

• 2024

Sécurisation des messageries professionnelles contre les cyberattaques

🇫🇷 Solution développée & hébergée en France

[Roadmap des solutions Mailinblack](#) 

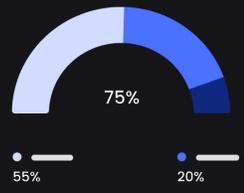


📧 Emails traités par Protect
1 992 ↓ 2%

📧 Emails en quarantaine
292 ↓ 9%

📧 Emails valides
1700 ↑ 8%

Répartition Mois



Historique ● Valide ● Quarantaines





Votre cybersécurité est notre métier



Lauréat Grand Défi
Cybersécurité



Catalogue
Tech.Gouv



Conformité
RGPD



Labellisé Cybersecurity
Made In Europe

20 ans

d'expertise en
cybersécurité

22 000

organisations sont
protégées par Mailinblack

+400 mille

collaborateurs formés
chaque année

+1 milliard

d'emails bloqués
chaque année

Protection des messageries



- Filtrage avancé
- IA propriétaire
- Gain de productivité
- Bien-être numérique

Sensibilisation et formation à la cybersécurité des collaborateurs



- Audit complet
- Programme automatisé
- Apprentissage par l'expérience



- Formation en micro-learning
- Gamification
- Réduction des risques

Gestionnaire de mots de passe professionnels



- Chiffrement de mots de passe robuste
- Partage simplifié
- Gestion unifiée pro/perso

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

MAILINBLACK

Aide Ismael Spencer Client : Rutherford-Howe 15

Bonjour Ismael Spencer 🙌

Aucune

Mes applications Manager

Protect

Gérez la sécurité des messageries de vos collaborateurs

- Protégez vos utilisateurs contre les risques cyber
- Soyez armé contre le piratage informatique

Accéder à Protect

Cyber Coach

Simulez des cyberattaques pour augmenter le niveau de cyberculture de vos collaborateurs

- Réalisez un rapport d'audit des vulnérabilités réelles de votre organisation
- Sensibilisez vos collaborateurs à travers des attaques simulées

Accéder à Cyber Coach

Cyber Academy

Formez efficacement et durablement vos collaborateurs à la cybersécurité

- Pilotez la formation de vos collaborateurs en un clin d'oeil
- Adaptez la formation au rythme d'apprentissage de vos collaborateurs

Accéder à Cyber Academy

Sikker

Stockez, gérez et partagez vos identifiants en toute sécurité.

- Gérez des coffres-forts partagés pour vos collaborateurs en un clin d'oeil
- Assurez le contrôle et la fiabilité des mots de passe stockés dans les coffres-forts partagés

Accéder à Sikker

Management

Paramétrez vos solutions et gérez vos utilisateurs

Accéder à Management



Management

Votre espace manager permet de gérer les éléments communs aux toutes vos solutions :

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

- À propos de nous

Les collectivités et établissements de santé nous font confiance



• État des lieux

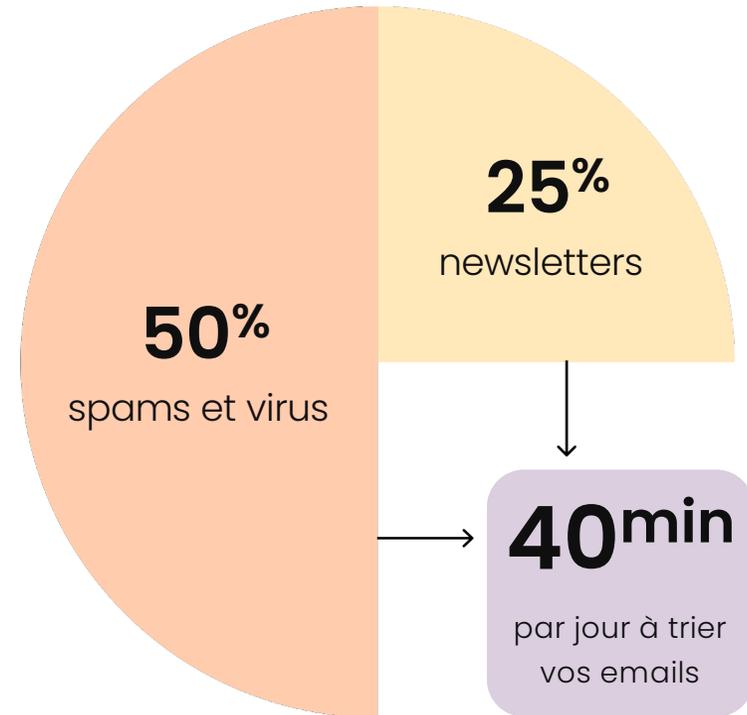

90%
des attaques abouties impliquent une erreur humaine


73%
des entreprises françaises sont ciblées par des cyberattaques


3ème
position pour les cyberattaques, dans le classement des risques mondiaux


2 milliards d'euros
c'est le coût global des cyberattaques en 2022

La messagerie est le vecteur principal d'attaques informatiques



Types d'attaques passant par l'email :

