series



Protocoles

FIDO 2

FIDO U2F

Smart Card

TOTP / HOTP

Slot 1&2

Open PGP

YubiHSM 2 Series



Cryptographic capabilities

Hashing (used with HMAC and asymmetric signatures)

- SHA-1, SHA-256, SHA-384, SHA-512

RSA

- 2048, 3072, and 4096 bit keys
- Signing using PKCS#1v1.5 and PSS
- Decryption using PKCS#1v1.5 and OAEP

Elliptic Curve Cryptography (ECC)

- Curves: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519
- Signing: ECDSA (all except curve25519), EdDSA (curve25519 only)
- Decryption: ECDH (all except curve25519)

Random numbers

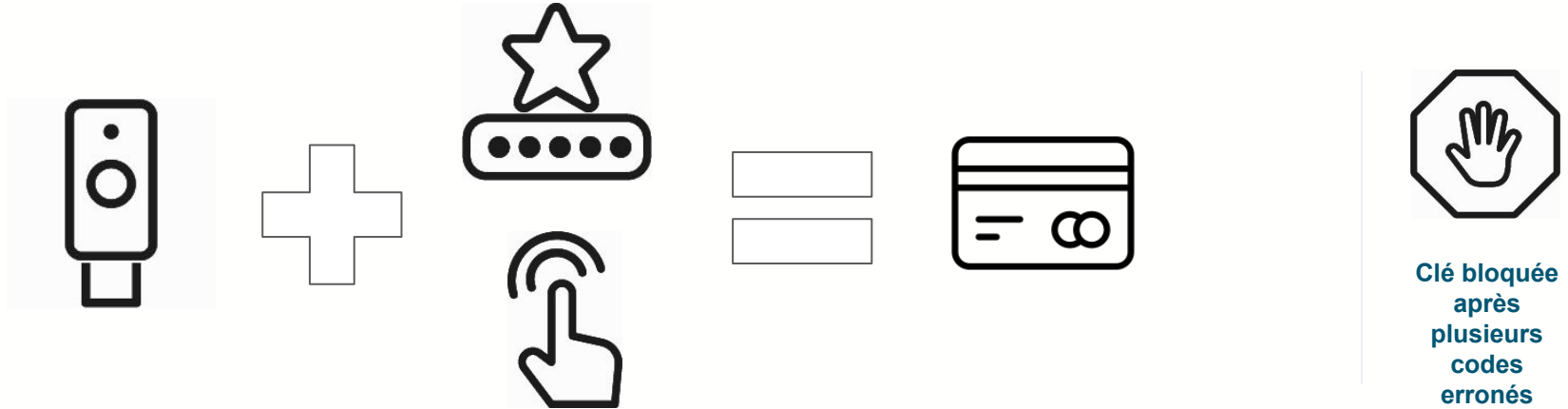
- On-chip True Random Number Generator (TRNG) used to seed NIST SP 800-90 AES 256 CTR_DRBG

Proposition de valeur



yubico

Expérience “Carte Bleue”



