Rapport annuel de **sécurité**

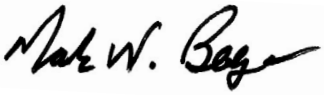
EQUIFAX®

Table des matières

> Nous avons véritablement construit l'un des programmes de cybersécurité les plus avancés et les plus efficaces au monde. En même temps, nous reconnaissons que notre travail en matière de sécurité n'est jamais terminé.
>
> – Mark Begor

Un message du président-directeur général d'Equifax

Mark Begor



Mark W. Begor

Président-directeur général
Equifax

L'année 2024 a marqué un chapitre stimulant de transformation et de croissance pour la nouvelle Equifax. Nous avons réalisé des progrès importants dans la finalisation de notre transformation des données et de la technologie. Alors que nous regardons vers l'avenir, nous nous appuyons sur la base solide du nuage Equifax[MC] et de nos capacités de l'IA.EFX pour stimuler l'innovation, les nouveaux produits et la croissance future. Il est important de noter qu'une cybersécurité renforcée est au cœur de chacune de nos actions commerciales.

Lorsque j'ai rejoint Equifax en 2018, je me suis personnellement engagé à faire d'Equifax un chef de file de l'industrie en matière de sécurité des données et à bâtir une culture où la sécurité est l'affaire de chacun et s'inscrit dans l'ADN de notre équipe mondiale. Depuis, nous avons transformé notre organisation à tous les niveaux pour tenir cette promesse. En 2024, notre programme de cybersécurité a atteint un niveau de maturité supérieur à toutes les principales références du secteur, pour une cinquième année consécutive. Notre score en matière de posture de sécurité continue de dépasser les moyennes du secteur de la technologie et des services financiers.

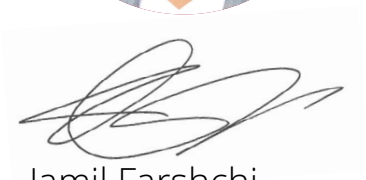
Avec la publication de notre cinquième rapport annuel sur la sécurité, nous célébrons les progrès en matière de sécurité accomplis à ce jour. Nous avons véritablement construit l'un des programmes de cybersécurité les plus avancés et les plus efficaces au monde. En même temps, nous reconnaissons que notre travail en matière de sécurité n'est jamais terminé.

L'année 2024 a aussi été marquée par une multitude de nouvelles menaces pour l'infrastructure mondiale de cybersécurité. L'année dernière, nous avons répondu à plus de 15 millions de cybermenaces, soit près de 175 tentatives hostiles à chaque seconde et une augmentation de 25 % par rapport à 2023. Rester en avance sur ces menaces nécessite d'évoluer, d'innover et de penser différemment. C'est la raison pour laquelle je suis fier d'initiatives telles que notre transformation sans mot de passe à la pointe de l'industrie et notre déploiement de technologie sans mot de passe au sein d'Equifax, y compris l'utilisation de la biométrie, pour aider à éliminer la menace numéro un à laquelle sont confrontées les équipes de sécurité : le vol d'identifiants.

Alors que nous envisageons l'avenir d'Equifax, la sécurité reste une priorité commerciale stratégique essentielle. Nous continuerons à développer et à faire évoluer notre posture et nos programmes de sécurité pour répondre aux menaces de cybersécurité en constante évolution et les anticiper. Nous continuerons à communiquer de manière transparente sur nos initiatives en matière de sécurité, en partageant les leçons apprises au profit de l'industrie dans son ensemble.

Un message du chef des technologies et de la sécurité de l'information

Jamil Farshchi



Jamil Farshchi

Chef des technologies
et chef de la sécurité
de l'information
Equifax

Nous entendons fréquemment qu'il est impossible de concilier une sécurité de haut niveau et une innovation rapide. En 2024, nous avons entrepris de briser ce mythe. Nous avons constaté une augmentation continue des menaces alimentées par l'intelligence artificielle et des tensions géopolitiques, rendant le paysage de la cybersécurité plus préoccupant que jamais, mais nous n'avons pas cédé à l'immobilisme. Nous avons modernisé nos défenses, accéléré l'adoption du nuage et repoussé les limites en nous attaquant à la cause la plus importante des violations de données : les identifiants compromis.

En effet, cette année, nous avons déployé l'authentification sans mot de passe pour l'ensemble de notre personnel, soit près de 22 000 employés et contractuels, pour environ 300 applications internes. Cette initiative audacieuse visait non seulement à nous protéger du vol de mots de passe, mais aussi à réduire considérablement les coûts du service d'assistance, d'améliorer la productivité du personnel et de renforcer nos défenses contre les techniques d'usurpation d'identité basées sur l'intelligence artificielle, comme le clonage vocal. D'un seul coup, nous avons amélioré l'expérience utilisateur et les résultats en matière de sécurité.

