

Derniers domaines autorisés

Domaines
lemonde.fr
aceo.com
universal.io
yahou.com

Derniers emails reçus

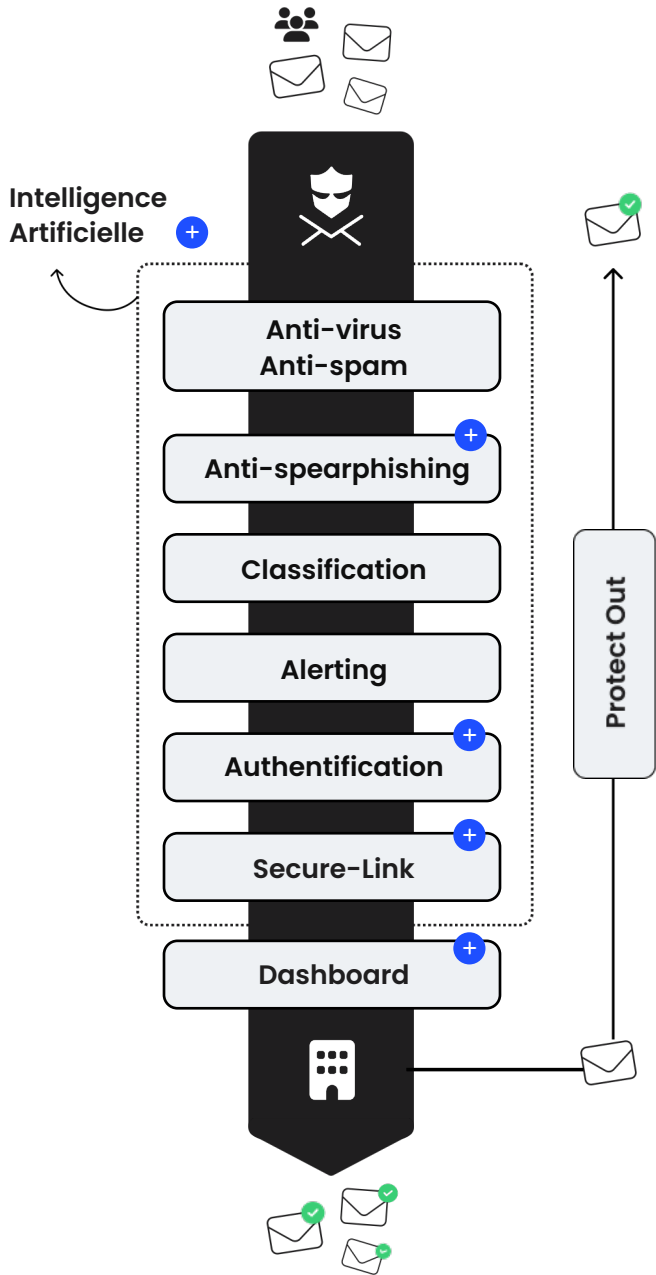
Expéditeur	Objet	Date	
---	---	---	
---	---	---	
---	---	---	
---	---	---	

La protection email conçue pour répondre aux exigences de sécurité les plus élevées

🇫🇷 Solution développée & hébergée en France

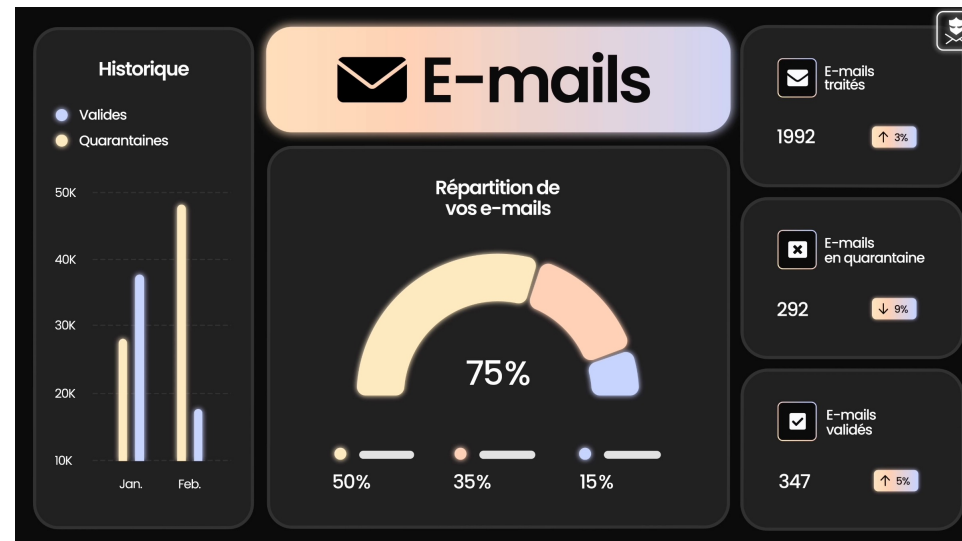
[Roadmap des solutions Mailinblack](#)

• Présentation



Élevez vos standards de protection de messagerie avec notre offre Protect **Advanced**

Protect Advanced utilise des technologies de pointe pour offrir une **protection proactive** et sécuriser vos échanges critiques. Sa **protection multi-couches** bloque les menaces à la source, tout en **améliorant les performances** de vos infrastructures et en renforçant la défense contre les **cyberattaques sophistiquées**.



