Sécurisez vos messageries

professionnelles contre les cyberattaques

Protect
BY MAILINBLACK

MAILINBLACK

Qui sommes-nous ?

20 ans
d'expertise en cybersécurité

14 mille
organisations protégées

96 %
de nos clients renouvellent

+1 milliard
d'emails bloqués chaque année

La FRENCH TECH

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Best Workplaces 50 à 250 salariés Great Place To Work. FRANCE 2022

RGPD

Nos solutions innovantes et accessibles qui protègent vos collaborateurs des risques cyber du quotidien :

Protect
BY MAILINBLACK

Sécurisez les messageries professionnelles contre les cyberattaques

- Anti : virus, phishing, spearphishing, spam, ransomware
- Technologies propriétaires couplées à de l'IA
- Analyse des liens dans les emails (Secure Link)
- Messagerie propre et sécurisée

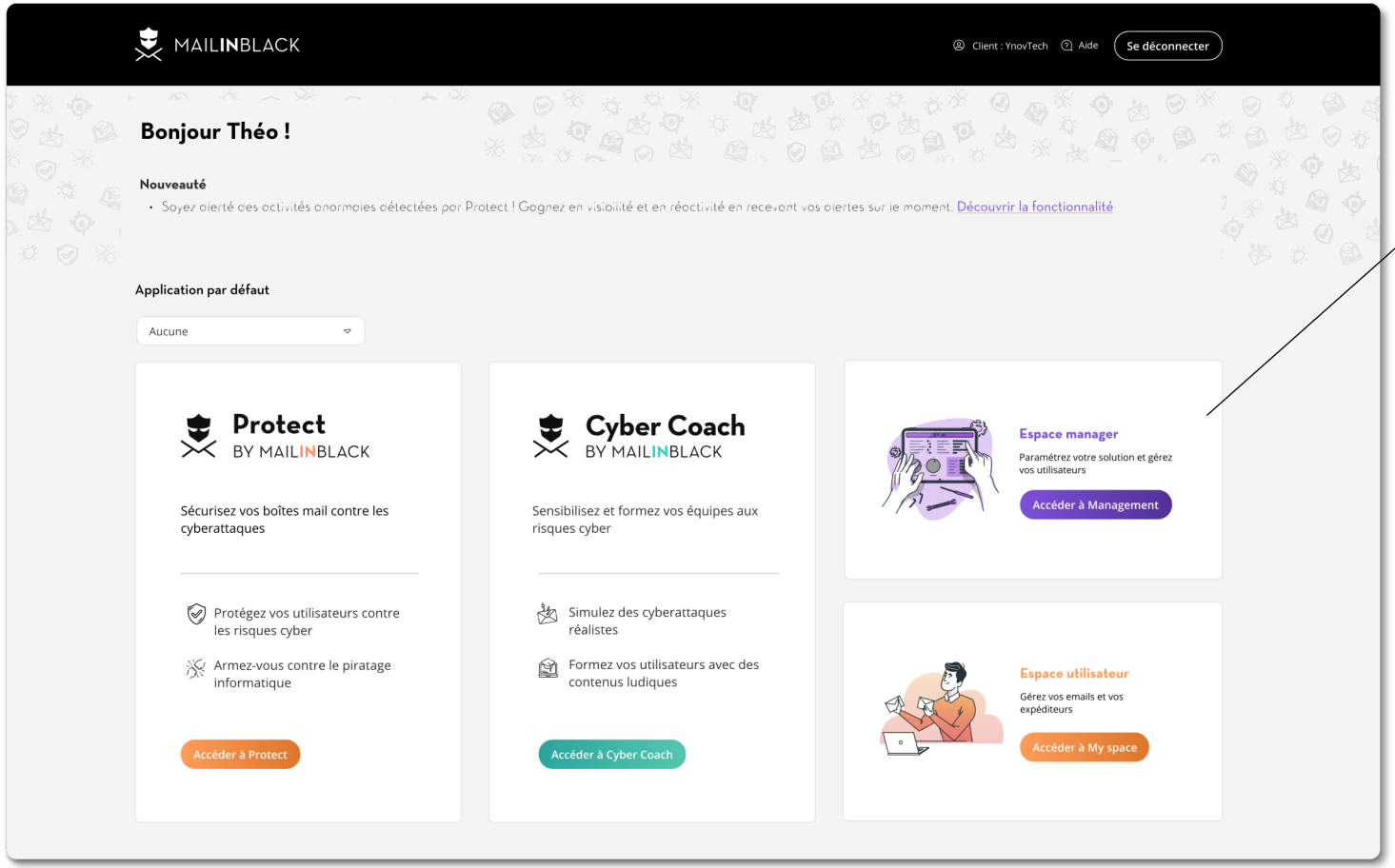
Cyber Coach
BY MAILINBLACK

Sensibilisez et formez les collaborateurs face aux risques cyber

- Audit des vulnérabilités humaines
- Simulations d'attaques réalistes
- Contenus de formation adaptés
- Pilotage de la progression des utilisateurs

Référencées auprès de : UniHA, UGAP, resah Réseau des Acheteurs Hospitaliers, C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière, CNG Groupe Logiciel

Une plateforme de gestion simple et centralisée pour accéder aux solutions et gérer les utilisateurs



Management : votre espace manager

Permet de gérer les éléments communs aux deux solutions Protect et Cyber Coach :

- Gestion des utilisateurs,
- Paramètres, délégations,
- Synchronisation des annuaires,
- Domaines autorisés,
- Contrats
- ...

