

Sécurisez vos messageries professionnelles contre les cyberattaques



- 01 **À propos de MIB**
- 02 **Cyberattaques : état des lieux**
- 03 **La solution Protect**
- 04 **Notre accompagnement**





Qui sont-ils ?



20 ^{ans} 
d'expertise en
cybersécurité

14 ^{mille}
organisations
protégées

96 %
des clients
renouvellent

+1 ^{milliard}
d'emails bloqués
chaque année

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



Sécurisez les messageries professionnelles contre les cyberattaques

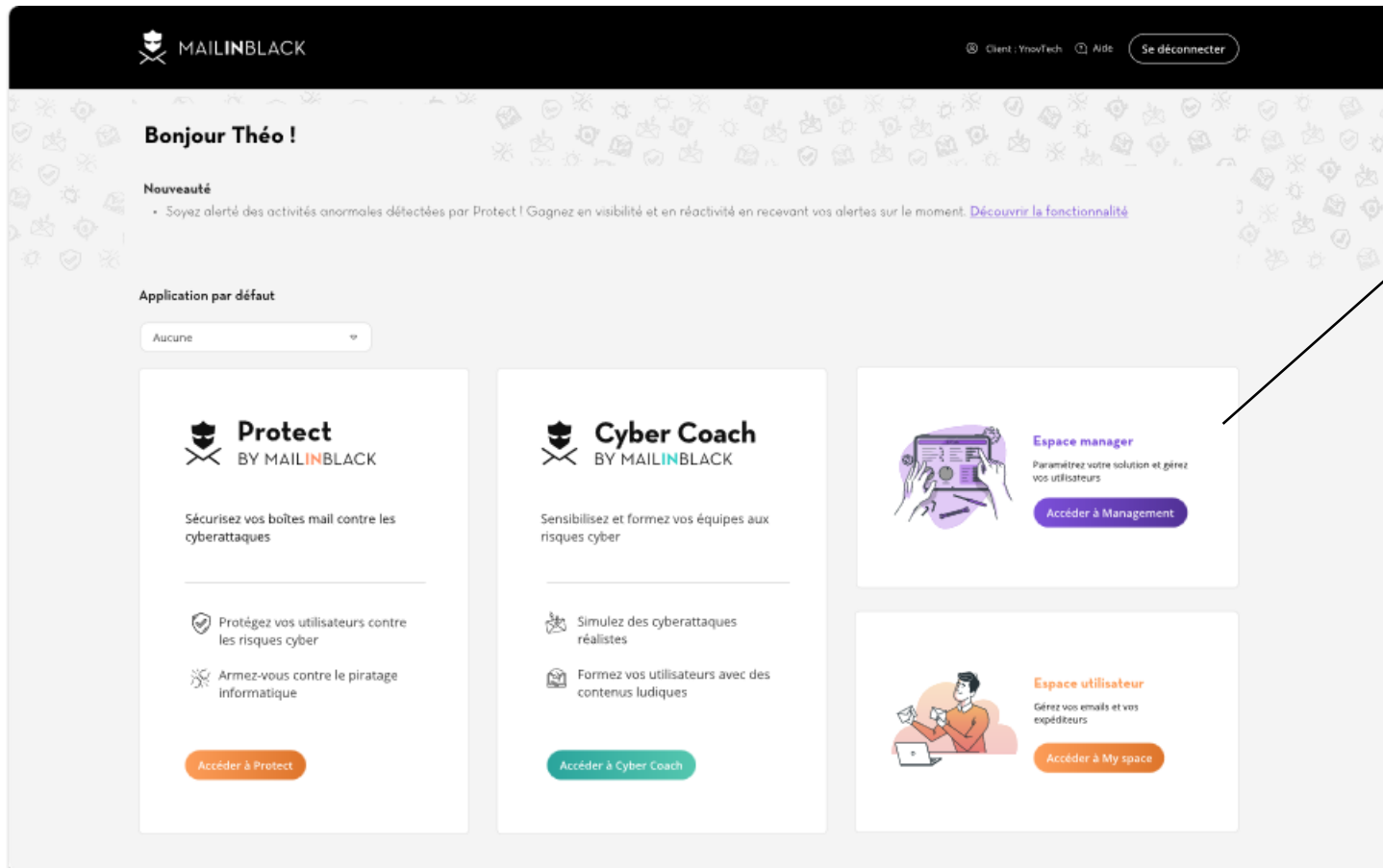
- ✓ Anti : virus, phishing, spearphishing, spam, ransomware
- 🧠 Technologies propriétaires couplées à de l'IA
- 🔗 Analyse des liens dans les emails (Secure Link)
- ✉️ Messagerie propre et sécurisée



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

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



Management :
un 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 leur font confiance



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

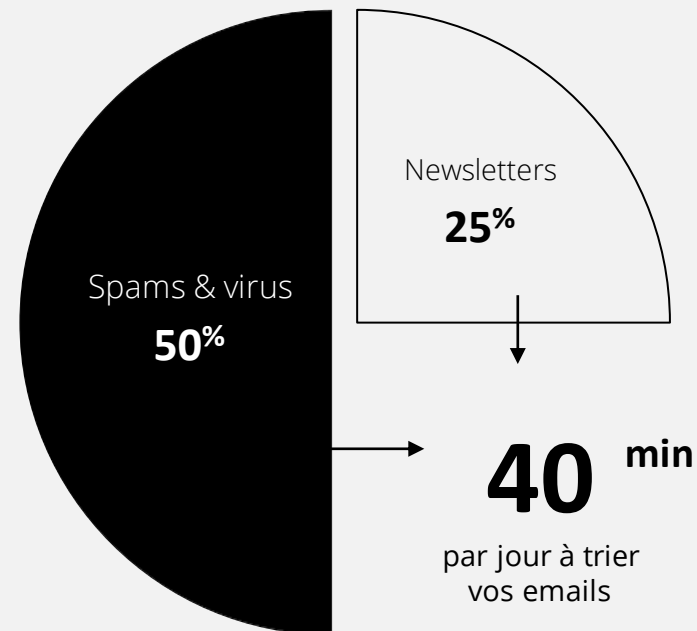
Les types de cyberattaques passant par l'email :

- 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.