Conçu pour les environnements IT complexes, il propose une **analyse comportementale avancée** et une **gestion centralisée des menaces** via une intégration fluide avec votre **SIEM**, simplifiant la surveillance et la **réponse aux incidents**.

+ Innovations technologiques

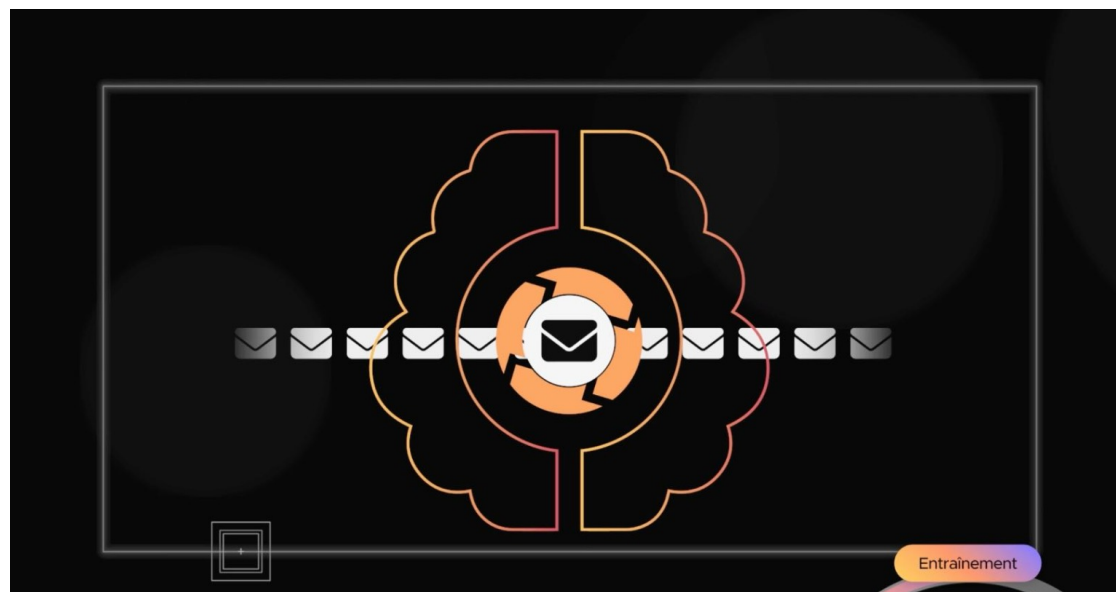


Intelligence Artificielle +



Intelligence Artificielle propriétaire

Protect Advanced intègre un modèle de **Deep Learning** basé sur l'**extraction automatique des caractéristiques des emails** pour identifier et distinguer les messages légitimes des illégitimes.



IA propriétaire

Notre équipe de docteurs en data science développe et **met à jour quotidiennement notre intelligence artificielle propriétaire** pour détecter :

- les spams sophistiqués,
- les attaques ciblées,
- les malwares polymorphes,
- les menaces APT ou Zero-Day





Protection anti-virus et anti-spam

Au coeur de notre solution, une protection antivirale avancée pour **bloquer les malwares et phishing**, complétée par une **IA évolutive** qui affine le **filtrage des spams** avec précision, assurant une **sécurité robuste** sans perturber l'expérience utilisateur.

Expertise anti-virus

- Technologies antivirus propriétaires
- Bases de données propriétaires
- Intégration de Bitdefender (détection de menaces avancées dans les pièces-jointes)

Pour une **sécurité complète et constamment actualisée** de votre infrastructure de messagerie.

Bitdefender

Anti-spam de haute précision

Les **contrôles SPF, DKIM et RBL** assurent un filtrage renforcé des emails non productifs et empêchent les falsifications d'identité. Notre **IA avancée ajuste en permanence** le filtrage pour une précision maximale face aux **nouvelles menaces**.

Spam

Votre compte a été sélectionné pour une récompense exclusive !
Félicitations ! Votre adresse e-mail a été choisie parmi des milliers pour ...

Infecté

Mise à jour urgente de votre logiciel de sécurité
Bonjour, Une nouvelle vulnérabilité critique a été détectée dans votre système. Pour protéger vos données personnelles et professionnelles ...

Newsletter

Découvrez nos dernières nouveautés et conseils exclusifs ! ✨
Bonjour Estelle ,Nous sommes ravis de vous présenter les dernières ...