Les collectivités et établissements de santé nous font confiance

BORDEAUX MÉTROPOLE

Marseille Fos
Le port euroméditerranéen

CHU ROUEN NORMANDIE

Pas-de-Calais habitat

CONSEIL DÉPARTEMENTAL GARD

GHT
Groupement Hospitalier de Territoire
Les Collines de Normandie

LA CANDÉLIE

CREUSOT MONTCEAU COMMUNAUTÉ URBAINE

FRANCE EJS

La messagerie est le vecteur principal d'attaques informatiques

Constat 1 : une augmentation des cyberattaques

90%
des cyberattaques sont véhiculées par email

730
cyberattaques ont visé des établissements de santé en 2021

contre 369 en 2020

+400%
de cyberattaques depuis la crise sanitaire

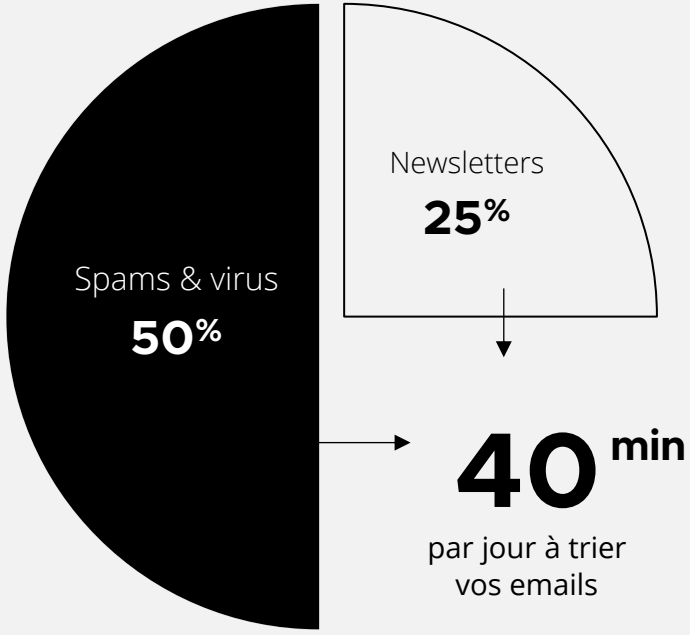
Les types de cyberattaques passant par l'email :

- Phishing (hameçonnage)
- Spearphishing (fraude au président)
- Ransomware

Les diversifications à venir :

- Browser-in-the-browser
- QR code
- ...

Constat 2 : des messageries polluées



Les collectivités, établissements de santé et entreprises au cœur de l'actualité cyber en 2022

Secteur Santé

Août 2022, france info : Essonne, l'hôpital Sud Francilien victime d'une cyberattaque, une rançon de 10 millions de dollars demandée.

Mars 2022, RTL : piratage à l'Assurance maladie, les données de 510 000 français dans la nature.

Janvier 2022, la Nouvelle République : Chambray-lès-Tours, le Pôle de Santé Vinci fortement perturbé par une cyberattaque.

Février 2022, Egora.fr : les cyberattaques contre les hôpitaux ont doublé en 2021.

Secteur Public

Avril 2022, le Figaro : Ardèche, les systèmes informatiques du département paralysés par une cyberattaque.

Mars 2022, Ouest France : Pays d'Ancenis, exposées aux cyberattaques, les collectivités doivent se protéger.

Mars 2022, Sud Ouest : présidentielle 2022, face au risque de cyberattaque, « la plus grande prudence » est de mise.

Mars 2022, La Dépêche : Toulouse, l'ENAC victime d'une inquiétante cyberattaque avec demande de rançon.

Secteur Privé

Août 2022, 20 min : les serveurs de l'enseigne de vêtements visés par une cyberattaque.

Mars 2022, Siècle Digital : le français Ubisoft victime d'une cyberattaque.

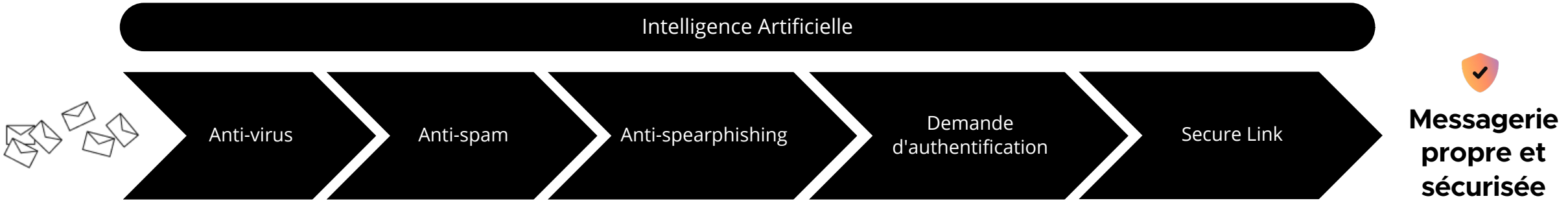
Mars 2022, le Figaro : un groupe de hackers vole des fichiers confidentiels appartenant à Samsung.

Avril 2022, le Parisien : cybersécurité des PME, les portes d'entrée préférées des cyberpirates.

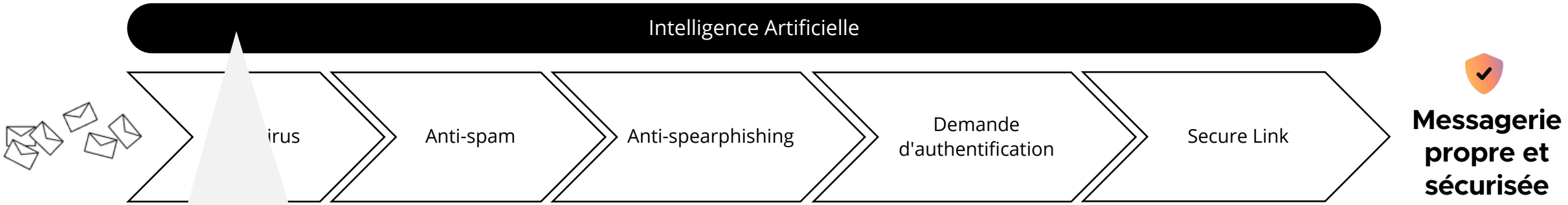
Protect, la solution du marché de la protection des emails :

- la plus simple
- la plus performante
- la plus accessible

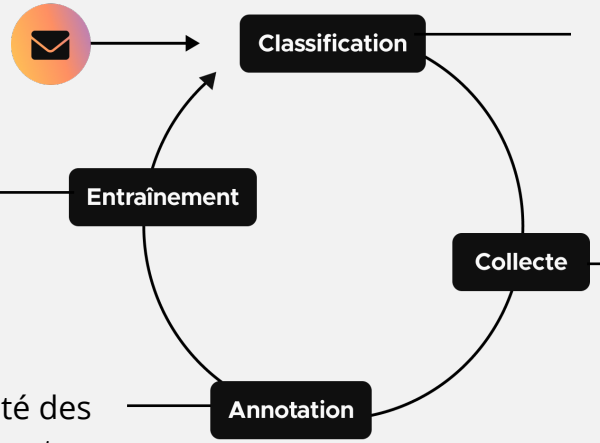
Fonctionnement de notre technologie :