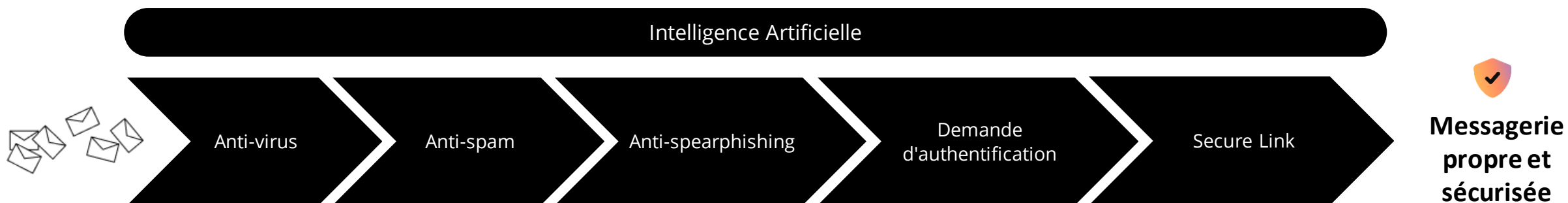
Protect, la solution du marché de la protection des emails :

la plus simple ✓

la plus performante ✓

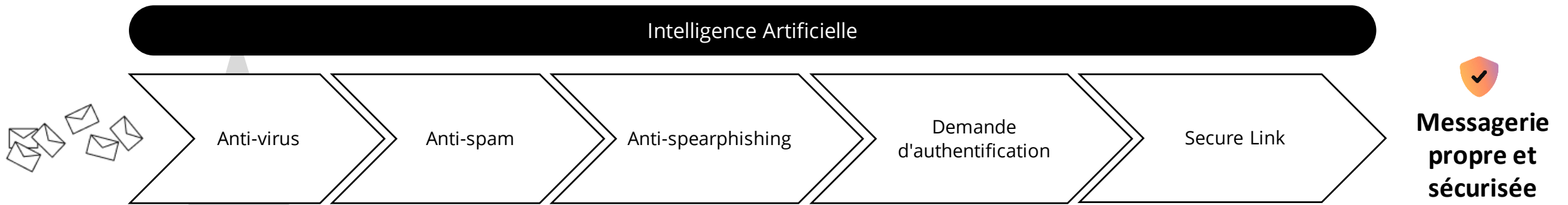
la plus accessible ✓

Fonctionnement de la technologie :

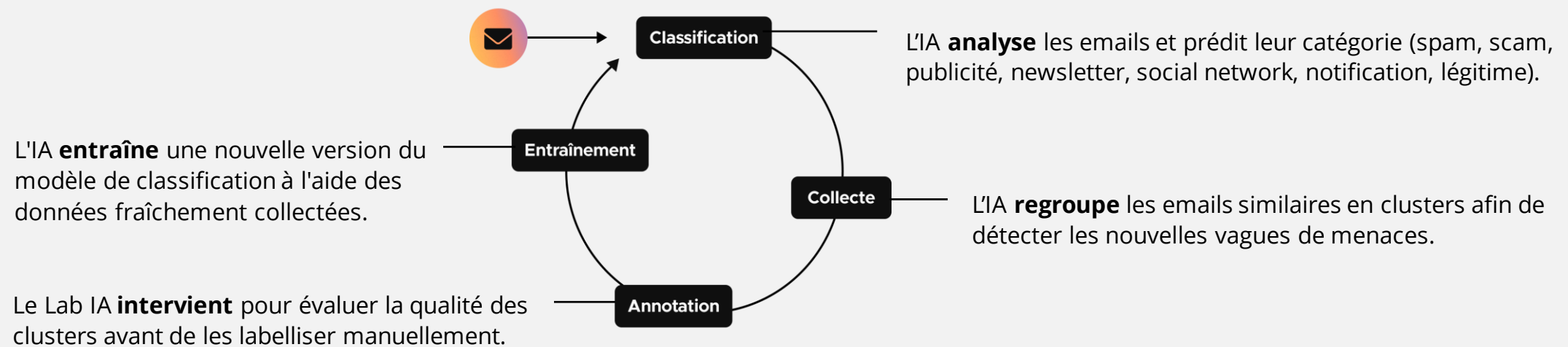


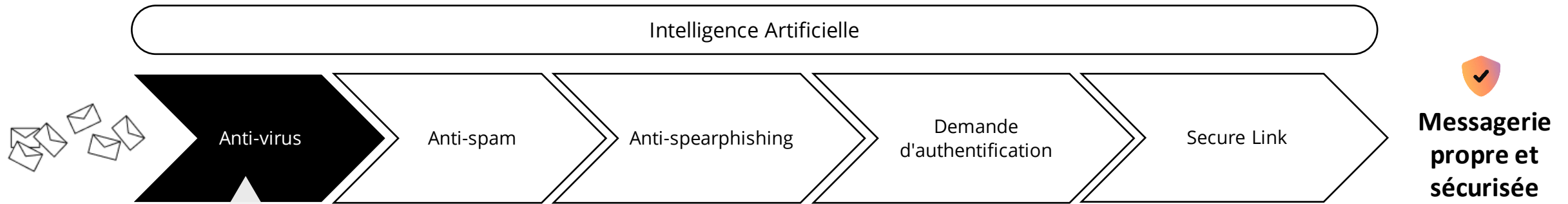
Découvrez en
en vidéo la
solution :