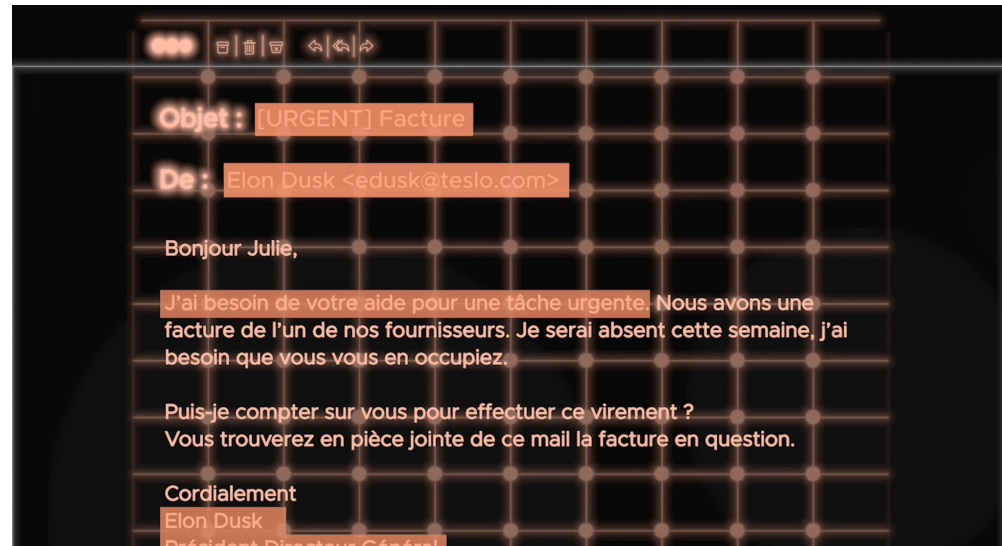


Anti-spearphishing

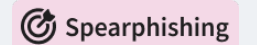


Protection anti-spearphishing

Les attaques sophistiquées d'aujourd'hui **ciblent davantage les utilisateurs** que les technologies. Protect Advanced **identifie et hiérarchise les vulnérabilités**, offrant ainsi une protection spécialisée contre les menaces ciblées telles que les **tentatives de fraude** ou de **compromission de comptes**.

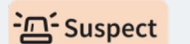


IA analytique



Analyse de l'authenticité des emails et des signaux d'urgence comme les **demandes de paiement**, grâce à l'apprentissage automatique.

Heuristiques avancées et prévention des fraudes



Plus de **1 000 vérifications heuristiques**, incluant la détection des **fraudes par virement** et les **modifications d'IBAN**, pour renforcer la précision du filtrage des emails.



Classification

Classification

Intègre des outils avancés vous permettant d'authentifier efficacement vos emails et réduire considérablement les risques de compromission.

Validation DKIM/DMARC

- Renforcent l'authenticité et la sécurité des emails grâce à des signatures numériques
- Améliorent la délivrabilité des messages
- Protègent contre les usurpations d'identité
- Renforcent la réputation de vos domaines

Tracer l'email

- Réception de l'email par Mailinblack
 - Date : le 3 avr. 2024 08:43:47
 - UUID : 377887d1012d428a941cb8afe62fe987
 - ID in : B8EF41C0200
 - IP de l'expéditeur : 10.1.24.6
- Traitement de l'email par Mailinblack
 - Antivirus
 - Mots clé - Objet
 - SPF NONE ip: 10.1.24.6 domaine : globaltech-solution.com
 - RBL ip: 10.1.24.6
 - DMARC
 - IA spearphishing

Résultat du traitement

Date : le 3 avr. 2024 08:43:50

Catégorisation : Spearphishing

Raison : L'email à été classé comme spearphishing car il contient des coordonnées bancaire de type : IBAN

Pré-visualisation de vos emails

Visualisez les emails suspects en quarantaine directement depuis votre tableau de bord pour gagner du temps dans l'analyse des menaces potentielles.

Contenu de l'email

Prévisualiser l'email

De : PayFit <no-reply@payfit.com>
Envoyé : mercredi 21 septembre 2022 12:23
À : Estelle Dupond <estelle@globaltech-solution.com>
Objet : Renseignements importants concernant votre compte

Bonjour,

Merci de vérifier vos informations de compte via le lien ci-dessous en cliquant sur le bouton de redirection. Vous devez confirmer vos données de comptes afin de conserver vos accès.