 Ransomware

 Phishing

 Spearphishing

 Browser in the browser

 QR code

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



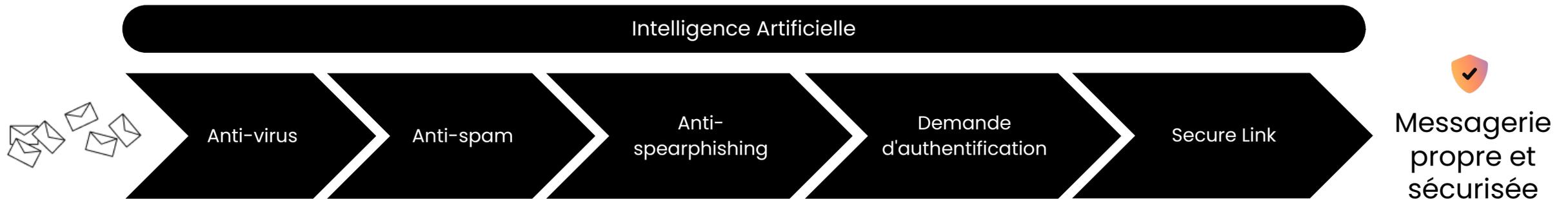
la plus performante



la plus accessible



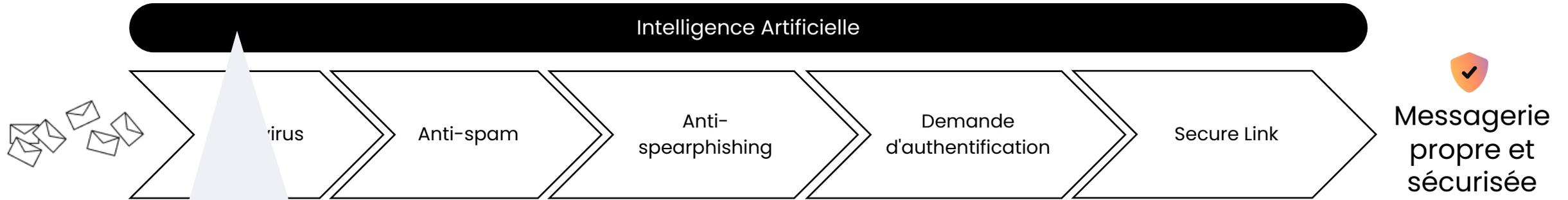
Fonctionnement de notre technologie



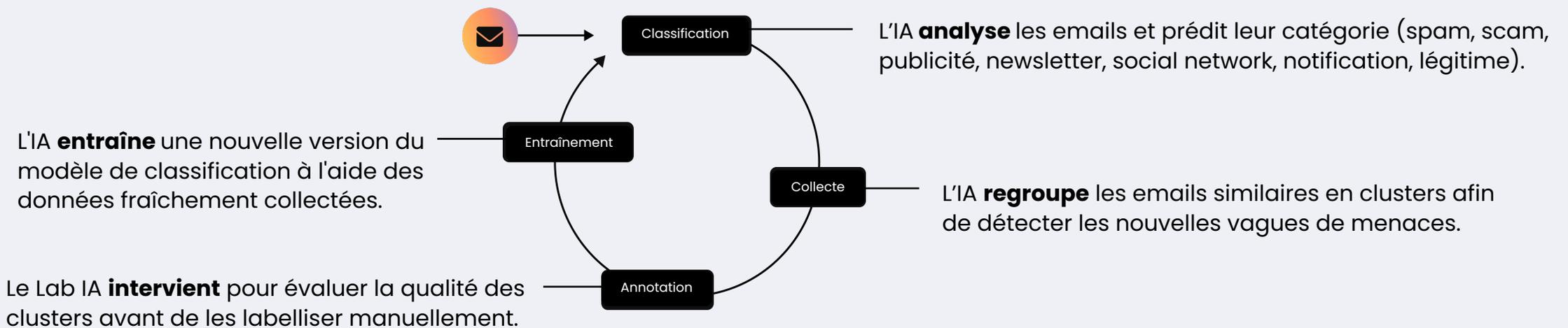
Découvrez en
en vidéo notre
solution :



