yubico

La simplicité au service de l’authentification

“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 mois[3]

70$

Le coût moyen du reset d’un mot de passe selon Gartner[6]

40 000

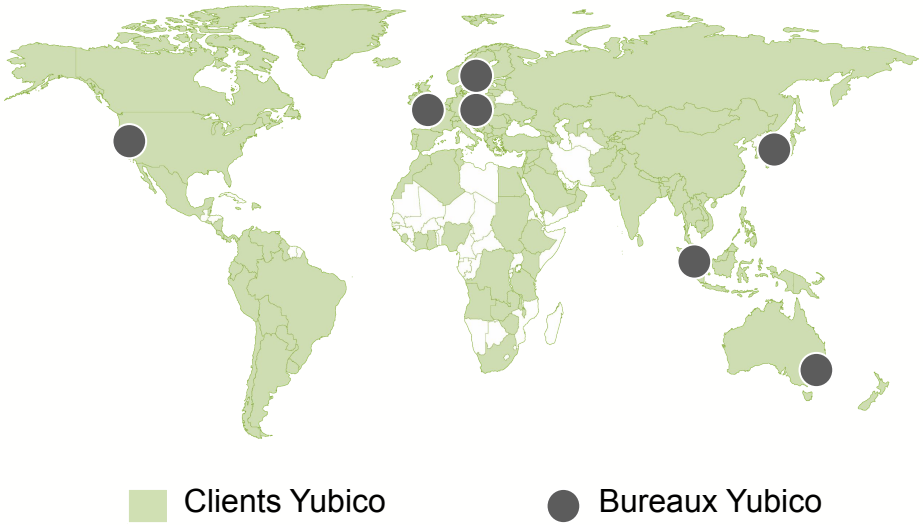
Attaques de MFA “fatigue” par mois[2]

250%

Coût moyen d’augmentation des assurances cyber.[5]

1. Microsft 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



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

Technologie


Finance & Assurance

Industrie

Retail & Services

Public, Education

Santé

La YubiKey

yubico

YubiKeys : les gammes

YubiKey 5 Series

Protocoles

- FIDO 2
- FIDO U2F
- Smart Card
- TOTP / HOTP
- Slot 1&2
- Open PGP

YubiKey 5 CSPN 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

Nouveautés 5.7 - natif

100 device bound passkeys FIDO2

64 OATH seeds

24 PIV slots

2 OTP seeds

+Grandes clefs RSA

Supporting RSA-3072 and RSA-4096 keys

New key types

Adding Ed25519 and X25519 keys

Advanced key management

Flexibility to move and delete PIV keys

Nouveautés 5.7 - custom

-Complexité du PIN (pas de suites ni de répétitions)

-Longueur minimale PIN*

-Forcer le changement du PIN au 1er login*

-Entreprise attestation

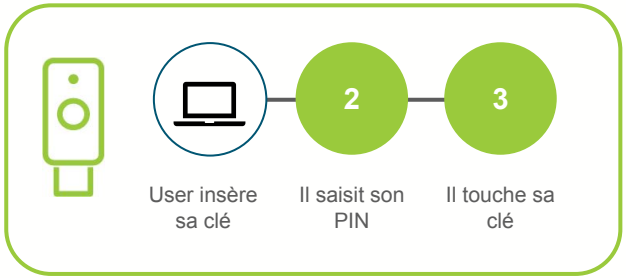
* *Possible de le faire à travers YKMAN / CLI*

