YAGO

Réduisez vos risques (et votre prime) cyber en 90 jours

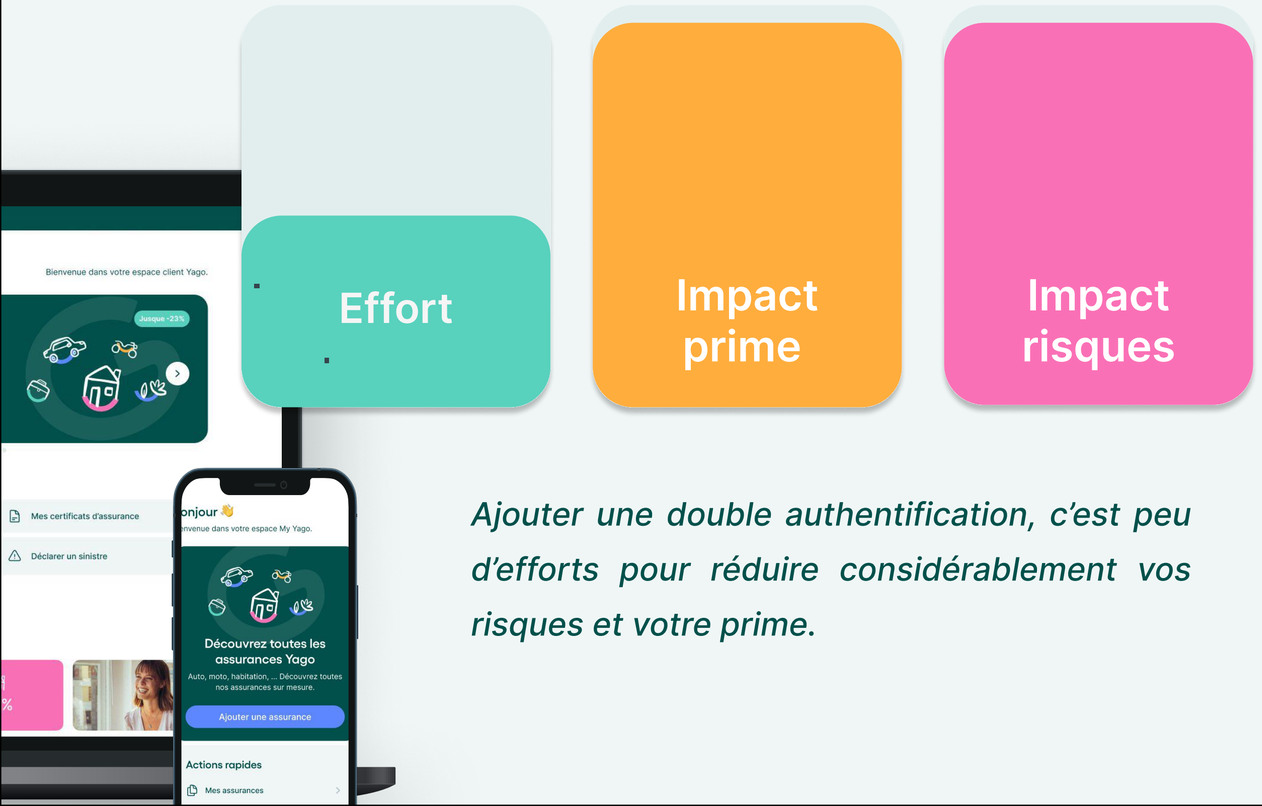
10 contrôles ultra concrets et faciles à implémenter

1. Faites votre auto évaluation en suivant la checklist
2. Priorisez les points selon une matrice impact sécurité/prime VS effort à founir
3. Contactez votre courtier d’assurance pour en discuter avec votre checklist à l’appui

1

Mettre en place une double authentification (MFA) partout !

Ajoutez un code (app/TOTP/clé physique) à chaque mot de passe critique.



Ajouter une double authentification, c'est peu d'efforts pour réduire considérablement vos risques et votre prime.

Le conseil Yago :

Comment mettre en place la double authentification ?