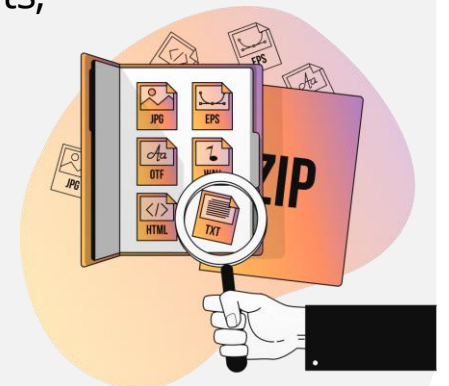
Notre IA intervient à plusieurs étapes pour assurer plus de sécurité et de confort :

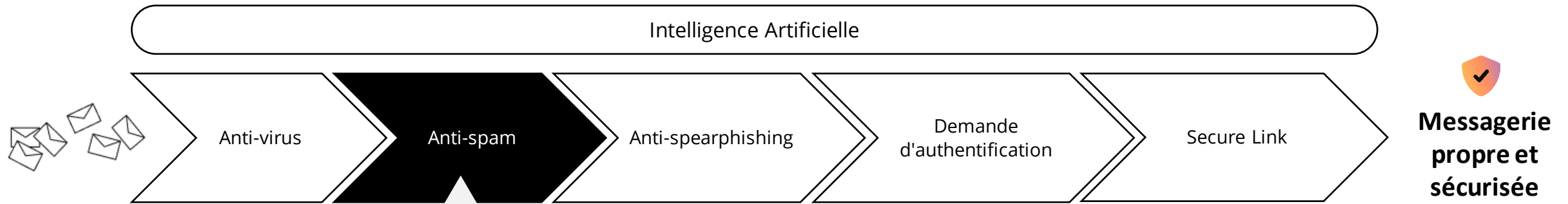




Contrôle antiviral : les emails et les pièces jointes contiennent-elles une signature virale ?

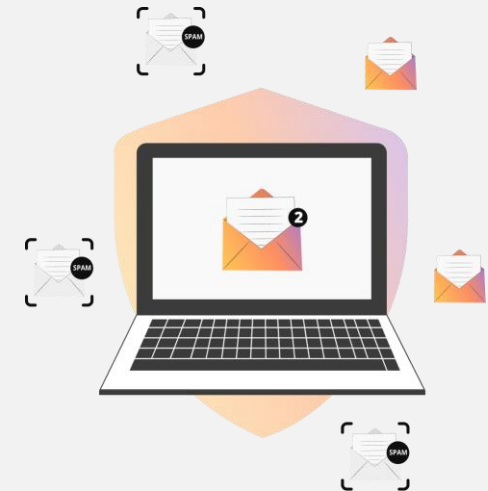
- Scan des documents Office (docx, xlsx, ppt), HTML et PDF pour détecter des liens malveillants, des macros ou du code suspect
- Analyse des exécutables (type ELF, PE...) et des scripts
- Blocage de certaines extensions connues pour contenir des malwares (.exe, .js, .docxm...)
- Décompression puis analyse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

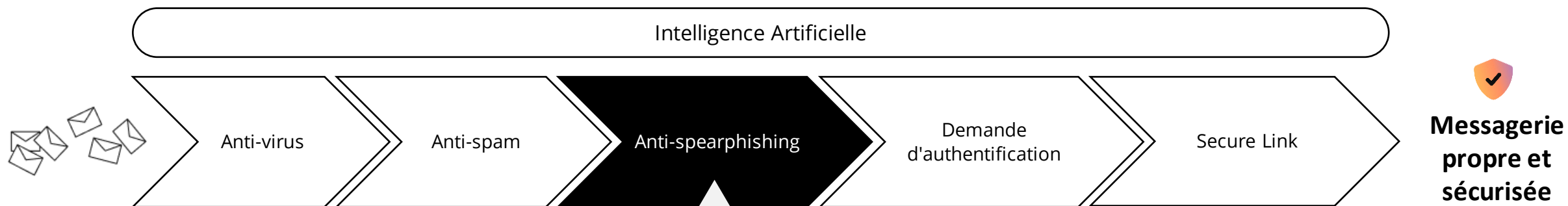




Contrôle anti-spam : cet email est-il envoyé par une personne légitime ?