Découvrez en **en vidéo** notre solution :



Notre IA intervient à plusieurs étapes pour assurer plus de sécurité et de confort :

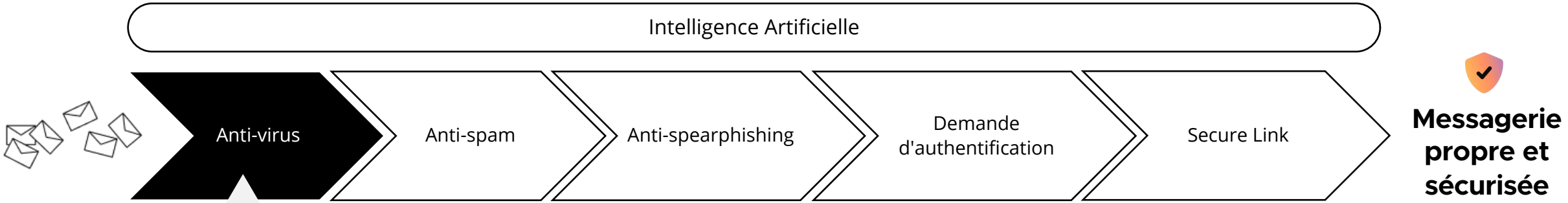


L'IA **entraîne** une nouvelle version du modèle de classification à l'aide des données fraîchement collectées.

Le Lab IA **intervient** pour évaluer la qualité des clusters avant de les labelliser manuellement.

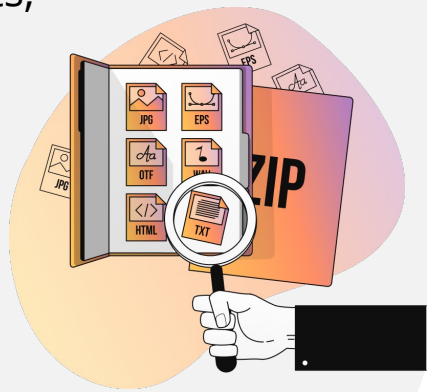
L'IA **analyse** les emails et prédit leur catégorie (spam, scam, publicité, newsletter, social network, notification, légitime).

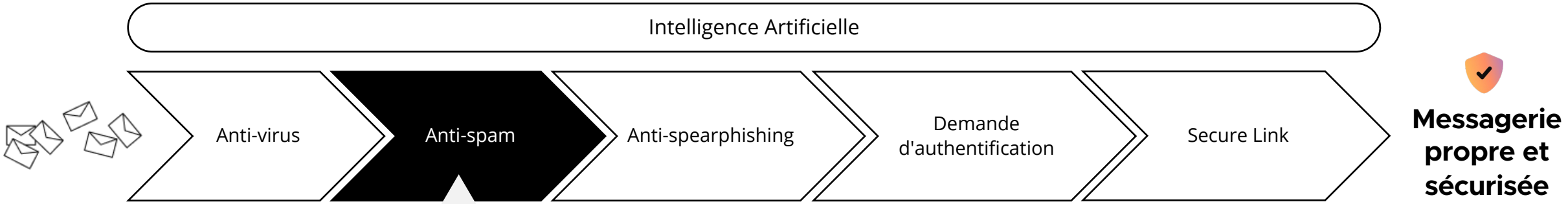
L'IA **regroupe** les emails similaires en clusters afin de détecter les nouvelles vagues de menaces.



Contrôle antiviral : les emails et les pièces jointes contiennent-elles une signature virale ?

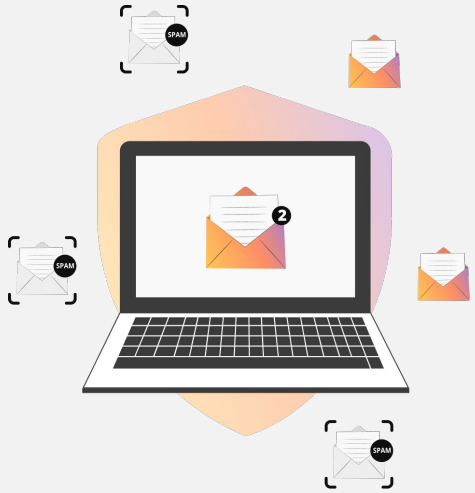
- Scan des documents Office (docx, xlsx, ppt), HTML et PDF pour détecter des liens malveillants, des macros ou du code suspect
- Analyse des exécutables (type ELF, PE...) et des scripts
- Blocage de certaines extensions connues pour contenir des malwares (.exe, .js, .docxm...)
- Décompression puis analyse des archives (zip, rar, 7zip, tar...)
- 1er niveau d'analyse des liens présents dans le texte et l'HTML

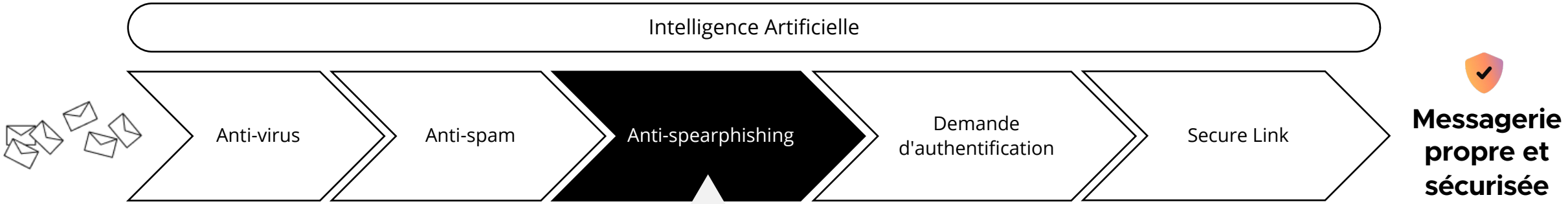




Contrôle anti-spam : cet email est-il envoyé par une personne légitime ?