Il faut s'assurer auprès de votre CTO ou de la personne chargée de la sécurité et de l'informatique que **la double authentification est obligatoire sur tous les comptes** (messagerie, saas, outils critiques, cloud...). Elle ne doit pas être une option. Dans l'idéal privilégiez des applications d'authentification comme Google Authenticator, Microsoft Authenticator ou Authy.

Pour justifier de cela auprès de votre assureur, vous pouvez montrer des **captures d'écran** qui prouvent que le **MFA est "obligatoire"** et que **le taux d'activation est de 100%.**

Quel outil utiliser ?

Microsoft Authenticator

Google Authenticator

Authy Authenticator

2 Installer un antivirus/EDR sur tous les postes/serveurs

Détectez en temps réel et bloquez les comportements malveillants.

Le conseil Yago :

Pourquoi et comment installer un antivirus et un EDR?

Avoir un **bon anti-virus bien à jour sur tous les postes de votre entreprise** est indispensable pour limiter les logiciels malveillants (ransomwares) et les intrusions, et cela est souvent demandé par les assureurs. Cependant, **l'antivirus étant souvent insuffisant seul**, de plus en plus d'assureurs attendent également qu'un **EDR** soit installé pour compléter votre protection. Vous devez demander à votre responsable informatique de l'installer sur tous les postes et serveurs, si ce n'est pas déjà le cas. Il devra alors activer des politiques de sécurité claires et s'assurer de les mettre à jour régulièrement ainsi que d'activer les alertes. Enfin, il faudra **corriger les machines « non couvertes » en 48 h et vérifier les licences**. Demandez également un rapport mensuel de couverture sur qui est protégé et qui ne l'est pas (pour vous assurer que 100% des postes sont protégés).Vous pourrez utiliser ce rapport mensuel à votre assureur pour prouver votre protection ainsi que les actions mises en place pour conserver votre protection.

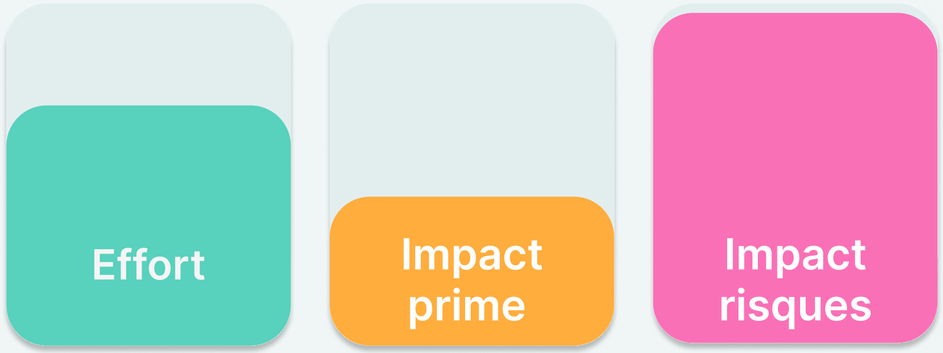
Vos outils : antivirus + logiciel EDR

McAfee · norton · Bitdefender · Microsoft Defender

Adopter un EDR et un antivirus, c'est fournir un effort élevé mais cela réduit considérablement les risques.

3 Implémenter un gestionnaire de mots de passe

Implémenter un gestionnaire de mots de passe c'est bénéficier d'un coffre-fort centralisé, d'un partage sécurisé, et d'une rotation et audit.



Migrer mots de passe partagés vers un gestionnaire peut considérablement réduire les risques de cyberattaques.

Le conseil Yago :

Comment mettre en place un gestionnaire de mot de passe ?

Il faut s'assurer auprès de la personne chargée de la sécurité et de l'informatique dans votre entreprise qu'un **gestionnaire de mots de passe d'entreprise** (type 1Password) est installé pour centraliser les mots de passe et garantir qu'ils sont uniques pour chaque compte. Assurez-vous que ce système est utilisé par l'ensemble des collaborateurs, qu'aucun mot de passe n'est stocké ailleurs que dans le logiciel, que les mots de passe sont suffisamment longs et complexes, et que leur partage est strictement restreint. Pour y parvenir, **migrez tous les mots de passe en les séparant par équipes** (Finance, Ops, Commercial, Marketing…), afin que chaque équipe n'ait accès qu'aux mots de passe qui lui sont utiles. Pour justifier cela auprès de votre assureur, vous pouvez montrer quel logiciel est en place, les politiques de complexité appliquées et la preuve que tous les mots de passe ont été migrés.