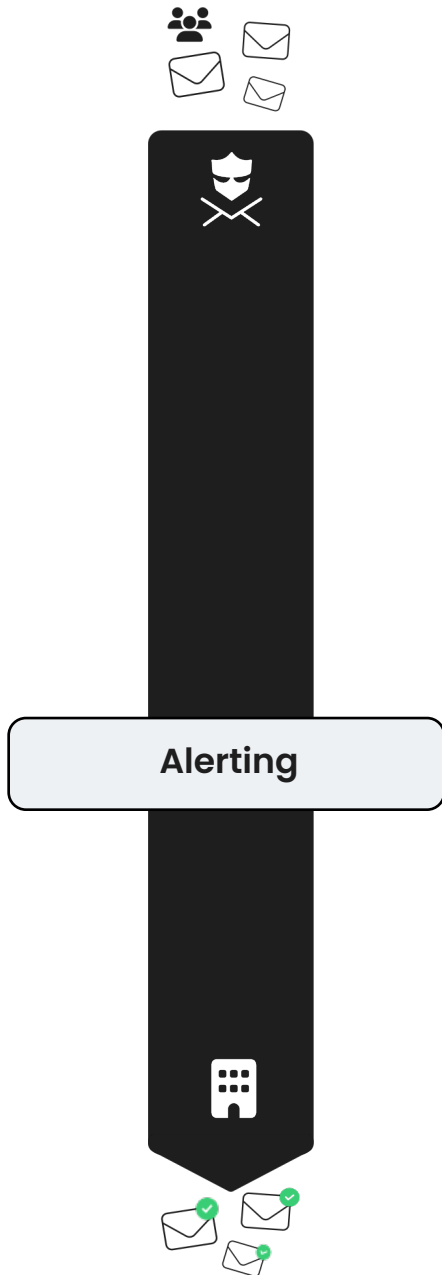
En cas de non action votre compte pourra être suspendu en attendant que la procédure soit effectuée toujours via cet email.

Suivre les démarches

Pour des raisons de sécurité ce lien ne peut être utilisé qu'une seule fois et expirera dans 30 minutes

L'équipe PayFit.

Fermer



Alerting

Déployez une **surveillance active** associée à des **alertes avancées** vous notifiant instantanément des **tentatives d'usurpation** et des **activités inhabituelles**.

Détection et notification des menaces

Le système vérifie l'authenticité des emails entrants, détecte les menaces potentielles en temps réel, et envoie des **alertes immédiates** grâce à une **analyse continue des tendances**, vous permettant d'agir rapidement pour protéger votre organisation.

🔔 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.

Engagement utilisateur et avertissements

Un **bandeau d'avertissement** incite à la prudence pour les emails suspects et un bouton dédié permet de signaler les menaces, facilitant la **gestion des spams par les administrateurs**.

Cet e-mail contient des éléments suspects

Ce email a été identifié comme **spam**. Veuillez vous assurer de la fiabilité de l'email avant toute interaction.

Autoriser l'expéditeur

Bannir l'expéditeur

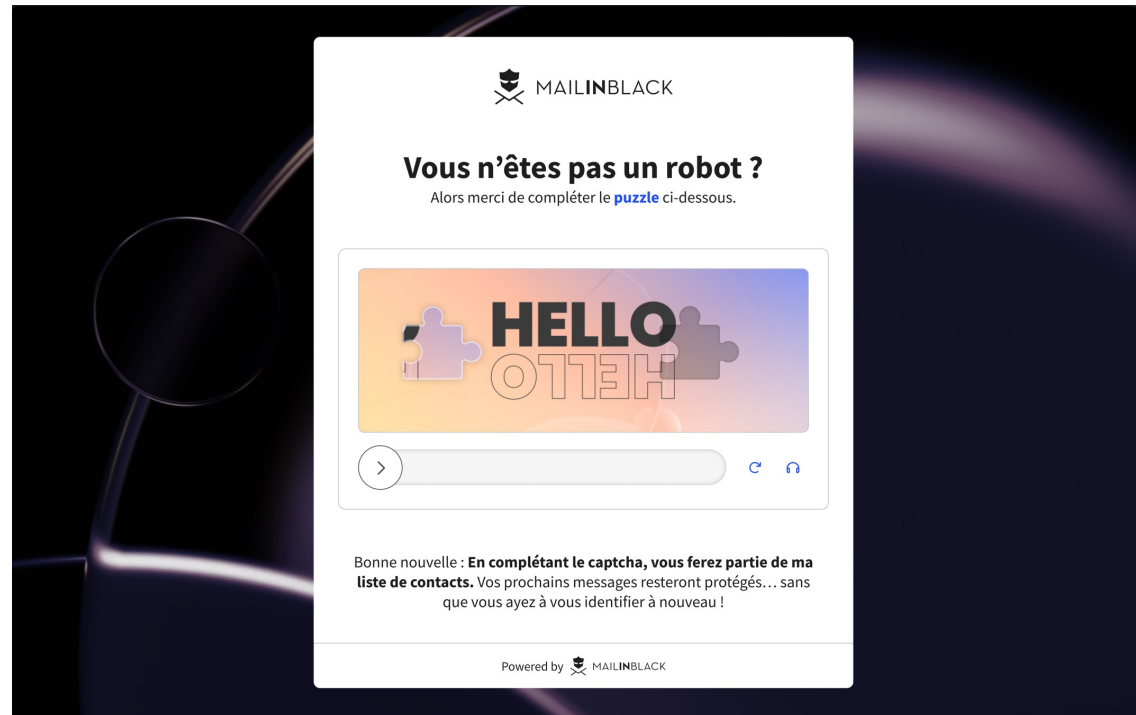


Authentification



Demande d'authentification

En activant la demande d'authentification, vous ajoutez une **barrière de sécurité supplémentaire** qui **vérifie l'identité des nouveaux expéditeurs** pour une classification plus précise de vos emails.