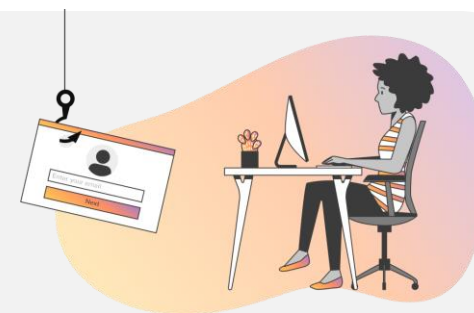
- Vérification de l'existence du domaine de l'expéditeur (**Reverse DNS**)
- Vérification de l'existence de l'utilisateur (**filtrage strict**)
- Contrôle de réputation de l'IP émettrice (**RBL**)
- Vérification de l'IP émettrice - droit d'envoyer un email avec ce domaine (**SPF**)
- Analyse des emails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



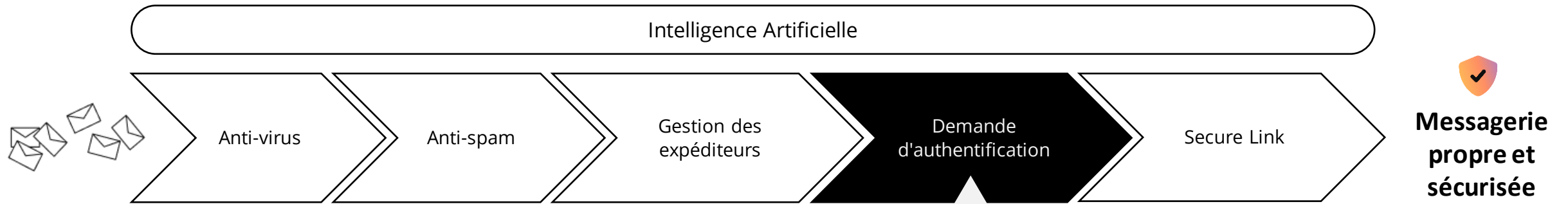


Contrôle anti-spearphishing: l'identité de vos collaborateurs a-t-elle été usurpée ?

- 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...)

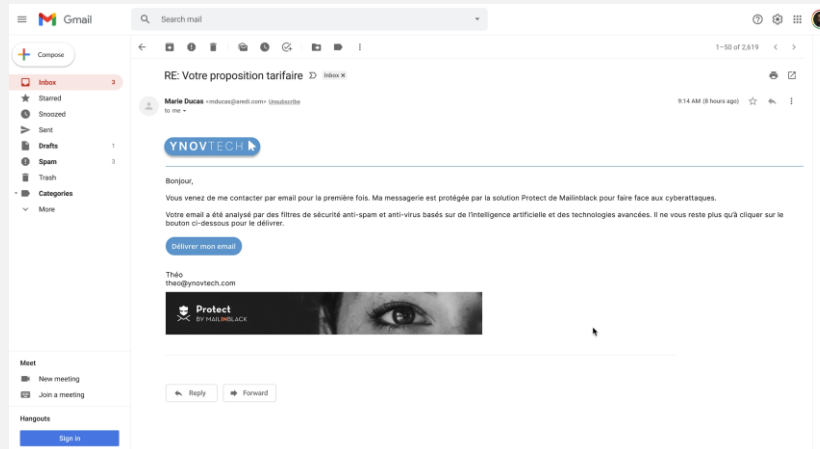


03 La solution Protect

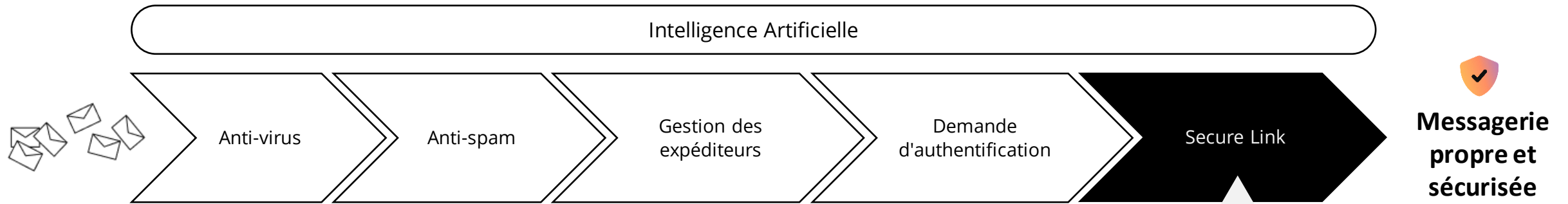


La demande d'authentification, votre plus haut niveau de confort :

- 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



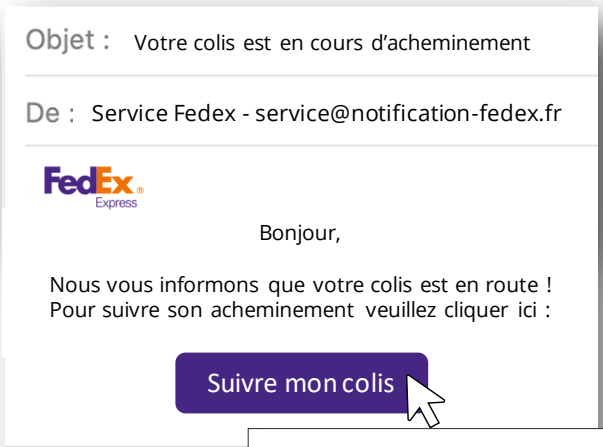
Secure Link, notre modèle d'IA de Deep Learning pour analyser les liens :