Proposition de valeur

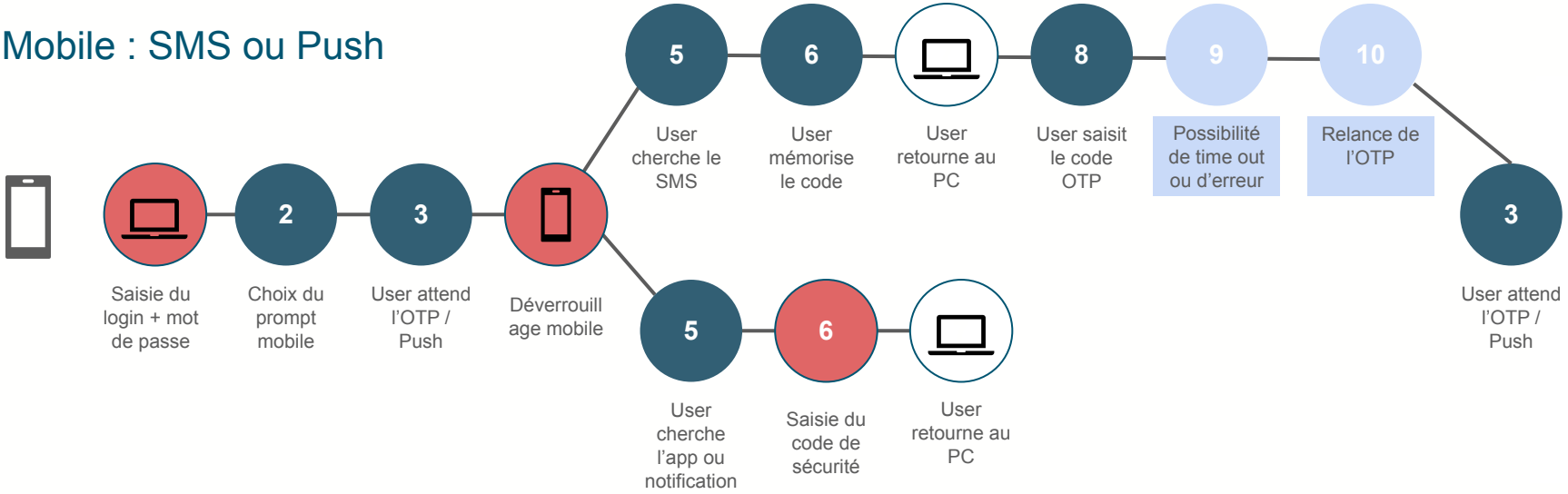
yubico

Productivité

FIDO2 & PIV



Mobile : SMS ou Push



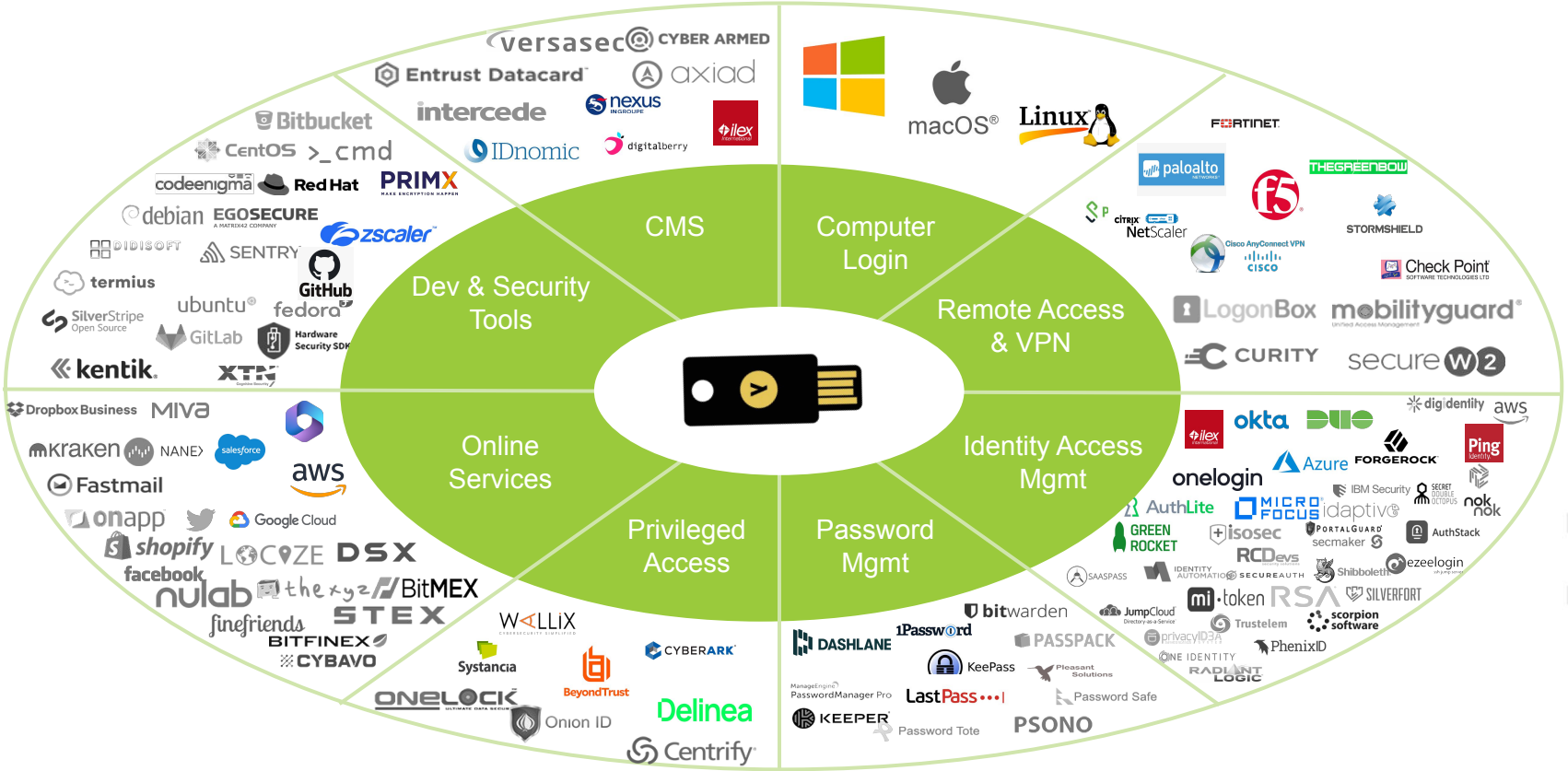
Le mode carte bleue - la fin de la complexité