Légitimité de l'expéditeur

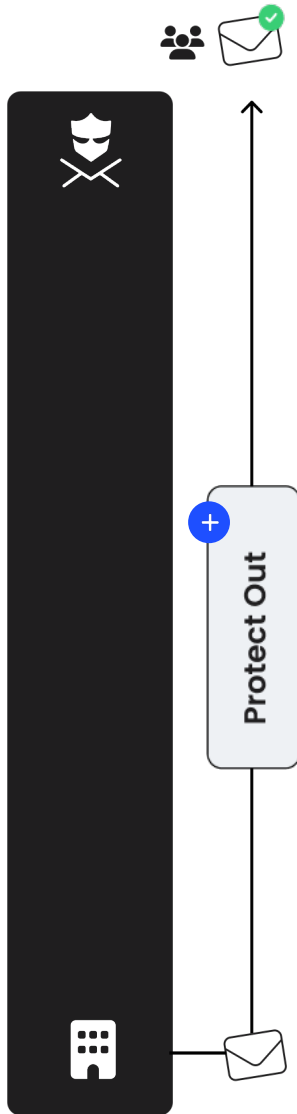
Un **CAPTCHA** simple pour valider l'identité des nouveaux interlocuteurs.

Personnalisation

Authentification **personnalisable** avec logo et charte graphique de votre organisation.

Engagement sécurité

Garantit une boîte mail **sans communications non désirées**.



Protect Out

Sécurisez vos envois et assurez la **protection de vos destinataires** grâce à notre technologie d'analyse des mails sortants.

1

Auto-apprentissage

Liste blanche automatique des destinataires.

2

Sécurité renforcée

Scan **antivirus, anti-phishing** et vérification des **pièces jointes**.

3

Préservation IP

Protection de la **réputation de votre IP** (en SaaS).

4

Alertes

Détection de **comportements anormaux** (envois massifs) et usurpations.

Data Loss Prevention (DLP)

Renforce le contrôle des **emails sortants** en analysant leur contenu pour identifier les **informations sensibles** susceptibles d'être divulguées. Lorsqu'un numéro de sécurité sociale, des coordonnées bancaires ou un mot de passe sont détectés, l'email est automatiquement bloqué et **placé en quarantaine**, accompagné d'un tag "Données sensibles" pour en faciliter le suivi.

Fonctionnalité DLP :

- Automatique
- Personnalisé : import de dictionnaires métier

La DLP nécessite l'activation de Protect Out

- Technologies

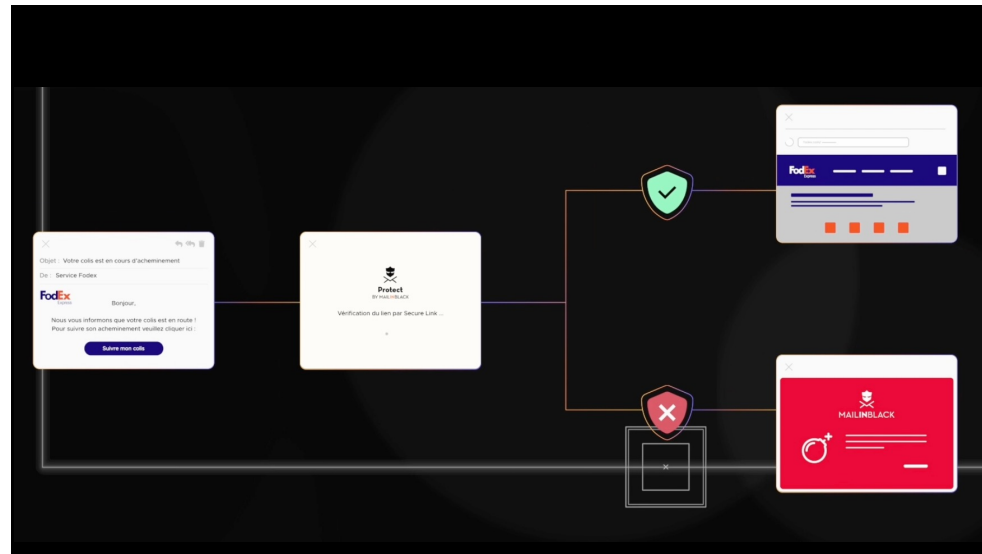


Secure Link



Secure Link

Mailinblack a développé une technologie anti-phishing nommée Secure Link qui **bloque les URLs forgées**, ayant pu contourner la 1ère analyse (lors du traitement anti-malware) via obfuscation.



+78%

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

Réécriture et chiffrement du lien

Au moment du scan de l'email, Protect réécrit et chiffre les liens (contenus dans le corps) **avant qu'ils ne soient délivrés** aux utilisateurs.