- 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

+78%

de protection au moment
du clic grâce à notre
technologie time of click

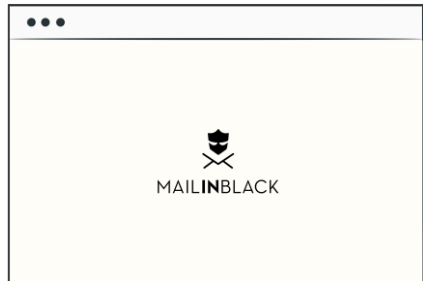
Secure Link : ce que voit l'utilisateur



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

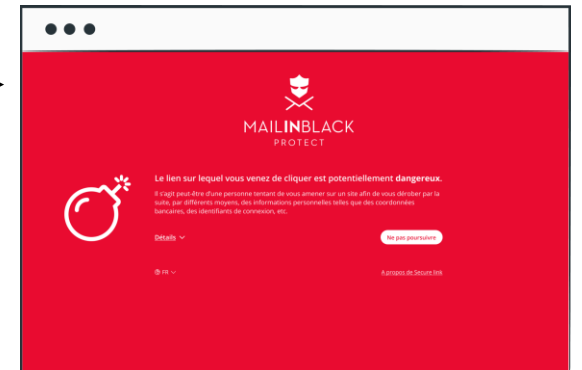
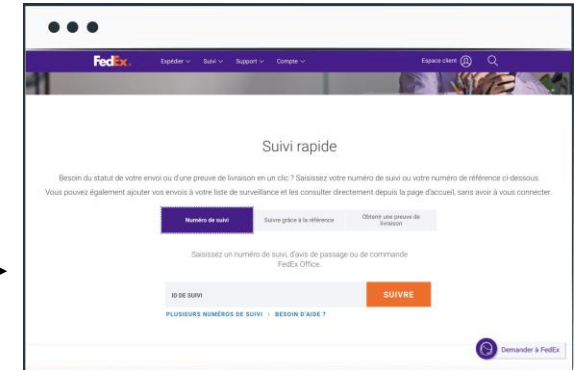
1. Check du **hostname**
2. Protocole pour **vérification** du lien

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



Lien bienveillant :

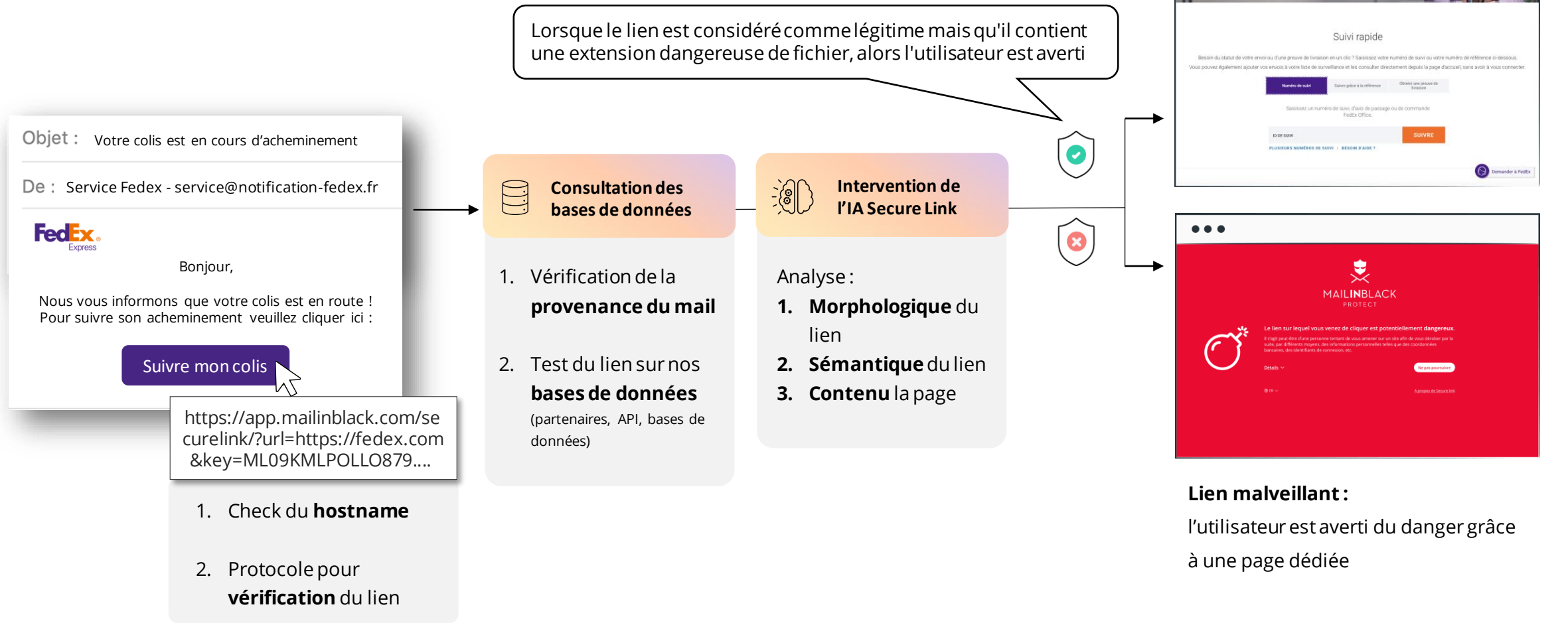
l'utilisateur est redirigé vers le site souhaité



Lien malveillant :

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

Secure Link : ce qui se cache derrière la technologie



L'option Protect Out

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

Simplicité

Efficacité

Sécurité



Contrôle Mailinblack

Email délivré
au destinataire

- Vérification multi bases : macro, phishing, IA Mailinblack
- Vérification des PJ : contrôle des extensions
- Détection des comportements anormaux (envois massifs)