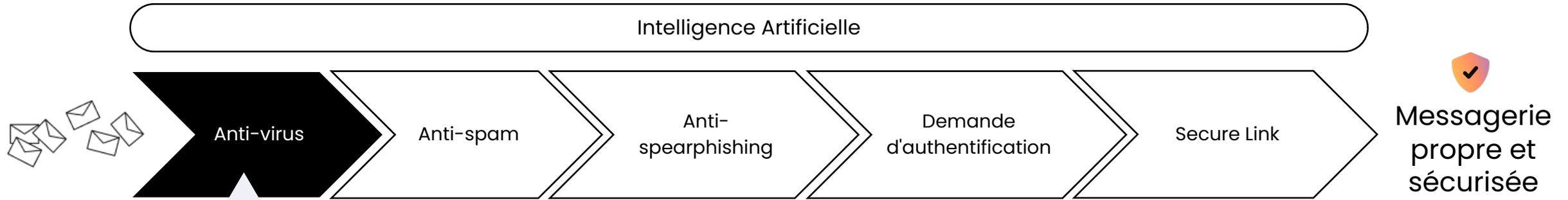
• Protect



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



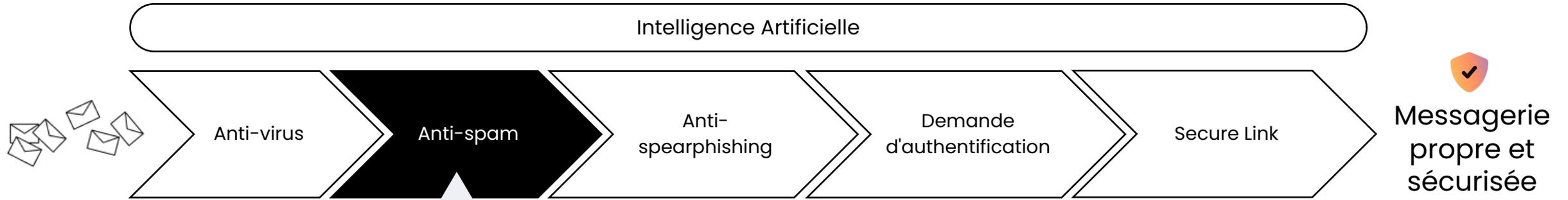
- Protect



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

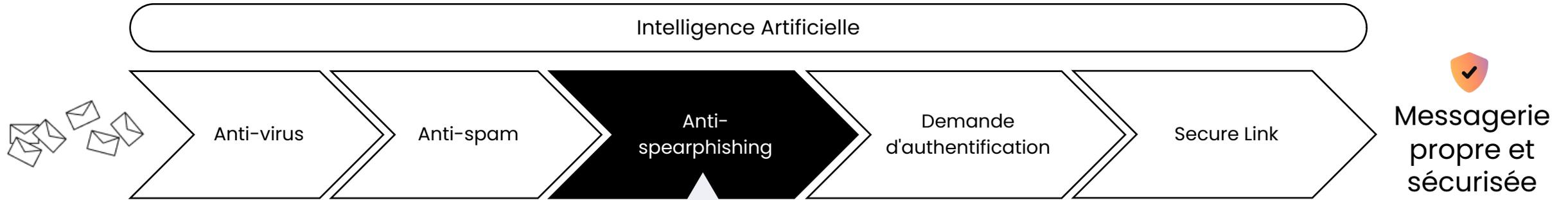
- Protect



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

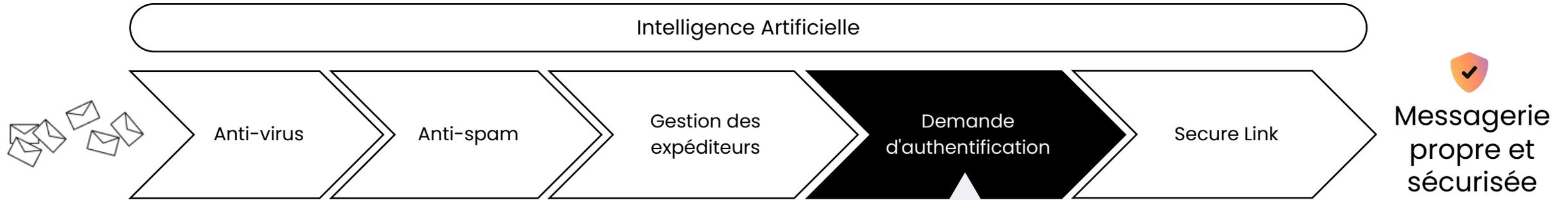
- Protect



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

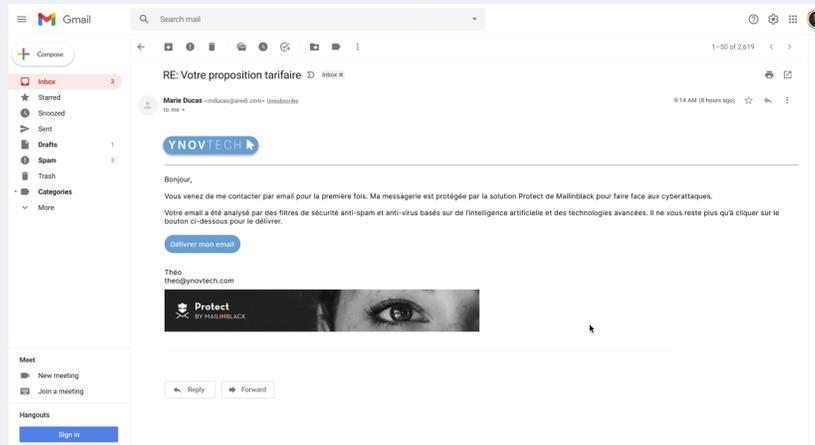
- Analyse heuristique sur les informations de l'expéditeur (nom d'affichage, alias, comparaison adresse en-tête vs adresse enveloppe, typosquatting)
- Analyse de l'authenticité et du contenu de l'email grâce à notre IA (données sensibles, sémantiques d'urgences...)

- Protect



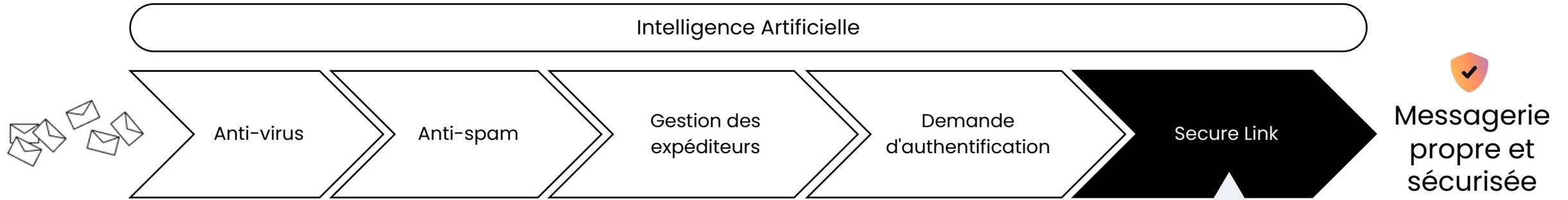
La demande d'authentification, votre plus haut niveau de confort :