Vérification du lien

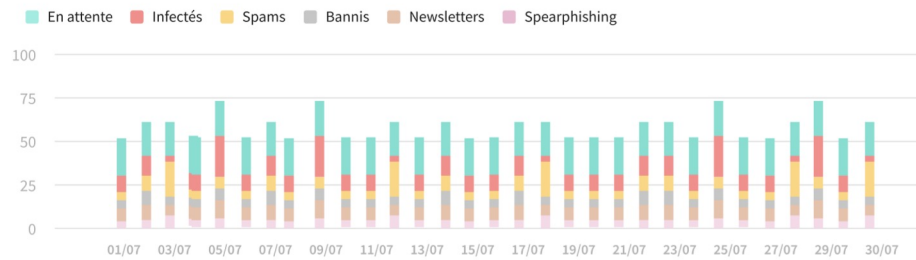
Lorsqu'un utilisateur clique sur un lien dans l'email, Protect effectue une **vérification instantanée**. Si le lien est malveillant, l'accès est bloqué, limitant le risque de partage de données sensibles.

Interface manager

Pilotez efficacement vos emails avec une **vue d'ensemble des données clés**, garantissant une **sécurité renforcée** et une **gestion optimisée**

Vue d'ensemble des emails reçus

Détail de vos emails reçus



Détail des emails sortants

Afficher le détail

Emails envoyés

216

Remis

159

Quarantaine

23

Non remis

34

Emails en quarantaine

Adrien Fillion

Catégories



En attente	37 %
Infectés	25 %
Spams	23 %
Bannis	14 %
Newsletters	9 %
Spearphishing	9 %

Derniers domaines autorisés

Voir tous

Email

google.com			
yahoo.com			
universal.io			
ryanair.com			

Analyse des utilisateurs et services

Répartition par utilisateurs

Rechercher

Gérer les colonnes

Toutes

Catégories

En attente Infectés Spams Bannis Newsletters Spearphishing

<input type="checkbox"/>	Nom	Emails	Menaces interceptées	Détail de leur quarantaine		
<input type="checkbox"/>	Adrien Fillion	afillion@acme.com	148			
<input type="checkbox"/>	Lucas Miel	lucas.miel@acme...	92			
<input type="checkbox"/>	Contact	contact@acme.com	89			
<input type="checkbox"/>	Raymond Dupont	rdupont@acme.c...	66			
<input type="checkbox"/>	Océane Barege	oceane.barege@a...	87			

Afficher 10 éléments par page.

1 2 3 4 ... > >>

Alimentation SIEM

Enrichissez votre SIEM avec **les données comportementales** de Protect Advanced pour des **prises de décisions éclairées** et une **analyse approfondie** de la sécurité de votre organisation, assurant une protection complète contre les cyberattaques.

Sélection de la période du rapport

Avant d'exporter votre fichier assurez-vous de sélectionner la période et le type d'agrégation que vous souhaitez.

Sélectionner la période

24-06-2024 - 24-07-2024

Type d'agrégation

Chaque jour Chaque semaine Chaque mois

Annuler

Exporter

Interface utilisateur

Vos utilisateurs profitent d'**outils performants et intuitifs** pour gérer leurs emails en toute **autonomie**, améliorant leur **productivité** et simplifiant la sécurité de leurs **communications**

My Protect

Interface intuitive pour une **gestion simplifiée** de la quarantaine.
Le **tri automatique** réduit les emails indésirables, et les utilisateurs ajustent leurs préférences en quelques clics.

The screenshot shows the 'My Protect' interface. At the top, there's a header with the MAILINBLACK logo and user information for Estelle ADMIN. A sidebar on the left contains navigation options: My Protect, Emails, Expéditeurs, Rapports d'emails stoppés, and Délégation. The main area is titled 'Emails (80)' and features a search bar, a 'Recherche avancée' button, and a 'Gérer les colonnes' dropdown. Below this, there are filter tabs for 'En attente', 'Newsletters', 'Spearphishing', 'Bannis', 'Spams', and 'Infectés'. A notification banner reads: 'Restez vigilant face aux emails suspects. Des caractéristiques potentiellement dangereuses ont été identifiées lors du filtrage de ce type d'email. Comment réagir face à un email suspect?'. Below the notification is a table of emails with columns for 'Expéditeur', 'Objet', and 'Date'. The table lists several emails, some marked as 'suspect'. At the bottom, there's a pagination control showing 'Afficher 20 éléments par page. (20/XXX)' and a page navigation bar with numbers 1, 2, 3, 4, and a 'Go to page' button.

Rapport d'emails stoppés

Visualisez les bénéfices de Protect Advanced **depuis votre boîte mail**.
D'un coup d'œil, voyez les emails bloqués, les menaces évitées, et récupérez les emails importants ou gérez les expéditeurs en un clic.