Ce que j'ai et ce que je sais / suis

Pré-enrôlement possible avec PIV et bientôt FIDO2.1

Cas d'usages et enjeux métiers



yubico

Enjeux métiers et cas d'usages

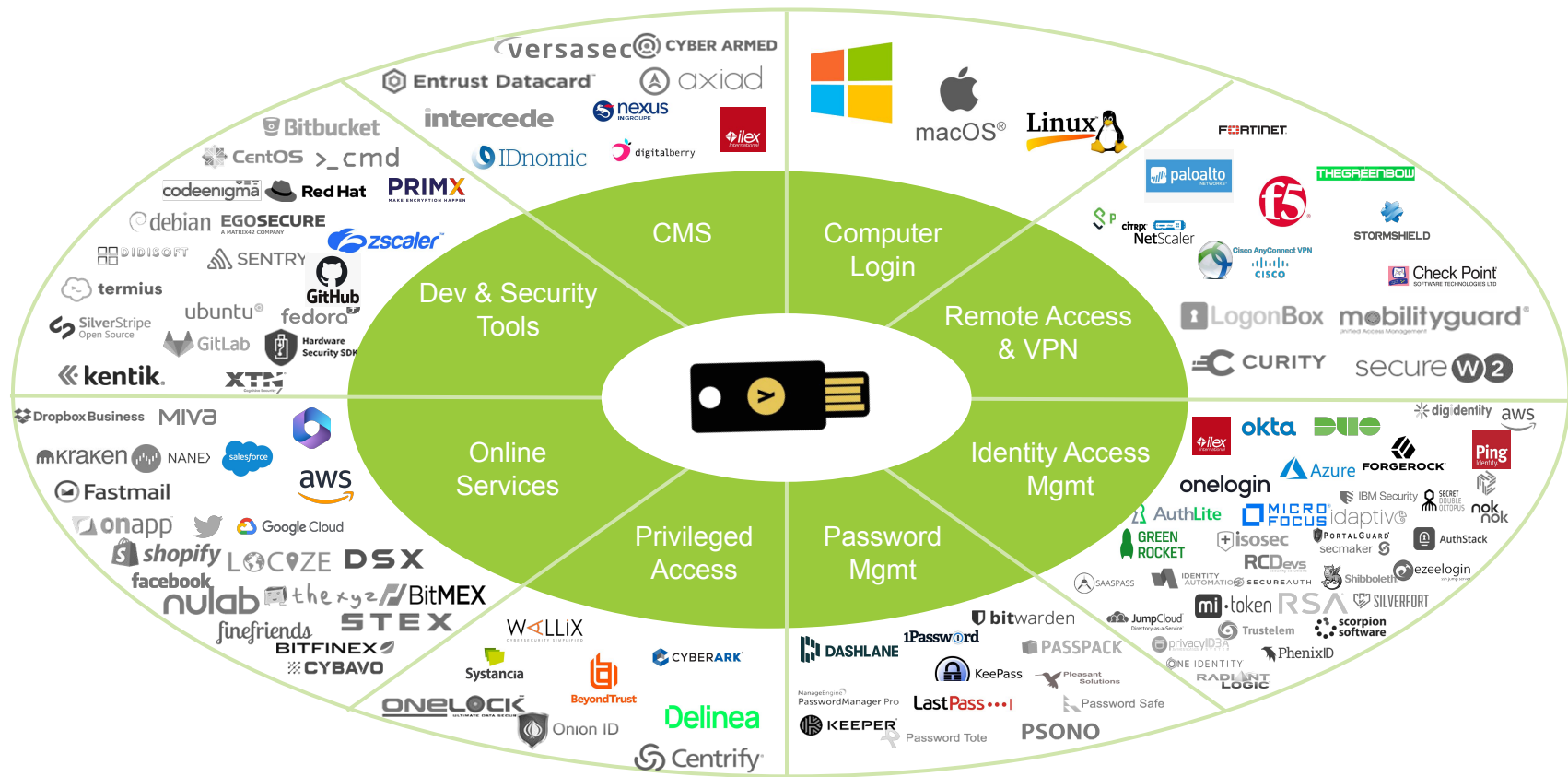
Enjeux métiers



Authentification autour des services et applications



Compatible avec plus de 1000 applications



yubico

Comparatif des méthodes

Cas d'usage		YubiKey Yubico 	OTP App Duo, Okta, Google, MSFT	Smart Card Thales, HID	Windows Hello Microsoft	FIDO built into iOS & Android (Apple, Google)
Sécurité	Résistance au phishing - protège contre les attaques MiTM	OUI	NON	OUI	OUI	Partielle
	Certifications CSPN & FIPS	OUI	NON	OUI	NON	NON
	Éléments sécurisés, firmware et chaînes de prod dédiées	OUI	Dépend	Dépend	Dépend	Dépend
Simplicité	Compatible avec la plupart des solutions IAM et Cloud	OUI	OUI	NON	NON	OUI
	Équipement de spare sécurisé et abordable	OUI	NON	OUI	NON	NON (2 devices)
	Indépendance au réseau	OUI	NON	OUI	OUI	Future
	Compatible postes de travaux, tablettes et mobiles	OUI	NON	Partiel	NON	Future
	Compatible postes partagés, kiosques	OUI	NON	OUI	NON	NON
	Multi périphériques	OUI	OUI	OUI	NON	OUI
	Multi-protocoles en un équipement	OUI	NON	NON	Partiel	Partiel
Stand alone	Pas besoin de plateforme ou de solution tierce	OUI	NON	OUI	NON	NON

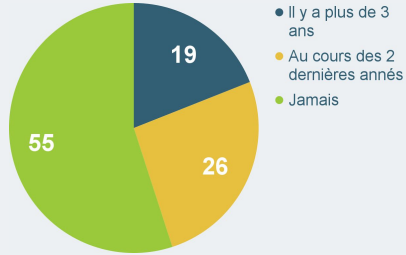
Pour aller plus loin



yubico

Best Practices

Dernières fois que vous avez perdu vos clefs de maison



- Il y a plus de 3 ans
- Au cours des 2 dernières années
- Jamais

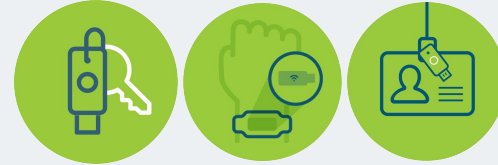


Spare - réactivité

Sur chaque site - possibilité de révoquer et réenrôler

Backup - profils á risque

VIP, IT, Management, Users distants



Oubli

Vol



Autre méthode
Push - TAP

Révocation



Autre méthode
Push - TAP

Prochaines sessions:

2. Jeudi 23 janvier 2025 18h00 - 19h00

Authentification sur M365 en FIDO2 + Démonos

3. Jeudi 27 Mars 2025 18h00 - 19h00

Ouverture de session Windows en FIDO2 + Démono

4. Date à définir

Ouverture de session Smart Card + Démono



yubico