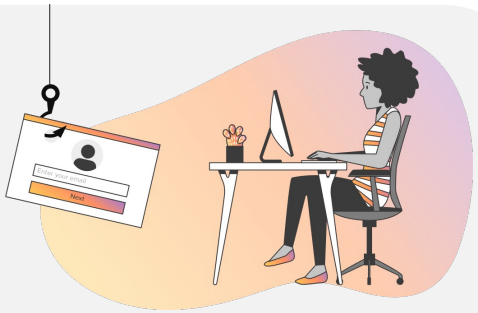
- Vérification de l’existence du domaine de l’expéditeur (**Reverse DNS**)
- Vérification de l’existence de l'utilisateur (**filtrage strict**)
- Contrôle de réputation de l’IP émettrice (**RBL**)
- Vérification de l’IP émettrice - droit d’envoyer un email avec ce domaine (**SPF**)
- Analyse des emails NDR (**Non-Delivery Reports**)
- Filtrage par objet de l’email

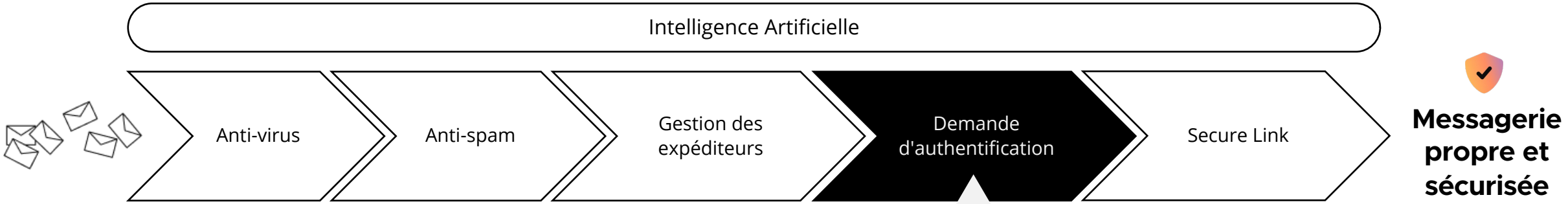




Contrôle anti-spearphishing : l'identité de vos collaborateurs a-t-elle été usurpée ?

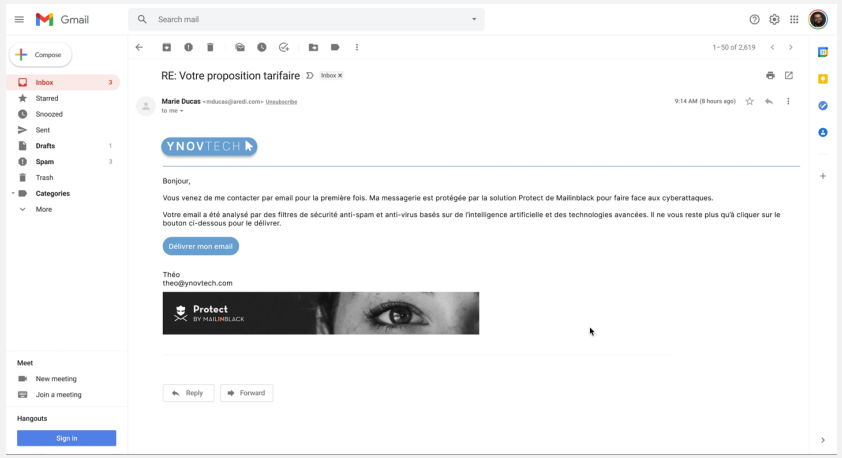
- Analyse heuristique sur les informations de l'expéditeur (nom d'affichage, alias, comparaison adresse en-tête vs adresse enveloppe, typosquatting)
- Analyse de l'authenticité et du contenu de l'email grâce à notre IA (données sensibles, sémantiques d'urgences...)



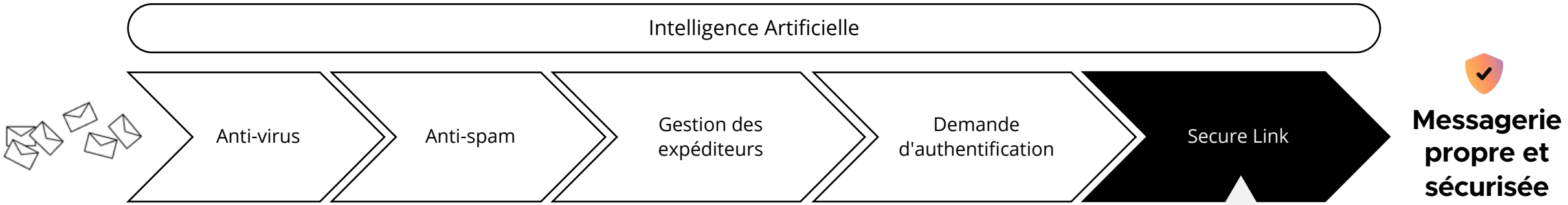


La demande d'authentification, votre plus haut niveau de confort :

- Captcha 100% personnalisable à votre entreprise
- Limite les interruptions de travail
- Aide à valoriser son image
- Instaure un climat de confiance

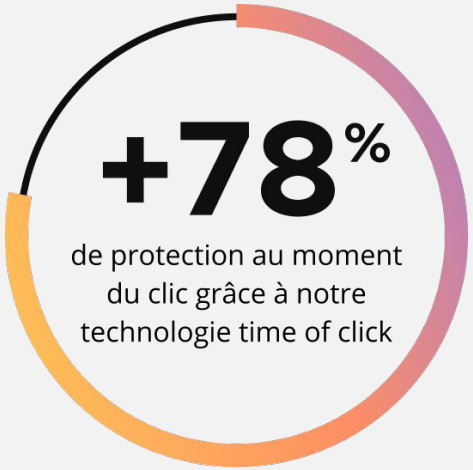


1. Chaque **nouveau correspondant** reçoit une demande d'authentification
2. Le correspondant répond correctement pour s'authentifier : il rejoint alors la **liste blanche** du destinataire
3. Un message lui **confirme** que son email a bien été délivré au destinataire