Votre outil : gestionnaire de mot de passe

Par exemple : 1Password

4

Mettre en place des sauvegardes “immuables”

Faire des copies non modifiables/supprimables et effectuer des test de restauration réguliers est crucial pour votre cybersécurité !

Le conseil Yago :

Pourquoi faut-il effectuer des sauvegardes immuables ?

Il est indispensable de **faire régulièrement des sauvegardes de vos données qu'on ne peut ni supprimer ni modifier** mais qui peuvent être restaurées pour vous protéger contre un ransomware ou des erreurs humaines. Dans l’idéal, **activez l’immutabilité sur votre stockage cloud** avec une rétention de 30–90 jours et conservez des copies hors ligne ou sur un site séparé. Pour justifier cela auprès de votre assureur, vous pouvez montrer des captures d’écran prouvant que l’immutabilité est active avec la durée de rétention, ainsi que le rapport de test de restauration (date, durée, résultat).

Migrer les mots de passe partagés vers un gestionnaire peut considérablement réduire les risques cyber.

5 Effectuer des mises à jour rapides (< 30 jours)

Faites des patch de failles critiques et des inventaires réguliers !

Les mises à jour régulières représentent un effort conséquent mais réduisent aussi considérablement les risques et permettent fréquemment d'obtenir des réductions sur votre prime cyber.

Le conseil Yago :

Comment et pourquoi faire des mises à jour rapides ?

Pensez à **installer des correctifs de sécurité pour corriger les vulnérabilités, les bugs ou les failles**. Les assureurs sont attentifs à votre vitesse de correction. L'idéal serait que les failles critiques soient corrigées en moins de 14 jours et pour les failles restantes, en moins de 30 jours.

Nous vous conseillons de tenir un **inventaire des machines et des logiciels** pour vous simplifier la tâche.

Pour justifier cela auprès de votre assureur, vous pouvez montrer **des rapports mensuels de patching** et de **non-conformités** ainsi qu'une liste des exceptions avec justification et date de correction prévue.

6 Favoriser le SSO et une activation/ désactivation rapide des comptes

Une identité, tous les accès; offboarding en un clic.

Le conseil Yago :

Pourquoi faut-il un SSO ?

Favorisez le SSO, afin qu'une seule identité permette de se connecter à plusieurs outils. Ne créez **qu'un accès par employé via son adresse e-mail** (ex : prenom.nom@entreprise).

Dans l'idéal, demandez à votre responsable RH d'utiliser un **outil adapté** (ex : Personio, BambooHR, Lucca...) **pour gérer les profils** (création, modification, suppression). Demandez à votre responsable IT d'**automatiser l'activation/désactivation des comptes depuis le dossier RH** afin que, 5 minutes après la demande de votre responsable RH, le profil de l'employé soit désactivé.

Vous pourrez utiliser la liste des applications branchées au SSO, la procédure d'offboarding et la capture horodatée d'un test réel comme justifications auprès de votre assureur.

Vos outils

Personio bambooHR

Un SSO, c'est la garantie de réduire les risques et diminuer votre prime d'assurance.

7 Centraliser les logs + mettre en place des alertes

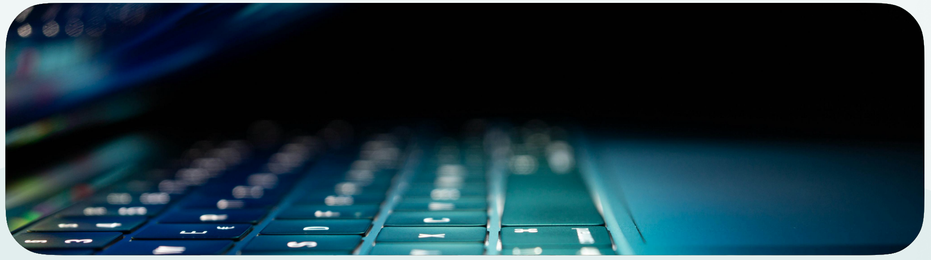
Conserver 12 mois de logs et implémenter des alertes en cas d'activité suspecte.