The screenshot shows the 'Rapport d'emails stoppés' interface. At the top, there's a header with the 'U-mail BY MAILINBLACK' logo. The main content starts with a greeting 'Bonjour Owen,' and a message: 'Voici votre dernier rapport d'emails stoppés :'. Below this is an 'Information importante' section with a warning icon and text: '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.' The next section is 'Vos données sur le mois de juin', which includes two summary cards: 'Vos emails reçus' (38 valid, 30 stopped) and 'Temps gagné*' (12h 35min). Below these are four category cards: 'Spearphishings' (10), 'Spams' (2), 'Infectés' (3), and 'Bannis' (15). A section titled 'email@mailinblack.com - 1 email(s) en attente' has an 'Accéder à mon espace' button. Below that is an email preview from 'noreply@email.teams.microsoft.com' with a subject 'Guillaume Dreyfuss dans Hangout' and a message snippet. At the bottom, there are three buttons: 'Récupérer', 'Autoriser', and 'Bannir'. A final notification at the bottom says: 'Vous avez également reçu 4 spams et 1 virus. Accéder à mon espace'.

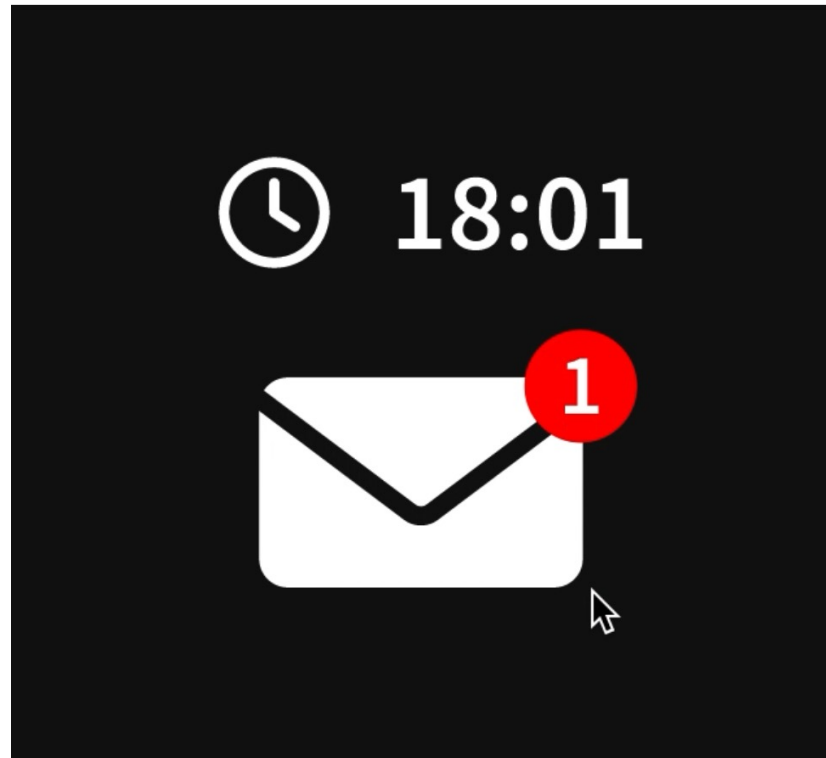


Droit à la Déconnexion



Le Droit à la Déconnexion

Activable selon vos besoins, la fonctionnalité de droit à la déconnexion incluse dans U-mail Advanced **préserve l'équilibre personnel** de vos collaborateurs.



Bien-être numérique

Permet à vos collaborateurs de se déconnecter en toute sérénité avec des **notifications automatiques** pour les emails envoyés **en dehors des horaires de travail**.

Gestion personnalisée

Pilotez et paramétrez la fonctionnalité pour l'organisation ou des **groupes spécifiques**, avec des **plages horaires sur mesure** et un **contenu d'email personnalisé**.