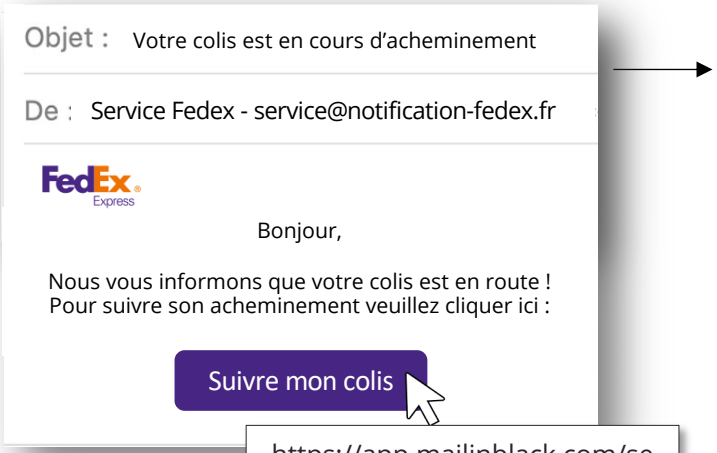
Secure Link, notre modèle d'IA de Deep Learning pour analyser les liens :

- Technologie propriétaire de Mailinblack
- Au moment du clic, analyse les liens contenus dans les emails : si le lien s'avère dangereux à un moment donné, alors l'IA permet de le sécuriser au moment du clic
- Vérification à travers une triple analyse
- Avertissement de l'utilisateur sur le danger de l'extension grâce à une page dédiée



Secure Link : ce que voit l'utilisateur

Lorsque le lien est considéré comme légitime mais qu'il contient une extension dangereuse de fichier, alors l'utilisateur est averti

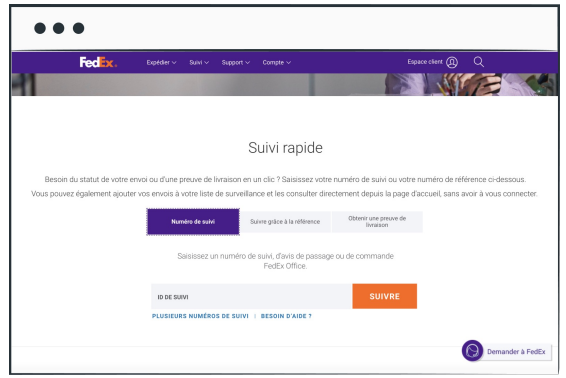


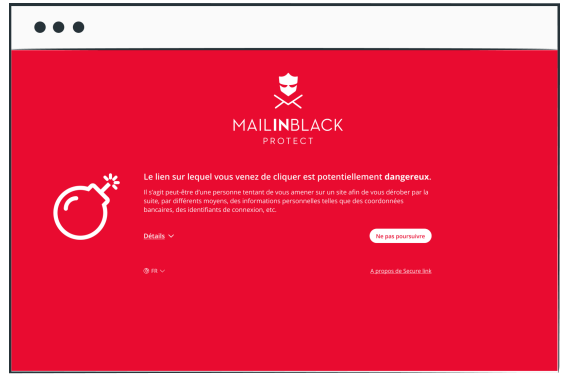
https://app.mailinblack.com/securelink/?url=https://fedex.com&key=ML09KMLPOLLO879....

1. Check du **hostname**
2. Protocole pour **vérification** du lien

Lien bienveillant :

l'utilisateur est redirigé vers le site souhaité



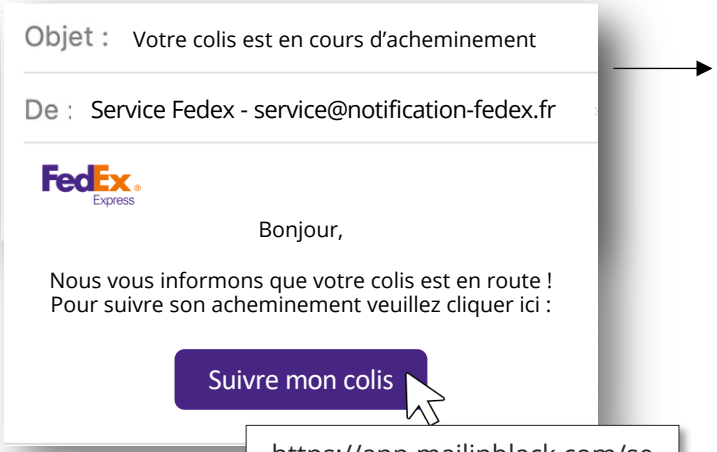


Lien malveillant :

l'utilisateur est averti du danger grâce à une page dédiée

Secure Link : ce qui se cache derrière la technologie

Lorsque le lien est considéré comme légitime mais qu'il contient une extension dangereuse de fichier, alors l'utilisateur est averti



https://app.mailinblack.com/securelink/?url=https://fedex.com&key=ML09KMLPOLLO879....

1. Check du **hostname**
2. Protocole pour **vérification** du lien

Consultation des bases de données

1. Vérification de la **provenance du mail**
2. Test du lien sur nos **bases de données** (partenaires, API, bases de données)

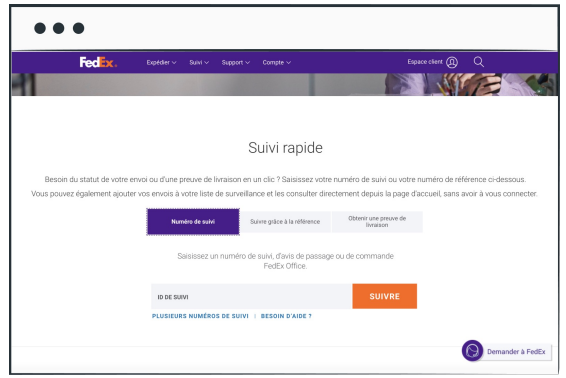
Intervention de l'IA Secure Link

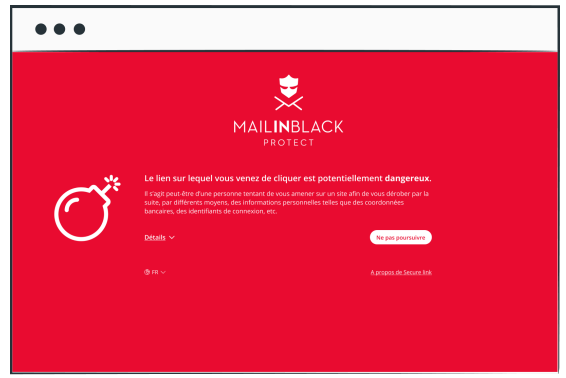
Analyse :