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

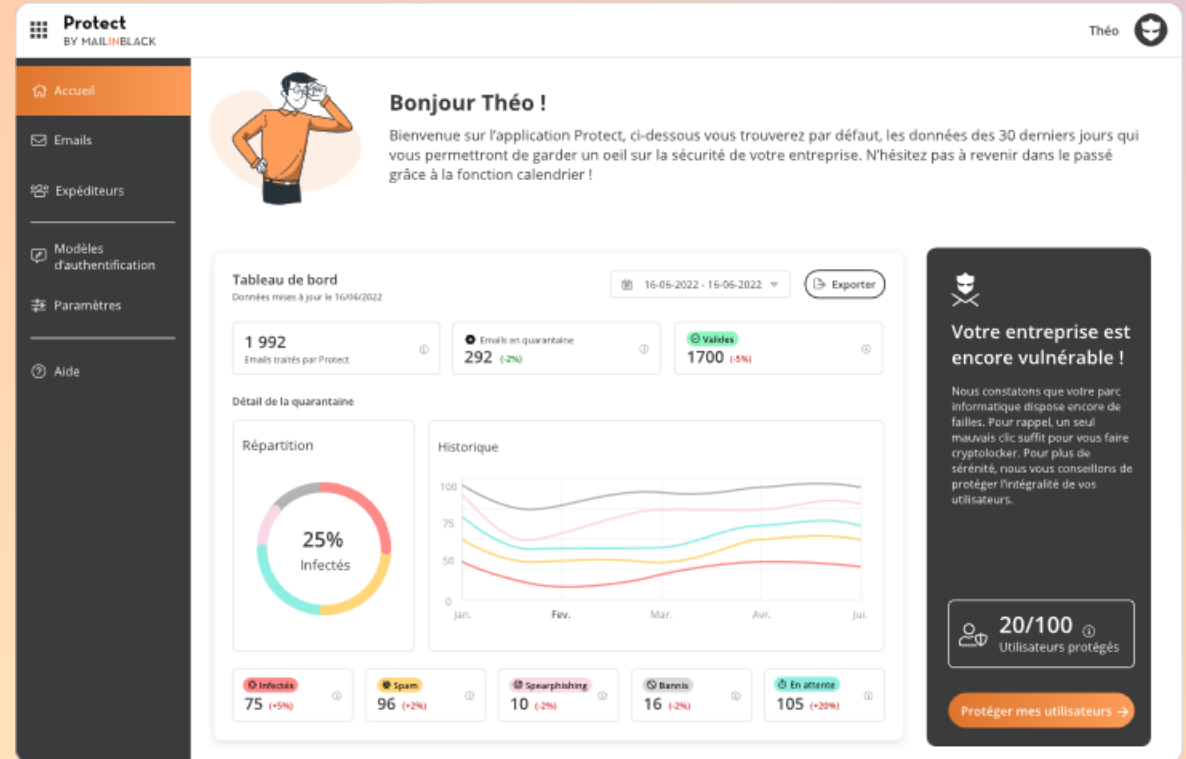
L'administrateur est **alerté** et les envois frauduleux sont **bloqués**



Les bénéfices pour votre structure ...

Sécurité

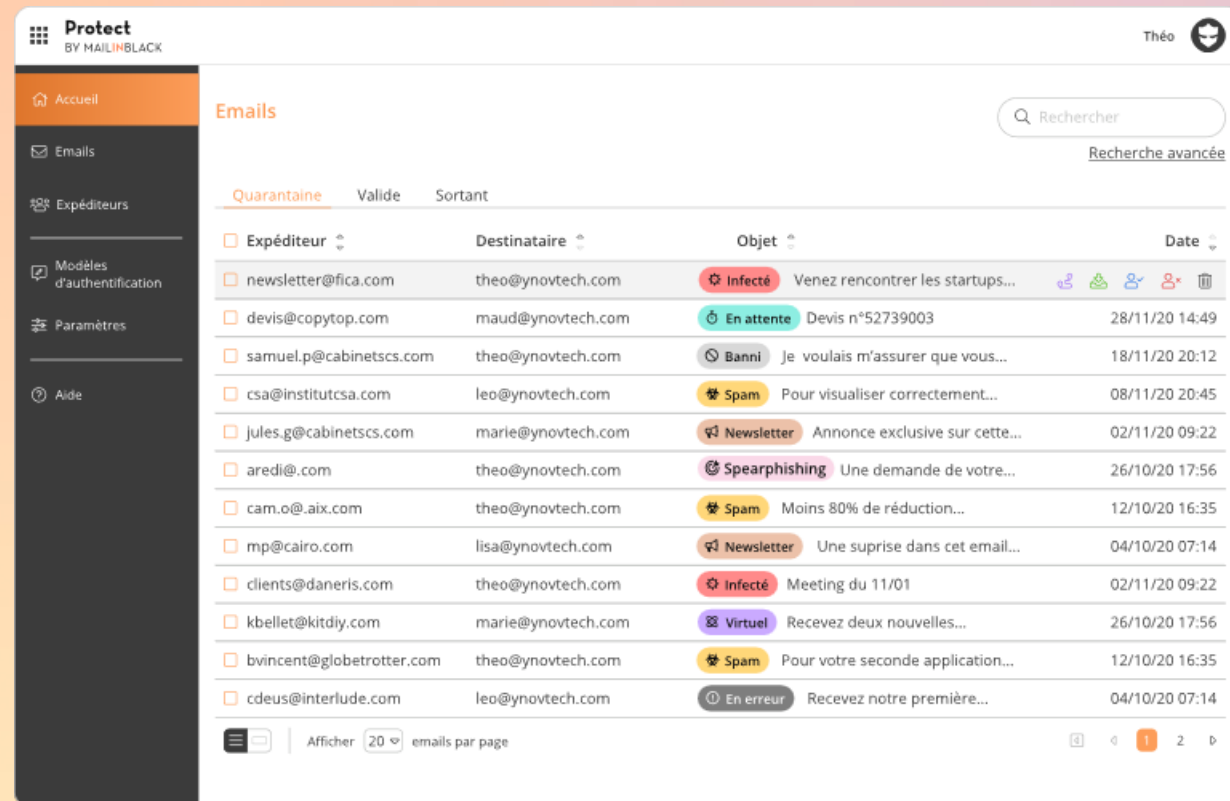
- **Sécurisation maximale** des données et des échanges par email
- **Protection des infections de votre système d'information** : blocage des virus, traitement des spams et usurpations, scan des pièces-jointes
- Limite le **risque d'erreur humaine**
- **Gestion centralisée** des paramètres de sécurité