Une activation du service adaptée à votre infrastructure

100% compatible avec votre messagerie

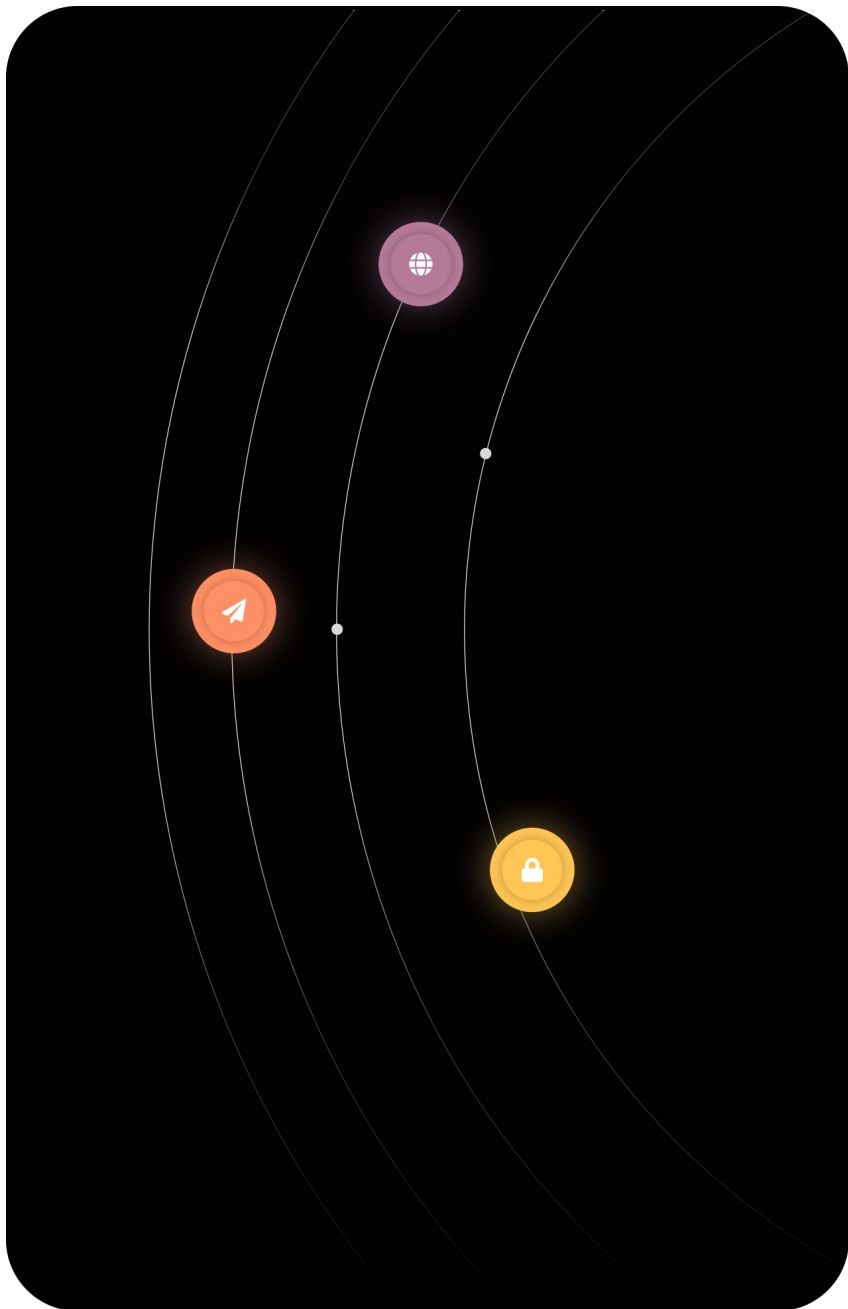


activation
CLOUD

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

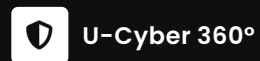


Contactez-nous

✉ contact@mailinblack.com

☎ +33(0)4 88 60 07 80

🌐 www.mailinblack.com



L'offre de cybersécurité complète pour couvrir le risque humain



Lauréat Grand Défi
Cybersécurité



Conformité RGPD



Labellisé Cybersecurity
Made In Europe



Catalogue
Tech.Gouv



Certification
ISO 27001

EN COURS



Certification
EN 17640

Notre histoire

Société française, Mailinblack dédie ses compétences humaines et ses ressources technologiques à la sécurité des organisations.

Après plus de 20 ans d'expertise, Mailinblack est positionné comme un leader sur le marché de la cybersécurité.

120 collaborateurs

13 pôles d'expertises

+20^{ans}

d'expertise en
cybersécurité

24 000

organisations protégées
par Mailinblack

96%

de nos clients
renouvellent

Notre mission

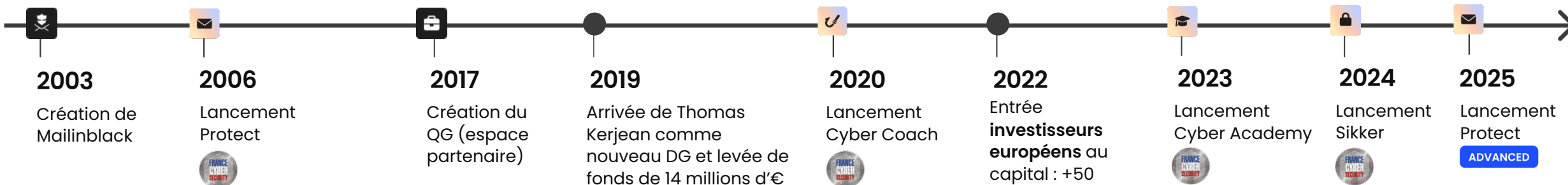
Démocratiser l'accès à la cybersécurité sur la base de **4 piliers** :

Pédagogie

Simplicité

Performance

Coût



U-CYBER 360°

Une protection centrée sur l'utilisateur à la pointe de l'innovation

Cockpit | Votre cockpit de pilotage du cyber-risque humain

Préparez-vous à relever tous les défis de la cybersécurité en protégeant votre entreprise de manière proactive

- ✓ CyberScore humain
- ✓ Conseils & remédiation
- ✓ Retour sur investissement

74%

Combinaison de données

A B C D E F

Composants du dashboard: un arc progressif à 74%, un radar à 4 axes, une grille de lettres A-F, un diagramme de réseau, une ligne de tendance et un diagramme à barres.

Sikker
Gestionnaire de mots de passe

Cyber Coach
Simulateur de cyberattaques

Cyber Academy
Formation cybersécurité

Protect
Protection des messageries

Copilote | L'agent Cyber dédié à vos collaborateurs