- 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

- Protect



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

- Protect

Secure Link : ce que voit l'utilisateur

Objet : Votre colis est en cours d'acheminement

De : Service Fedex - service@notification-fedex.fr



Bonjour,

Nous vous informons que votre colis est en route !
Pour suivre son acheminement veuillez cliquer ici :

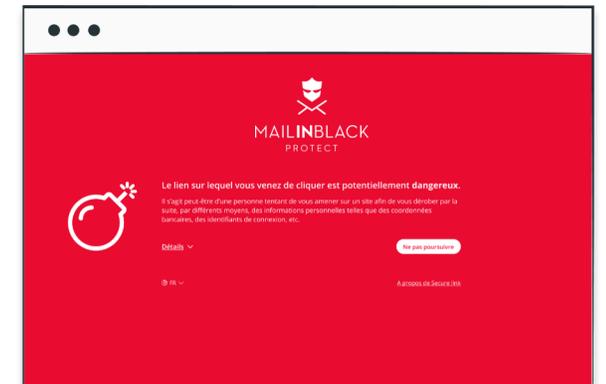
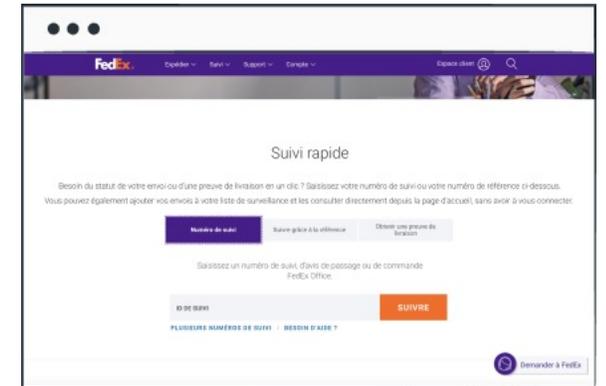
Suivre mon colis

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



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

Objet : Votre colis est en cours d'acheminement

De : Service Fedex - service@notification-fedex.fr



Bonjour,

Nous vous informons que votre colis est en route !
Pour suivre son acheminement veuillez cliquer ici :

Suivre mon colis

<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)