Déporter la complexité de l’utilisateur vers la solution

Cas d’usages et enjeux métiers

yubico

Compatible avec plus de 1000 applications



Enjeux métiers et cas d'usages

Enjeux métiers

Comptes à privilèges | Mobile restreint | Postes partagés | Mobilité et télétravail | Employés | Partenaires | Clients finaux

Authentification autour des services et applications

Applications Web

Google Cloud, aws, salesforce, GitHub

Ouverture de session

macOS®, Linux

VPN & VDI

Pulse Secure, FORTINET, THEGREENBOW, NetScaler, paloalto, STORMSHIELD, f5, Cisco AnyConnect VPN, Check Point

IAM / SSO

ilex, okta, FORGEROCK, DUO, Ping Identity, onelogin

Tous les services et applications

WALLIX, zscaler, BeyondTrust, CYBERARK, PRIMX, Systancia

Postes partagés

yubico

Les enjeux

Efficacité

Connexion rapide

Impacts support IT

Traçabilité

Qui se connecte ?

Comptes génériques

Coûts

BYOD

Impacts indirects

Sécurité

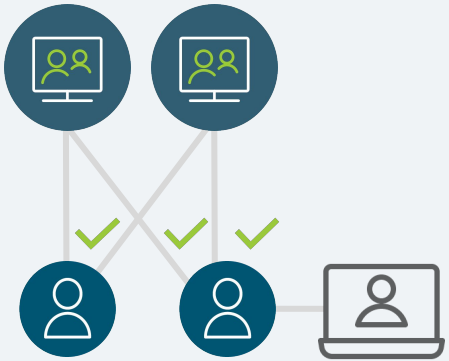
Difficile à maintenir

Solutions inadaptées

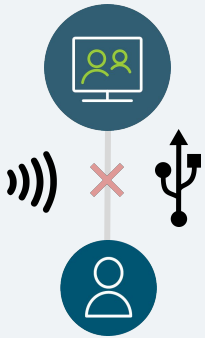
Les besoins

Plusieurs clés sur un compte générique

Plusieurs postes et un compte nominatif



Verrouillage de la session au retrait de la clé



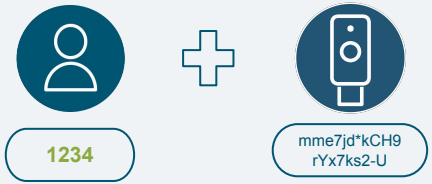
yubico

Scénarios pour toutes les architectures

Poste isolé sans aucune application tierce

Mots de passe complexe

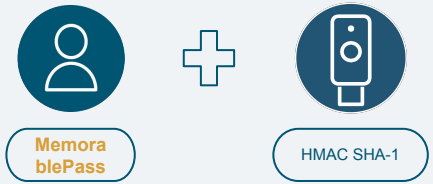
*1234mme7jd*kCH9rYx7ks2-U*



Poste isolé avec Yubico Login for Windows

Mots de passe simplifié

MemorablePass



Poste connecté à l'AD on-premises ou Azure