1. **Morphologique** du lien
2. **Sémantique** du lien
3. **Contenu** la page

Lien bienveillant :

l'utilisateur est redirigé vers le site souhaité





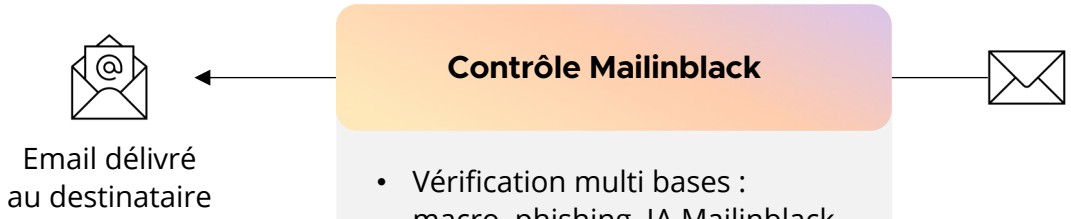
Lien malveillant :

l'utilisateur est averti du danger grâce à une page dédiée

L'option Protect Out

Elle permet de sécuriser **tous les messages envoyés**

Simplicité | Efficacité | Sécurité

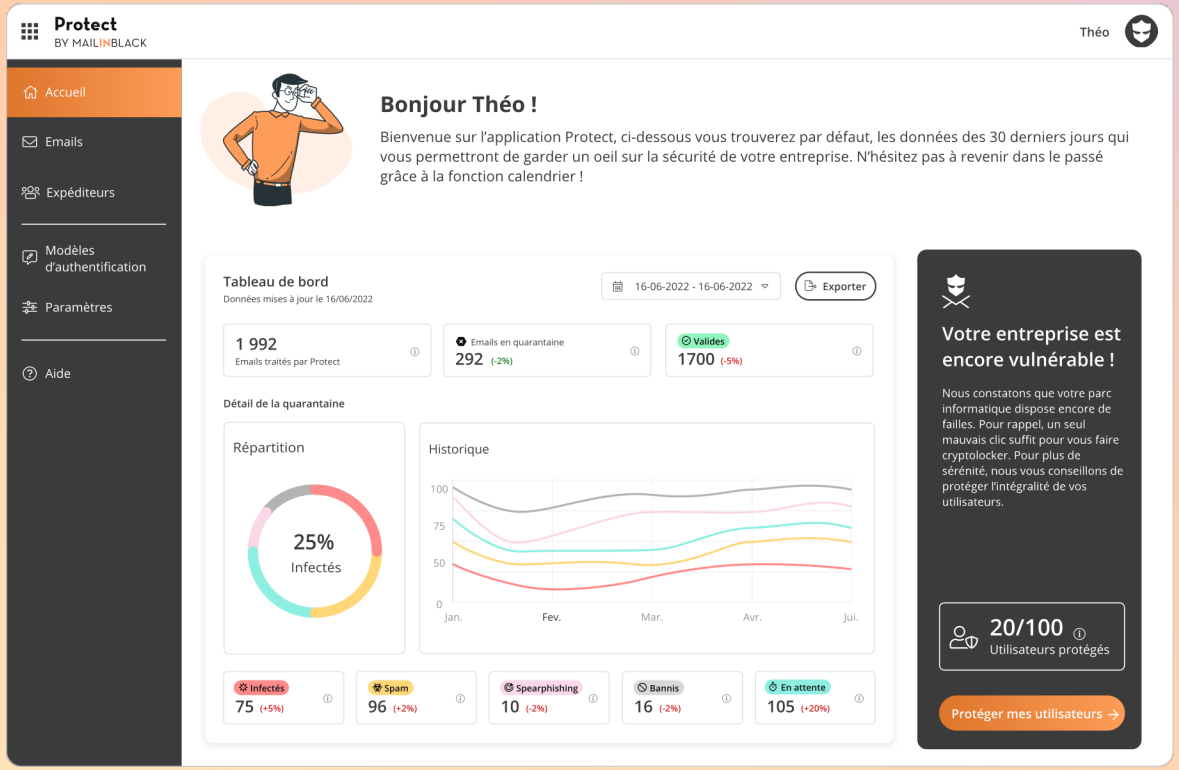


1. Les destinataires sont automatiquement ajoutés à la **liste blanche**
2. Les adresses IP d'envoi ne sont pas **blacklistées**
3. Un **scan antiviral** est réalisé sur tous vos emails envoyés
4. L'administrateur est **alerté** et les envois frauduleux sont **bloqués**

Les bénéfices pour votre entreprise ...

Sécurité

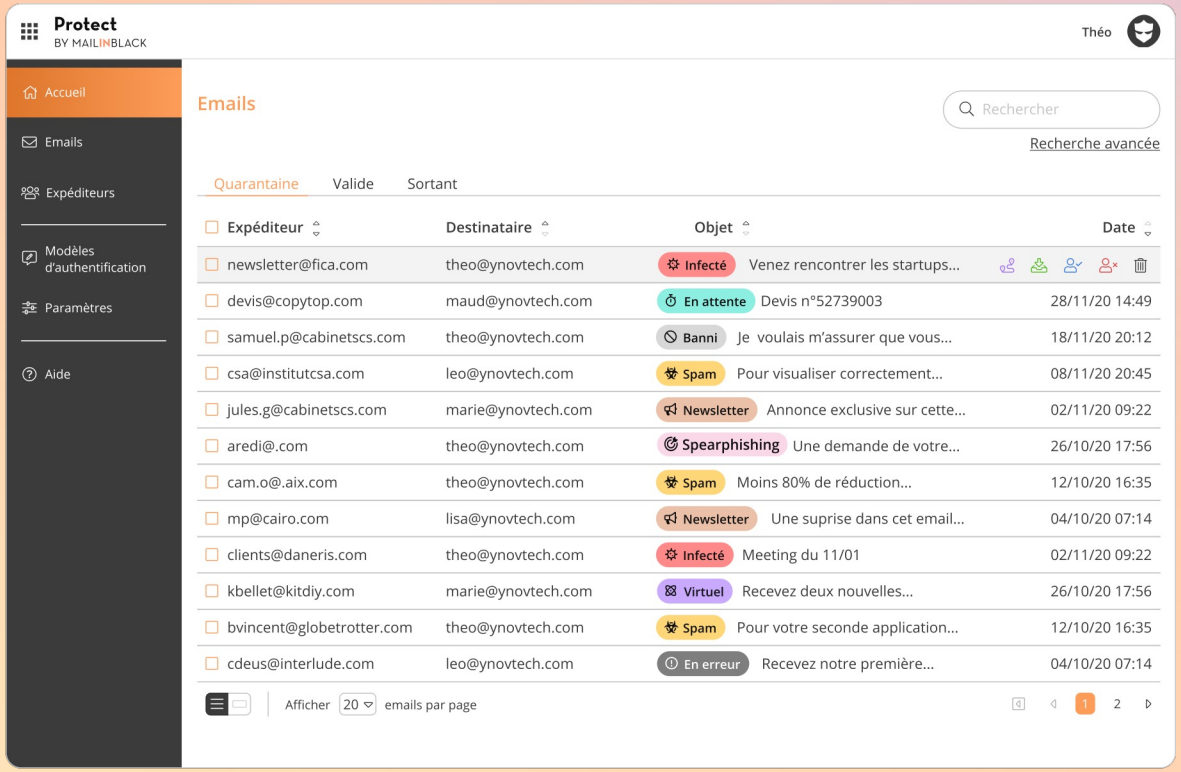
- **Sécurisation maximale** des données et des échanges par email
- **Protection des infections de votre système d'information** : blocage des virus, traitement des spams et usurpations, scan des pièces-jointes
- Limite le **risque d'erreur humaine**
- **Gestion centralisée** des paramètres de sécurité