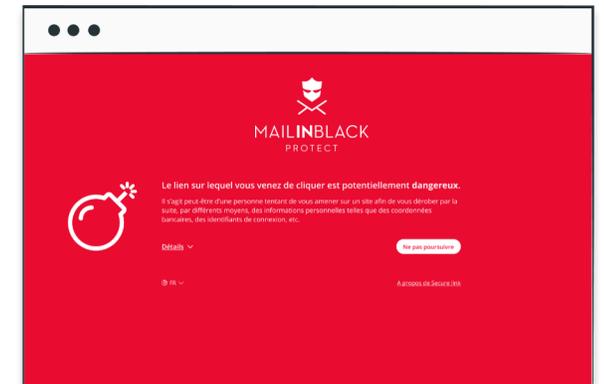
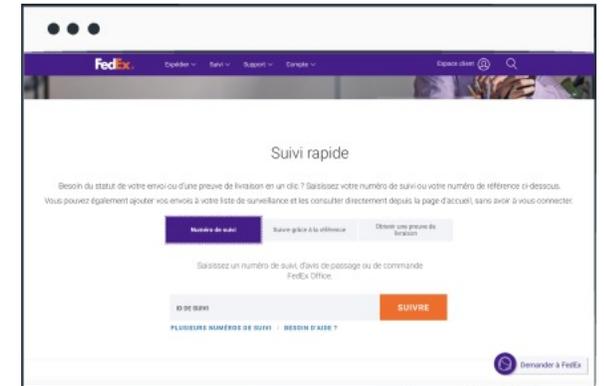
Intervention de l'IA Secure Link

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

✔ Simple

✔ Efficace

✔ Sécurisé


**Email délivré au
destinataire**



Contrôle Mailinblack

- 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

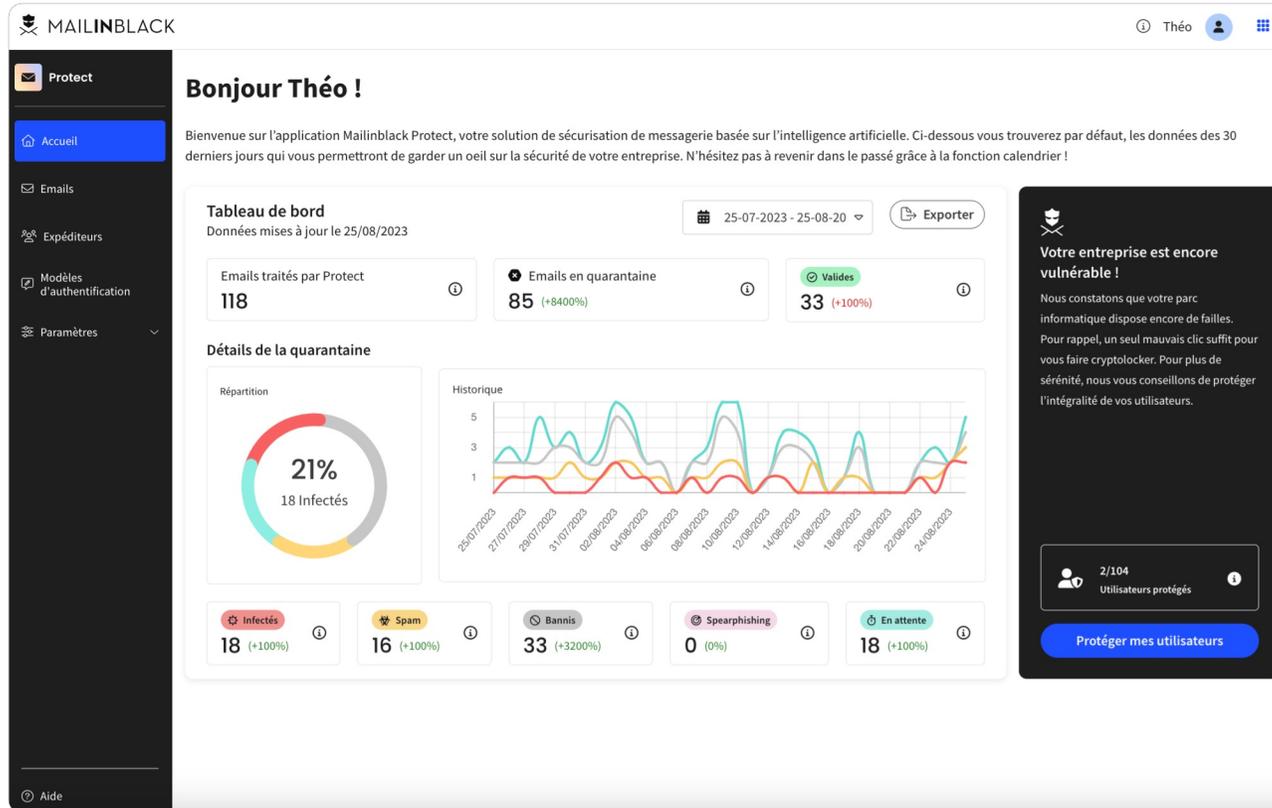
3

Un scan antivirus est
réalisé sur tous vos emails
envoyés

4

L'administrateur est alerté
et les envois frauduleux
sont bloqués

- Protect



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

- Protect

The screenshot displays the MAILINBLACK web interface. On the left is a dark sidebar with navigation options: Accueil, Emails (highlighted), Expéditeurs, Modèles d'authentification, Paramètres, and Aide. The main content area is titled 'Emails' and features a search bar with the text 'Rechercher dans tous le' and buttons for 'Rechercher' and 'Recherche avancée'. Below the search bar are tabs for 'Quarantaine', 'Valide', and 'Sortant'. The 'Quarantaine' tab is active, showing a list of 20 email entries. Each entry includes a checkbox, the sender (Expéditeur), the recipient (Destinataire), the subject (Objet), and the date. The subject line is color-coded by status: 'Banni' (grey), 'En attente' (green), 'Infecté' (red), and 'Spam' (yellow). The table data is as follows:

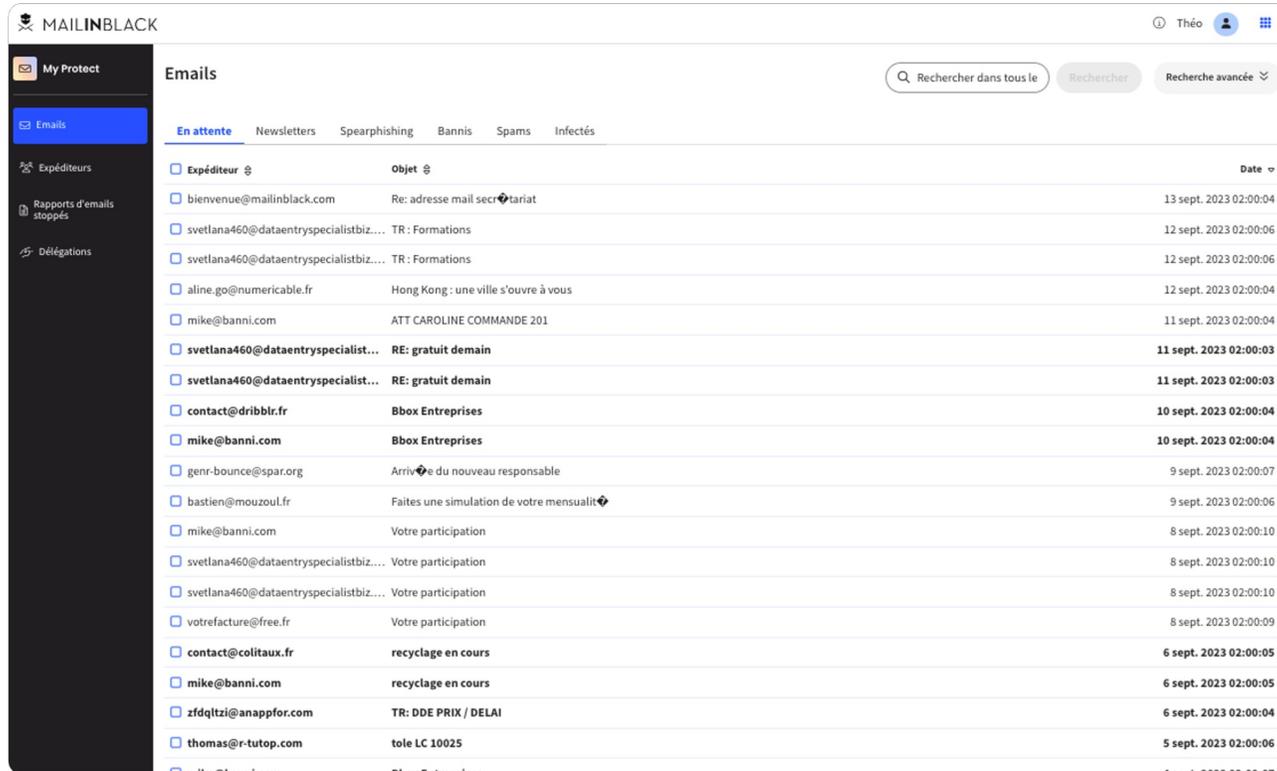
Expéditeur	Destinataire	Objet	Date
kyzar@socialcirtraining...	nicolas@democom.com	Banni Hong Kong : une ville s'ouvre à vous	25 août 2023 02:00:06
mike@banni.com	nicolas@democom.com	En attente Hong Kong : une ville s'ouvre à vous	
alex@boximail.com	thomas@democom.com	Infecté Re: Ordonnance	25 août 2023 02:00:03
regul-noc@plass.com	thomas@democom.com	Spam La newsletter Emploi Format	25 août 2023 02:00:02
steve@ferra.fr	nicolas@democom.com	Infecté Devis no 4572	25 août 2023 02:00:02
akour@dima-g.net	nicolas@democom.com	Infecté INVITATION - AFTERWORK	24 août 2023 02:00:07
aline.go@numericable.fr	nicolas@democom.com	Infecté Hong Kong : une ville s'ouvre à vous	24 août 2023 02:00:02
lucasmaury@meunier.fr	lucyberger@democom.com	Banni Engager trouver chiffre écrire.	23 août 2023 05:11:28
lucasmaury@meunier.fr	lucyberger@democom.com	Infecté Considérer chance crier.	23 août 2023 05:11:28
lucasmaury@meunier.fr	lucyberger@democom.com	Spam Rencontrer te sombre moment ouvrir haut compagnie ou.	23 août 2023 05:11:28
lucasmaury@meunier.fr	lucyberger@democom.com	Spam Regarder essayer douter.	23 août 2023 05:11:28
lucasmaury@meunier.fr	lucyberger@democom.com	En attente Français campagne tout.	23 août 2023 05:11:28
lucasmaury@meunier.fr	lucyberger@democom.com	Banni Prison arme demain observer nouveau histoire envie.	23 août 2023 05:11:28
isaac47@baron.fr	victorcarpentier@democo...	Infecté Nation essayer fusil avec chute inquiétude absolu.	23 août 2023 04:22:18
isaac47@baron.fr	victorcarpentier@democo...	Infecté Lieu demeurer entraîner créer convenir voir plus.	23 août 2023 04:22:18
isaac47@baron.fr	victorcarpentier@democo...	En attente Devant fatiguer abattre répéter mois dominer te.	23 août 2023 04:22:18
abonnet@legrand.fr	rolandfort@testdemo.fr	Spam Cependant habitant fin million partir.	23 août 2023 03:14:37
abonnet@legrand.fr	rolandfort@testdemo.fr	En attente Effort pencher militaire assister.	23 août 2023 03:14:37