PIN code + certificate / passkey

132436

Bénéfices pour HYATT®

Facilité d’usage - Acceptation

Moins de prompts & connexion 4 fois plus rapide

Aucun ticket support - déploiement facilité grâce à l’UX

Plus de mots de passe

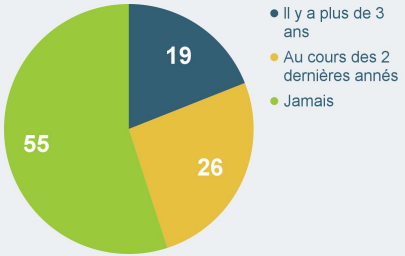
Expérience client optimale

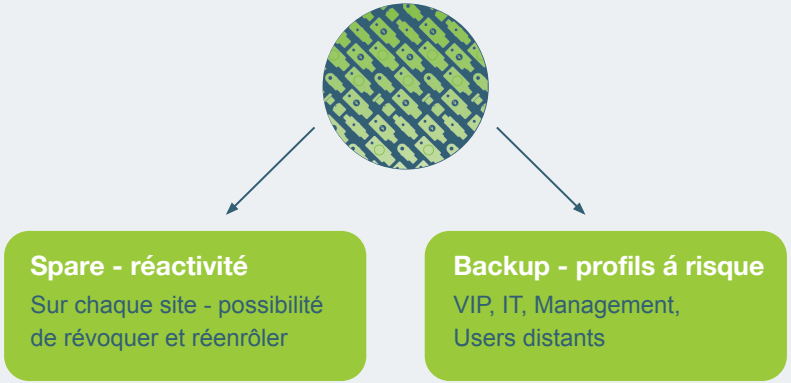
Pour aller plus loin

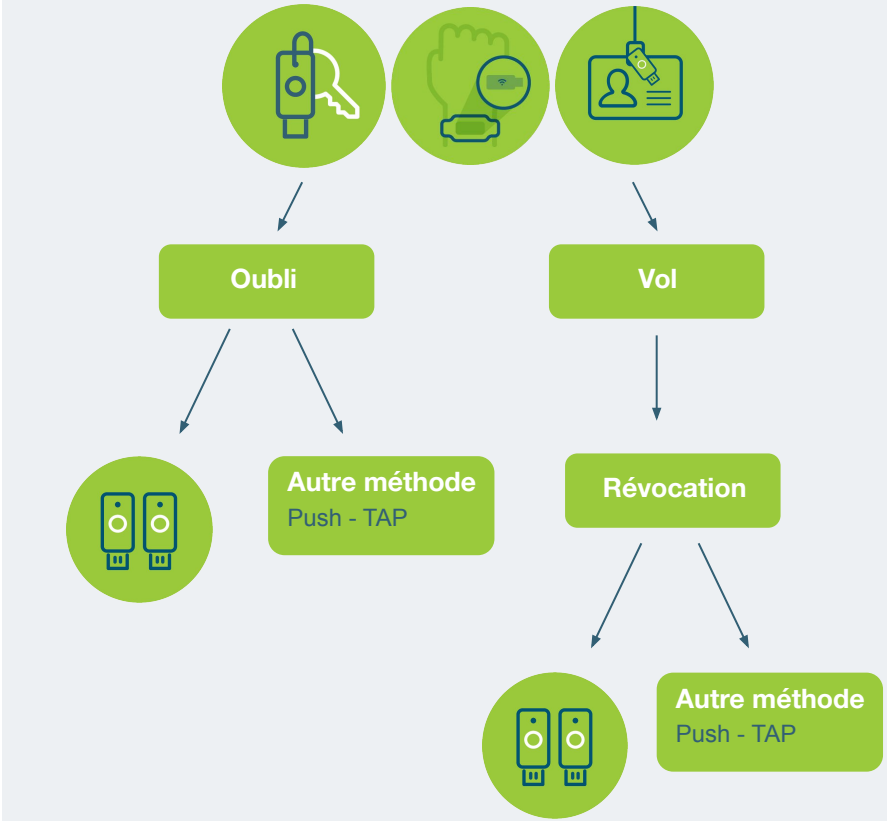
yubico

Best Practices

Dernières fois que vous avez perdu vos clefs de maison







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
	Equipement de spare sécurisé et abordable	OUI	NON	OUI	NON	NON (2 devices)
	Indépendance au réseau	OUI	NON	OUI	OUI	Future
	Compatible postes de travails, 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

YubiHSM

yubico

Le YubiHSM

Attractif

Abordable
Chaîne d'approvisionnement sécurisée
Fabrication **haute qualité**

Efficace

Format **Nano**
Faible consommation d'énergie
Extrêmement **durable**

Intégrable

Solution "plug and play"
Network HSM
Environnements virtualisés

YubiHSM : Cas d'usages

PKI

Protège l'infrastructure **smart card/PKI**

Maintient la clé privée de l'**Autorité de Certification** stockée en toute sécurité

Industrie

Assure **l'intégrité de la chaîne logistique** dans les usines

Permet une **communication sécurisée entre les devices IoT**

Signature de codes

Assure l'**intégrité des applications**

Garantit la livraison d'**applications inviolables**

Cryptomonnaie

Sécurise **l'écosystème crypto**

Protège l'**échange** de cryptomonnaie