

MFA souverain, universel et sans smartphone obligatoire

La plateforme souveraine d'authentification et de gestion des identités

POURQUOI AGIR MAINTENANT ?

Les mots de passe compromis, les OTP interceptés et les parcours d'accès fragmentés exposent les comptes des collaborateurs, partenaires et clients.

Les environnements hybrides ajoutent une difficulté : appliquer des politiques cohérentes à des applications cloud, sur site et historiques.

Les organisations doivent **moderniser l'authentification**, **réduire la dépendance aux mots de passe** et au **smartphone**, **fédérer** les identités et **tracer les décisions** d'accès.

TrustBuilder réunit ces fonctions dans une plateforme conçue pour préserver la maîtrise des identités, des accès et des données.

LA RÉPONSE TrustBuilder

Une solution MFA souveraine destinée aux collaborateurs, partenaires et clients. TrustBuilder renforce l'accès aux applications cloud, sur site, web et mobiles, sans imposer l'usage d'un smartphone.

L'authentification s'effectue sur poste de travail, navigateur enrôlé, application mobile ou clé FIDO.

Chaque organisation retient les méthodes adaptées à ses utilisateurs et à ses applications.

Les fonctions de SSO et de fédération facilitent l'intégration du MFA dans les environnements existants.

TRUSTBUILDER EN CHIFFRES

500+

Clients dans le monde

85

Collaborateurs

60+

Partenaires technos

2012

1^{er} brevet déposé

99,95%

SLA annuel

MFA CERTIFIÉ ANSSI

Solution MFA certifiée CSPN par l'ANSSI, fondée sur une technologie brevetée à clés dynamiques.

SANS SMARTPHONE OBLIGATOIRE

Authentification possible sur poste de travail, navigateur enrôlé, application mobile ou clé FIDO.

INTÉGRATION RAPIDE

Plus de 50 intégrations documentées. SAML, OpenID Connect, RADIUS, LDAP Proxy, API et SDK. POC opérationnel en deux jours.

SOUVERAINETÉ

Maîtrise des données et des infrastructures : une part majeure des serveurs est hébergée en France, le reste en Belgique.

MFA UNIVERSEL

Authentification forte des collaborateurs, partenaires et clients sur les applications cloud, sur site, web et mobiles.

EXPÉRIENCE UTILISATEUR

MFA passwordless, authentification adaptative et self-service. Le SSO simplifie les parcours lorsque cette fonction est utilisée.

UNE ARCHITECTURE MODULAIRE EN 3 COMPOSANTS

TRUSTBUILDER.IO

Composant SaaS qui administre les politiques MFA, les sessions, les notifications et les règles d'authentification adaptative.

TRUSTBUILDER.CONNECT

Couche d'intégration entre TrustBuilder MFA, les applications, les annuaires et les services externes. Elle prend notamment en charge OIDC et SAML.

TRUSTBUILDER.MFA

Service d'authentification passwordless et de signature de transactions fondé sur une technologie propriétaire, utilisable avec ou sans smartphone.



Enrôlement

- Self-service
- Administration déléguée
- Intégration de parcours de vérification d'identité et de prestataires KYC
- Synchronisation d'annuaires



Authentification

- MFA et passwordless
- SSO et fédération d'identité
- Authentification contextuelle
- Évaluation du risque d'accès et adaptation du parcours



Autorisation

- Contrôle d'accès fondé sur des politiques, PBAC
- Décisions granulaires selon le contexte, le rôle et la ressource
- Sélection du persona dans le parc

L'AVANTAGE DIFFÉRENCIANT

Les clés dynamiques brevetées

✗ Clés statiques (marché)

OTP = Fonction (clé secrète + compteur)

- Vol de la clé secrète = OTP valides à l'infini
- Sensible au reverse-engineering
- Dépendance au smartphone

✓ Clés dynamiques TrustBuilder

OTP = Fonction (clé + PIN + compteurs + clé service + données app + clés aléatoires)

- PIN jamais stocké, clés renouvelées
- Sécurité renforcée fondée sur des mécanismes propriétaires de clés dynamiques
- Multi-supports : PC, navigateur, mobile, FIDO

Protocoles et API	SAML 2.0 • OpenID Connect • RADIUS • LDAP Proxy • API REST et SOAP • SDK Java, Web, iOS et Android
VPN et Réseau	Fortinet • Ivanti / Pulse Secure • Citrix • F5 • Palo Alto • Stormshield • Sophos
Cloud et SaaS	Microsoft 365 • Google Workspace • Salesforce
IAM et SSO	AD FS • Microsoft Entra ID • Okta • Ping • SailPoint • Shibboleth • FranceConnect
PAM, bastion et SIEM	CyberArk • Wallix • BeyondTrust • One Identity • Delinea / Thycotic

Plus de 50 intégrations documentées couvrent les principaux environnements réseau, cloud, IAM, SSO et PAM. Les protocoles standards facilitent aussi la connexion aux applications existantes.

OTP à secret partagé

OTP = fonction d'un secret et d'un compteur ou d'un temps

- Un secret compromis reste exploitable jusqu'à sa révocation ou son renouvellement.
- Un OTP saisi par l'utilisateur peut être intercepté lors d'une attaque de phishing en temps réel.
- La sécurité repose durablement sur la protection du secret partagé.

Clés dynamiques TrustBuilder

Le mécanisme combine plusieurs éléments de contexte et renouvelle les clés utilisées.

- PIN non stocké et clés régulièrement renouvelées.
- Le renouvellement des clés limite l'exploitation durable d'un secret compromis.
- La liaison au contexte renforce la protection contre le phishing et le jeu.
- Plusieurs supports : poste de travail, navigateur, mobile et FIDO.

MFA certifié ANSSI / CSPN • Technologie brevetée à clés dynamiques • Données hébergées en France et en Belgique



PASSEZ À UN MFA SOUVERAIN, UNIVERSEL, SANS DÉPENDANCE ET SANS SMARTPHONE OBLIGATOIRE

Oprium - Distributeur et intégrateur TrustBuilder
Audit • Conseil • POC • Intégration • MCO • Support