… grâce à un contrôle de l’administrateur

Interface web dédiée

- Aperçu des **statistiques** de sécurité
- Gestion des **emails**
- Gestion des **expéditeurs**
- **Profil** de l’entreprise
- Gestion des **domaines**, des **utilisateurs**, des **délégations** et des **licences**
- Gestion de la **demande d’authentification**
- **Synchronisation** d’annuaires
- **Alerting** des activités anormales détectées

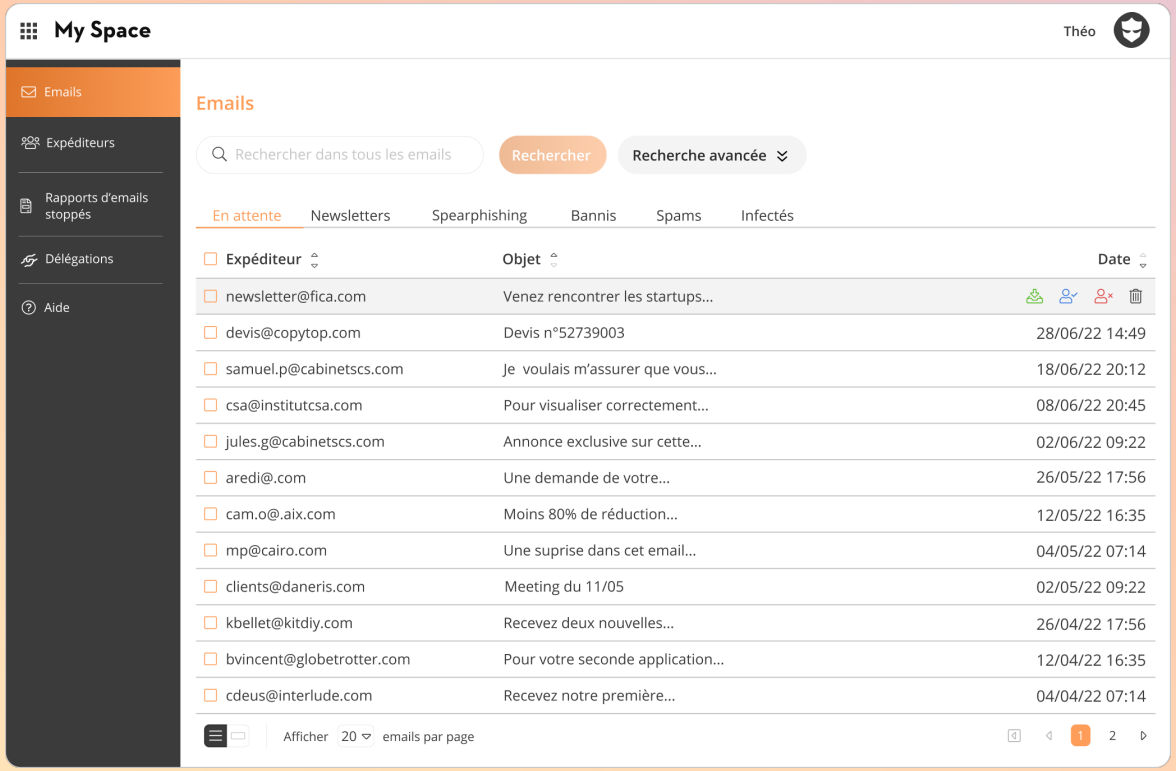


Les bénéfices pour vos collaborateurs ...

Interface web personnelle My Space

Sérénité Confort

- Gain de **productivité** avec une messagerie propre
- Gain de **temps** grâce au tri automatique des emails, spams et newsletters
- **Moins de stress** lié à la surcharge d'emails indésirables
- **Facilité d'utilisation** et **gestion individuelle** des préférences de sécurité
- **Soulagement** face aux risques d'attaques et sensibilisation aux pratiques de sécurité