... 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



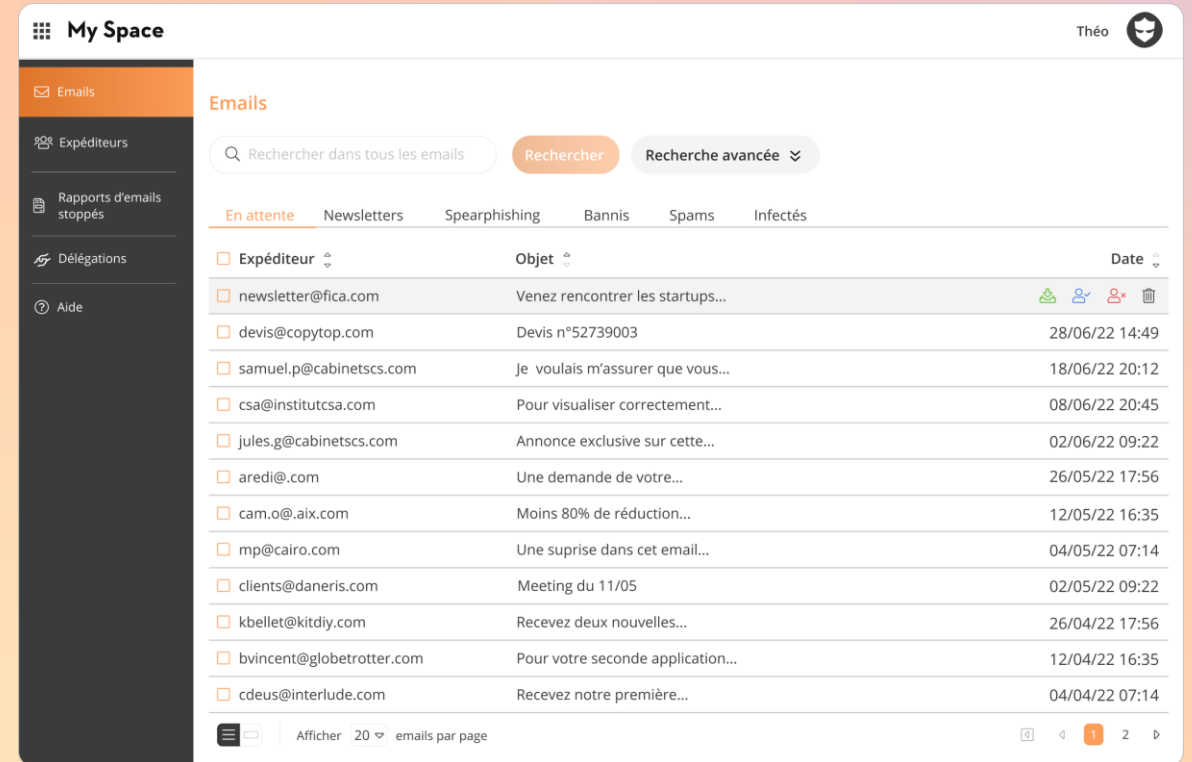
Les bénéfices pour vos collaborateurs ...