Effort

Impact prime

Impact risques

Des logs centralisés et les alertesmises en place permettent de réduire considérablement les risques.



Le conseil Yago :

Comment centraliser les logs ?

Une bonne pratique est de **conserver au même endroit les journaux (logs) des outils principaux (Microsoft 365/Google, VPN, serveurs, cloud…) pendant 12 mois**, avec des alertes en cas d'activité anormale.

Dans l'idéal, votre équipe IT devrait **configurer des alertes sur les connexions administrateurs, les échecs répétés, la désactivation du MFA et les élévations de privilèges**. De cette façon, vous pourrez détecter les éventuels incidents et enquêter rapidement.

Pour justifier cela auprès de votre assureur, vous pouvez montrer des c**aptures d'écran de la configuration d'export des logs ainsi qu'un rapport prouvant la rétention 12 mois et des alertes test.**

8 Mettre en place un réseau cloisonné (segmentation)

Il faut accorder les accès nécessaires uniquement aux collaborateurs qui en ont besoin.

Le conseil Yago :

Comment et pourquoi se protéger en mettant en place un réseau cloisonné?

Pour éviter à une cyber attaque de se propager partout, il est primordial de séparer votre réseau en zones. De cette façon, tout le monde n'a pas accès à tout.

Assurez-vous au minimum que la bureautique est séparée de la production, des utilisateurs, des serveurs et forcez l'administration à **passer par un bastion/VPN.**

Votre équipe IT doit appliquez une règle par défaut "tout bloquer puis n'autoriser que les flux nécessaires", s'assurer de fermer les ports inutiles et limiter les accès d'administration à des adresses IP connues en imposant également le **MFA** (Multi-Factor Authentication). Le but est que chaque collaborateur n'ait accès qu'à ce dont il a besoin, et rien d'autre, quelque soit son niveau de hiérarchie.

Il sera pertinent de présenter à votre assureur un schéma d'un réseau simple avec les différentes zones établies ainsi qu'un export des règles principales et preuves de restrictions sur l'administration

Vos outils : VPN + MFA

ProtonVPN CyberGhost NordLayer® +

Mettre en place un réseau cloisonné permet de diminuer la prime et les risques cyber.

9 Exercices de simulation d’incidents (1/an)

Rôles, contacts, délais en cas d’incident cyber…il s’agit de mettre en place les bons réflexes pour agir vite le jour d’une cyber attaque.

Effort	Impact prime	Impact risques

Les exercices et les simulations sont très efficaces pour réduire les risques cyber.

Le conseil Yago :

Pourquoi faut-il réaliser des exercices de simulation ?

Une bonne pratique à avoir serait **d'implémenter des entraînements, une fois par an, où vous simulez (de façon réaliste) une cyberattaque**. Le but est de savoir **qui fait quoi, qui appelle qui et ça en combien de temps**. De cette façon, les différents collaborateurs sauront comment agir rapidement et efficacement en situation réelle.
Un **compte-rendu** avec des axes d'améliorations (3-5 actions), des responsables, des dates vous permettra de montrer que votre équipe est préparée à ce genre de situations. Cela rassurera non seulement votre assureur mais aussi votre conseil d'administration.

10 Faire des formations de sensibilisation annuelle

Réduire le risque humain (phishing, mots de passe, pièces jointes).

Le conseil Yago :

A quel point les formations sont-elles utiles pour votre cybersécurité?

Formez tous les employés aux risques de base (phishing, mots de passe, pièces jointes), avec des rappels et des tests réguliers. En effet, environ 90% des incidents commencent par une erreur humaine ! De plus, vous montrez à votre assureur que vous travaillez à réduire le risque directement.