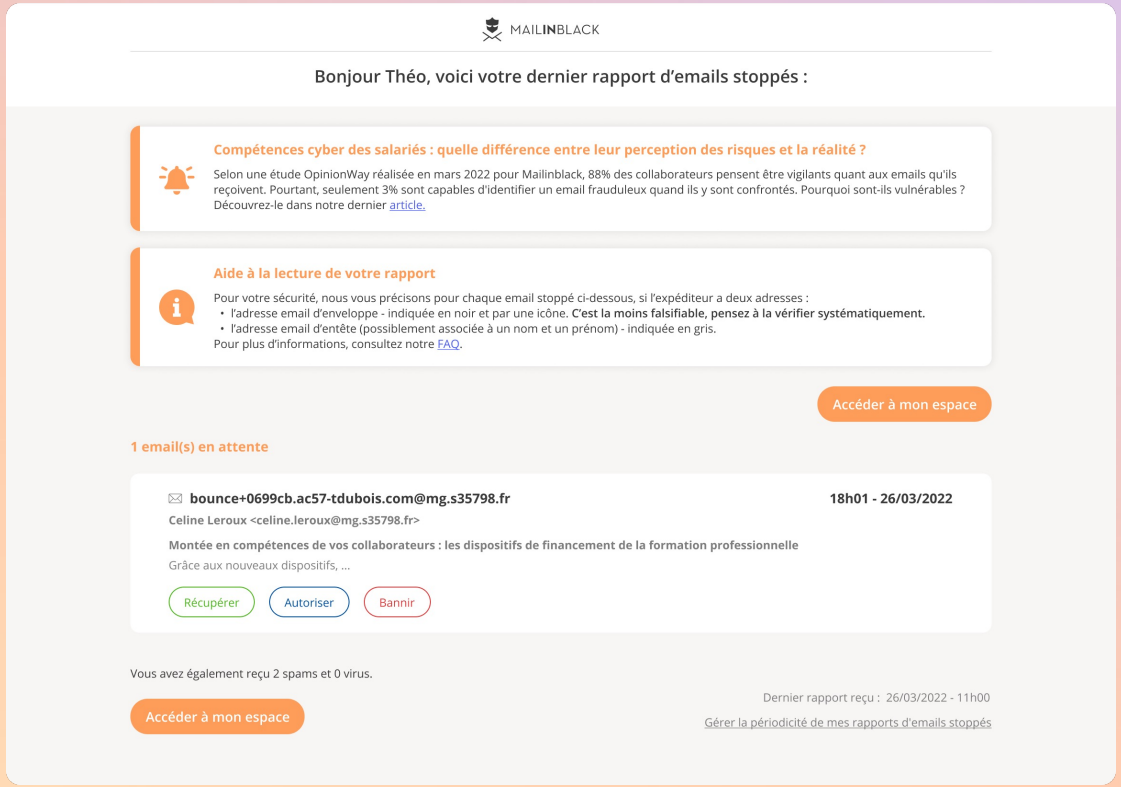
.. autonomes et impliqués

- **Gestion des emails stoppés**
  En attente, newsletters, bannis, spams, infectés, spearphishings

- **Gestion des expéditeurs**
  Expéditeurs autorisés et bannis

- **Edition du compte utilisateur**
  Langue de l'interface, fréquence du rapport, MDP, délégation

- **Rapport d'emails stoppés**
  Emails en attente, possibilité d'ajouter les newsletters, les spearphishings et gestion de la fréquence de réception



Une activation du service adaptée à votre infrastructure

100% compatible avec votre messagerie

Office 365 · 1&1 IONOS · G Suite · OVH.com · Exchange

activation
CLOUD

Datacenter sécurisé en France (RGPD)
Supervision 24/7 & redondance des serveurs
Aucune installation requise

installation
ON-PREMISE

Respect de votre politique d'hébergement
100% adaptée à votre infrastructure
Installation simplifiée

Une équipe qui vous accompagne tout au long de votre parcours

Nos programmes vous permettent de maximiser la sécurité et la satisfaction de vos collaborateurs

- 200 licences

Mise à disposition de plusieurs aides :

- ✓ Onboarding pour accompagnement ou réalisation de l'installation
- ✓ Proposition de formation à la solution

+ 200 licences

Suivi personnalisé par un Customer Success Manager (CSM) dédié :

- ✓ Réponse à vos questions
- ✓ Équipe à votre disposition durant la période d'installation
- ✓ Proposition de formation à la solution
- ✓ Comité de pilotage trimestriel
- ✓ Présentation des nouveautés

Notre Service Client est disponible du lundi au vendredi de 8h à 18h

Chat ✓ Email ✓ Téléphone ✓

MAILINBLACK

CONTACTEZ-NOUS

contact@mailinblack.com

+33 (0)4 88 60 07 80

www.mailinblack.com

Conduite du projet – SaaS

Set up préparatoire	On-boarding	Installation, pilote , changement	Finalisation
• Présentation du Success Program • Définir le planning de déploiement • Programmer les formations • Aligner les attendus et les prochaines étapes	• Déclaration des NDD et Serveurs Messagerie • Synchronisation des utilisateurs • Personnalisation	• Lien On-Boarding terminé • Réception des accès manager • Redirection des champs MX <u>Protect Out</u> • Enrichissement automatique des listes d'expéditeurs • Déploiement progressif des protections <u>Conduite du changement</u> • Information et présentation • Découverte de l'interface par l'utilisateur • Formations	• Suivi Post Installation • CSM dédié • Escalade support
30 minutes	1 heure	2-4 semaines	CoPil trimestriel

Conduite du projet – On Premise

Set up préparatoire	On-boarding	Installation, pilote , changement	Finalisation
• Présentation du Success Program • Définir le planning de déploiement • Programmer les formations • Aligner les attendus et les prochaines étapes	• Réception de l'image disque • Création de la machine • Ouverture des ports nécessaires	• Installation et formation avec chargé de production • Redirection des champs MX <u>Protect Out</u> • Enrichissement automatique des listes d'expéditeurs • Déploiement progressif des protections <u>Conduite du changement</u> • Information et présentation • Découverte de l'interface par l'utilisateur • Formations	• Suivi Post Installation • CSM dédié • Escalade support
30 minutes	1 heure	2-4 semaines	CoPil trimestriel

CHU de Martinique

« Protect nous apporte une réelle sécurité supplémentaire. Les dernières attaques visant l'hôpital ont été stoppées et mises en quarantaine par Mailinblack et la boîte mail du personnel est désormais triée et propre. Un vrai gain de temps au quotidien ! La confiance que nous avons dans la solution nous permet de travailler plus sereinement tout en assurant une surveillance permanente de notre système informatique. »

M. Gérald Galim - RSSI

Marseille Fos
Le port euroméditerranéen

« Nous avons constaté de réels bénéfices et une adhésion massive de nos collaborateurs et de nos correspondants. Mailinblack propose une offre simple et intuitive qui nous permet, grâce à une authentification des expéditeurs, de nous prémunir de grands volumes de spams et de travailler en toute sécurité."

M. COLONNA - Chargé de l’exploitation de Mailinblack