Interface web personnelle My Space

Sérénité

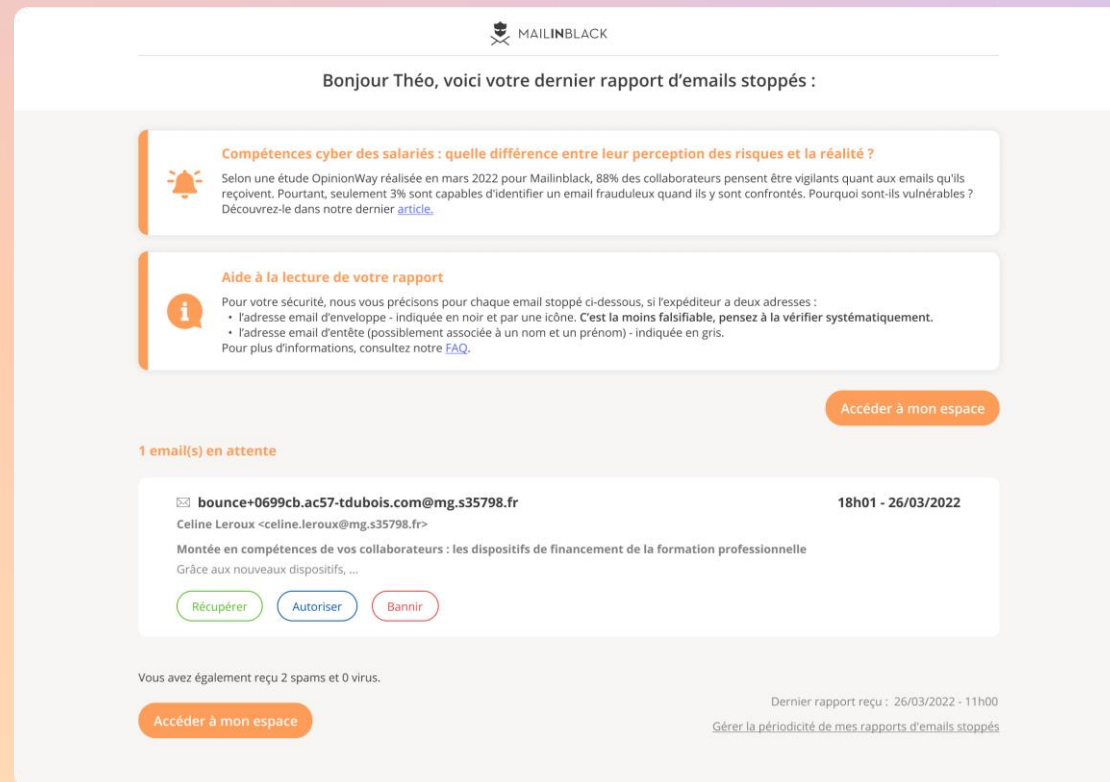
Confort

- 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, spearfishings
- **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 spearfishings et gestion de la fréquence de réception



MAILINBLACK

Bonjour Théo, voici votre dernier rapport d'emails stoppés :

Compétences cyber des salariés : quelle différence entre leur perception des risques et la réalité ?

🔔 Selon une étude OpinionWay réalisée en mars 2022 pour Mailinblack, 88% des collaborateurs pensent être vigilants quant aux emails qu'ils reçoivent. Pourtant, seulement 3% sont capables d'identifier un email frauduleux quand ils y sont confrontés. Pourquoi sont-ils vulnérables ? Découvrez-le dans notre dernier [article](#).

Aide à la lecture de votre rapport

📘 Pour votre sécurité, nous vous précisons pour chaque email stoppé ci-dessous, si l'expéditeur a deux adresses :

- l'adresse email d'enveloppe - indiquée en noir et par une icône. C'est la moins falsifiable, pensez à la vérifier systématiquement.
- l'adresse email d'entête (possiblement associée à un nom et un prénom) - indiquée en gris.

Pour plus d'informations, consultez notre [FAQ](#).

Accéder à mon espace

1 email(s) en attente

✉ bounce+0699cb.ac57-tdubois.com@mg.s35798.fr 18h01 - 26/03/2022

Celine Leroux <celine.leroux@mg.s35798.fr>

Montée en compétences de vos collaborateurs : les dispositifs de financement de la formation professionnelle

Grâce aux nouveaux dispositifs, ...

Récupérer Autoriser Bannir

Vous avez également reçu 2 spams et 0 virus.

Accéder à mon espace

Dernier rapport reçu : 26/03/2022 - 11h00

[Gérer la périodicité de mes rapports d'emails stoppés](#)



⚠ Vous avez récupéré cet email qui était catégorisé en spearfishing.

Pour plus de sécurité, nous vous conseillons de vérifier à nouveau l'identité de votre expéditeur ainsi que l'ensemble de son email : l'adresse d'entête correspond-elle bien à l'adresse d'enveloppe ? Attendez-vous cet email ?

N'hésitez pas à contacter votre administrateur Mailinblack si vous avez le moindre doute.

Si vous êtes sûr(e) qu'il ne s'agit pas d'une tentative d'usurpation, vous pouvez nous le signaler en cliquant sur le bouton ci-dessous.

Ce n'est pas un spearfishing

Jean,

Nous avons trouvé un problème de configuration concernant votre boîte mail le **08/24/2022 à 15:12**

Pour éviter tout problème et récupérer vos emails nous conseillons de faire une maintenance.

[Effectuer la maintenance en cliquant sur ce lien](#)

Sans action de votre part, vous risquez de perdre des messages importants.

Merci pour votre coopération !

Une activation du service adaptée à votre infrastructure

100% compatible avec votre messagerie



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





**CONTACTEZ-
NOUS**



contact@aldaran.fr



+33 (0)2 78 26 03 45

Conduite du projet

Préparation	Paramétrage solution « On Boarding »	Installation, pilote , changement	Suivi poste déploiement
<ul style="list-style-type: none"> • Présentation du Success Program • Définir le planning de déploiement • Aligner les attendus et les prochaines étapes • Programmer les formations 	<ul style="list-style-type: none"> • Déclaration des NDD et Serveurs Messagerie • Synchronisation des utilisateurs • Personnalisation 	<ul style="list-style-type: none"> • Pré-paramétrage de listes d'expéditeurs autorisés, • Redirection des champs MX • Tests et validation <p><u>Protect Out</u></p> <ul style="list-style-type: none"> • Enrichissement automatique des listes d'expéditeurs • Déploiement progressif des protections <p><u>Conduite du changement</u></p> <ul style="list-style-type: none"> • Information et présentation • Découverte de l'interface par l'utilisateur • Formations 	<ul style="list-style-type: none"> • Suivi Post Installation • Assistance à l'administration / administration déléguée • Escalade support
30 minutes	1 heure	2-4 semaines	Suivi mensuel / CoPil trimestriel