... 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

• Protect



Les bénéfices pour vos collaborateurs ...

Interface web personnelle My Protect

✓ Serenité

✓ 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

• Protect

 **Protect**
BY MAILINBLACK

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

Information importante :

Une nouvelle campagne de **malware** nommée "**Emotet**" se propage actuellement et nécessite votre plus grande vigilance. Mailinblack vous invite à [consulter ses recommandations](#) pour vous en protéger.

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 [centre d'aide en ligne](#).

theo@ynovtech.com - 1 email(s) en attente [Accéder à mon espace](#)

Expéditeur	Objet	Date
 noreply@email.teams.microsoft.com <small>Teams <clientmessage@teams.microsoft.com></small>	Guillaume Dreyfuss dans Hangout	09:32 09/10
Récupérer Autoriser Bannir		

1 email(s) catégorisés en spearphishing

Une attaque par spearphishing est caractérisée par l'usurpation de l'adresse email d'un de vos contacts et un contenu d'email imitant une demande crédible.

Pour détecter ce type d'attaque, vérifiez toujours que l'adresse d'enveloppe correspond bien à l'adresse d'entête et au nom et prénom qui peuvent y être associés. Attention aux caractères qui se ressemblent : un i et un l par exemple. Si vous avez le moindre doute, contactez votre administrateur Mailinblack.

 bounce+0699cb.ac57-tdubois.com@mg.s35798.fr <small>Celine Leroux <celine.leroux@mg.s35798.fr></small>	Montée en compétences de vos...	10:04 09/10
Récupérer Autoriser Bannir		

1 newsletter(s) en attente

 805-ptz-019.0.393241441@email.lucidchart.com <small>Lucidspark <email@lucidspark.com></small>	Sautez du tableau blanc à la planche ...	10:54 09/10
Récupérer Autoriser Bannir		

 Vous avez également reçu 2 spams et 0 virus. [Accéder à mon espace](#) 

Dernier rapport reçu : 09/10/2023 - 11h00
[Gérer la périodicité de mes rapports d'emails stoppés](#)

 MAILINBLACK

... 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



Vous avez récupéré cet email qui était catégorisé en spearphishing. 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 spearphishing

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

• Notre accompagnement



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

Notre service client est disponible du lundi au vendredi de 8h à 18h :