Concrètement, demandez à votre RH et/ou DSI/IT de superviser l'apprentissage par un module e-learning court pour 100% des équipes, à refaire annuellement. Pour accompagner ces modules, un t**ableau de suivi des complétions par équipe** peut permettre de prévenir et suivre les risques. Au niveau de l'entreprise, une campagne de phishing simulé avec des indicateurs (taux de clics, signalement) peut également jouer en faveur de la cybersécurité à long terme.

Notre conseil : évitez les formations one shot sans véritable suivi et n'exemptez pas les managers de formation : il est tout aussi important qu'il se forment sur les enjeux de la cybersécurité pour superviser leur équipe.

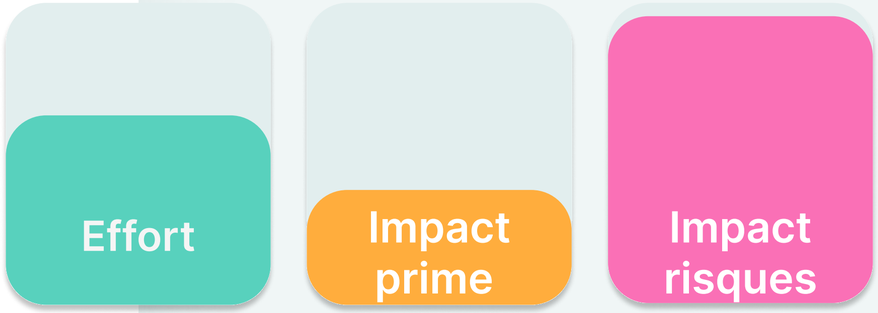
Présentez ensuite à votre assureur le taux de complétion de la formation (visez un taux supérieur à 95%) et le résultat des simulations afin qu'il le prenne en compte dans le calcul de la prime

Vos outils : modules e-learning

BUREAU VERITAS

NEO ACADEMIE !

LAMY LIAISONS Académie



Former les équipes est clef dans la réduction des risques cyber.

Vous avez completé notre checklist?

Bravo, votre prime et les risques cyber sont efficacement réduits

- Mettre en place une double authentification (MFA) partout !
- Installer un antivirus/EDR sur tous les postes/serveurs
- Implémenter un gestionnaire de mots de passe
- Mettre en place des sauvegardes “immuables”
- Effectuer des mises à jour rapides (< 30 jours)
- Favoriser le SSO et une activation/ désactivation rapide des comptes
- Centraliser les logs et mettre en place des alertes
- Mettre en place un réseau cloisonné (segmentation)
- Faire des exercices de simulation d’incidents (1/an)
- Faire des formations de sensibilisation annuelles

A propos de Yago

Vos assurances entreprise, enfin simples. Yago est le courtier en assurance qui simplifie la gestion de vos polices d'assurance et vous offre un service rapide et expert en cas de sinistres.

- **Bénéficiez de l'expertise Yago**

  Des assurances adaptées à votre entreprise et à vos besoins.

- **Libérez-vous de la paperasse grâce à votre espace My Yago**

  Consultez et modifiez vos contrats en ligne & suivez vos sinistres en temps réel.