Chat ✓

Email ✓

Téléphone ✓

- 250 licences

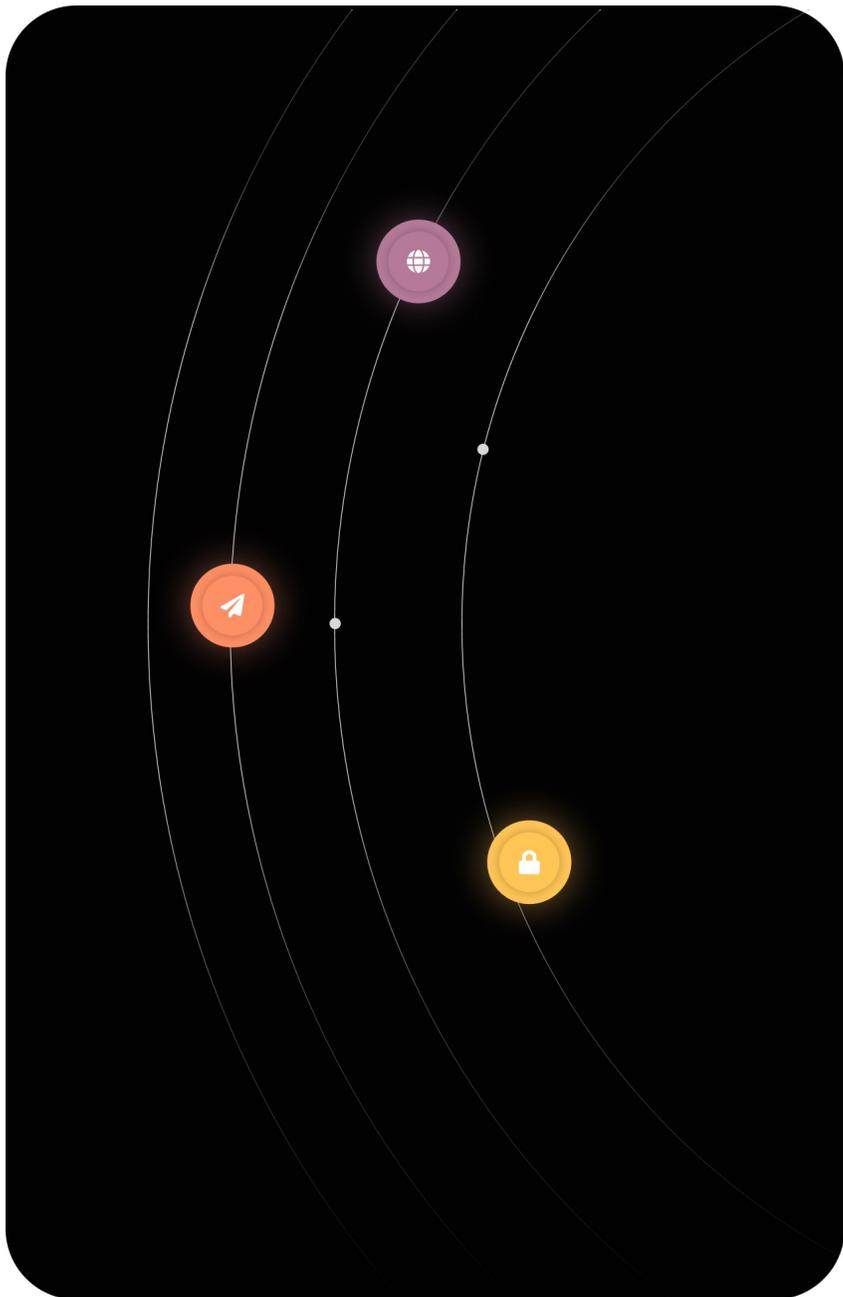
Mise à disposition de plusieurs aides :

- Onboarding et pack accompagnement : tutoriel in-app
- Équipe à votre disposition

+ 250 licences

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

- Analyse de votre taux de vulnérabilité
- Conseils & préconisations adaptés à votre organisation
- Équipe à votre disposition



Contactez-nous

✉ contact@mailinblack.com

☎ +33(0)4 88 60 07 80

🌐 www.mailinblack.com



Déploiement Cloud

Set up préparatoire

- Présentation du Success Program
- Programmation des formations
- Alignement sur les attendus et les prochaines étapes

20 minutes

Onboarding

- Réception des accès manager
- Déclaration des NDD et Serveurs Messagerie
- Synchronisation des utilisateurs
- Personnalisation DA

Protect Out :

- Pré-configuration du connecteur
- Validation du SPF

45 minutes

Installation, pilote, changement

- Lien Onboarding terminé
- Redirection des champs MX

Protect Out :

- Activation
- Enrichissement automatique des listes d'expéditeurs
- Déploiement progressif des protections

Conduite du changement :

- Information et présentation
- Découverte de l'interface par l'utilisateur
- Formations

1 à 3 semaines

Finalisation

- Suivi post-installation
- CSM dédié prend le relai
- Escalade support

CoPil trimestriel



Déploiement On Premise

Set up préparatoire

- Set up préparatoire
- Présentation du Success Program
- Définition du planning de déploiement
- Programmation des formations
- Alignement sur les attendus et les prochaines étapes
- Envoi des éléments pour installer la VM

🕒 30 minutes

Onboarding

- Réception de l'image disque
- Création de la machine
- Ouverture des ports nécessaires

Protect Out :

- Pré-configuration du connecteur
- Validation du SPF

🕒 1 heure

Installation, pilote, changement

- Installation et formation avec chargé de production
- Synchronisation des utilisateurs

Protect Out :

- Enrichissement automatique des listes d'expéditeurs
- Déploiement progressif des protections
- Redirection des champs MX

Conduite du changement :

- Information et présentation
- Découverte de l'interface par l'utilisateur
- Formations

🕒 2 à 4 semaines

Finalisation

- Suivi post-installation
- CSM dédié prend le relai
- Escalade support

🕒 CoPil trimestriel



« 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

- Annexes



« 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