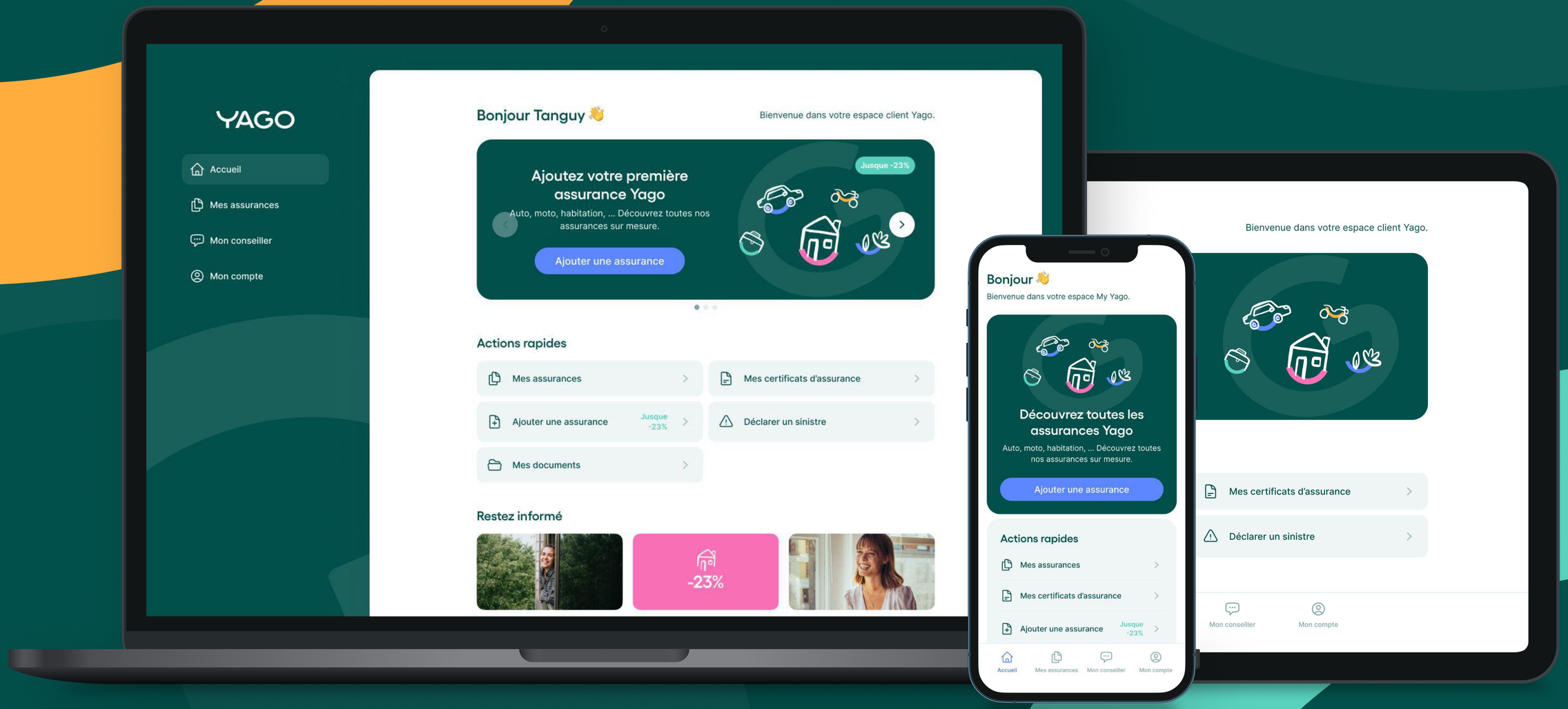
- **Profitez de votre conseiller dédié 100% à vos côtés**

  Il connaît votre dossier, et répond à toutes vos questions dans les 4 à 8 heures ouvrables.

Réservez votre audit gratuit d'assurance.

Nous auditons vos contrats existants et identifions les optimisations possibles. Vous découvrez aussi les facilités de la plateforme Yago.

Rencontrer mon conseiller Yago


YAGO
Accueil
Mes assurances
Mon conseiller
Mon compte
Bonjour Tanguy 👋
Bienvenue dans votre espace client Yago.
Ajoutez votre première assurance Yago
Auto, moto, habitation, ... Découvrez toutes nos assurances sur mesure.
Ajouter une assurance
Jusque -23%
Actions rapides
Mes assurances
Mes certificats d'assurance
Ajouter une assurance
Jusque -23%
Déclarer un sinistre
Mes documents
Restez informé
-23%
Bienvenue dans votre espace client Yago.
Mes certificats d'assurance
Déclarer un sinistre
Mon conseiller
Mon compte
Bonjour 👋
Bienvenue dans votre espace My Yago.
Découvrez toutes les assurances Yago
Auto, moto, habitation, ... Découvrez toutes nos assurances sur mesure.
Ajouter une assurance
Actions rapides
Mes assurances
Mes certificats d'assurance
Ajouter une assurance
Jusque -23%
Accueil
Mes assurances
Mon conseiller
Mon compte

YAGO

yago.be