Chez Equifax, nous ne croyons pas au compromis entre la sécurité et la rapidité. Nos résultats parlent d'eux-mêmes : en 2024, nous avons lancé plus de 100 innovations de nouveaux produits (INP) tout en maintenant un score de maturité en matière de sécurité qui a, une fois de plus, surpassé les principales références de l'industrie. Le rapport annuel sur la sécurité de cette année est le cinquième consécutif, ce qui témoigne de notre engagement en faveur de la transparence, de la collaboration et de l'amélioration continue.

Tout au long de ce parcours, nous avons rendu public notre cadre de contrôle, exposé notre posture de sécurité infonuagique en temps réel à nos clients grâce au Contrôle infonuagique, renforcé nos partenariats publics et privés, et partagé nos connaissances avec l'ensemble de la communauté.

Suis-je satisfait? Absolument pas. Nous savons que les adversaires améliorent constamment leur jeu, en exploitant les vulnérabilités du jour zéro, les faiblesses de la chaîne d'approvisionnement et, plus récemment, l'IA, pour s'infiltrer. Notre réponse est de redoubler d'efforts en matière de sécurité. La sécurité n'a plus rien à voir avec un ralentissement des activités : elle est devenue un élément essentiel pour propulser notre élan et notre croissance.

En 2024, les clients ont cité notre réputation en matière de sécurité comme l'une des principales raisons pour lesquelles ils ont choisi Equifax. La rapidité et la stabilité de nos produits ont atteint un niveau record l'année dernière. Nous avons encore beaucoup à accomplir, mais une chose est claire : **la sécurité et l'innovation ne s'excluent pas mutuellement.**

Alors que nous tournons notre regard vers l'avenir, nous continuerons de repousser les limites, de rejeter les idées dépassées et de faire ce qu'il faut pour être les meilleurs dans la défense des données des consommateurs *et* pour permettre une innovation audacieuse chez Equifax. Merci d'être avec nous dans ce parcours.

Notre impact

La sécurité chez Equifax en 2024

Plus de 15 millions

de cybermenaces repoussées chaque jour, près de 175 tentatives hostiles chaque seconde, soit une augmentation de 25 % par rapport à l'année dernière.

Plus de 210 000

simulations lancées pour tester notre main-d'œuvre mondiale sur divers scénarios de sécurité.

Environ 22 000

employés et contractuels formés avec des modules de sécurité personnalisés, atteignant notre taux de clics le plus bas jamais enregistré (2,9 %) dans les simulations d'hameçonnage ciblées.

Plus de 3 550

questionnaires et vérifications clients réalisés pour renforcer la confiance dans notre posture de sécurité.

Plus de 4 200

utilisateurs externes ont accédé à notre cadre de contrôles de sécurité et de confidentialité dans plus de 80 pays.

Plus de 2 250

analyses approfondies des risques sur les fournisseurs tiers critiques et à haut risque, ce qui a permis de cibler des failles de sécurité potentielles avant qu'elles soient exploitées.

Plus de 700

organisations soutenues par les services liés aux brèches d'Equifax, offrant une protection d'identité à plus de 22 millions de victimes de brèches à l'échelle mondiale.

Plus de 450

professionnels dédiés à la cybersécurité qui protègent les données des consommateurs 24 heures sur 24.

Plus de 370

vérifications de sécurité automatisées du nuage surveillées en temps réel, alimentant une réponse plus rapide aux menaces et une connaissance quasi instantanée de la posture de sécurité.

Plus de 100

innovations de nouveaux produits mises sur le marché en toute sécurité, prouvant que vitesse et sécurité ne sont pas incompatibles.

51

certifications et autorisations obtenues auprès de vérificateurs externes, validant notre profondeur et notre rigueur.

38

évaluations de sécurité physique réalisées pour protéger nos collaborateurs, nos données et nos actifs.

Plus de 30

forums auxquels nous avons participé à l'échelle mondiale pour partager des renseignements et renforcer les défenses collaboratives.

15

exercices théoriques simulant des scénarios de crise avec la haute direction et des équipes régionales.

5

années consécutives avec un score de maturité en matière de sécurité qui surpasse toutes les principales références du secteur.

2

intégrations d'acquisitions complétées en vertu d'un nouveau plan de sécurité simplifié.

Moins de 1

minute en moyenne pour détecter des cybermenaces — nous ne laissons pas les adversaires s'attarder.

État des lieux

La cybersécurité en 2024

Les thèmes ci-dessous représentent les thèmes prédominants de l'année passée, et la façon dont Equifax y a répondu.

Vitesse d'attaque de la chaîne d'approvisionnement

En 2024, les attaques contre les chaînes d'approvisionnement ont augmenté en fréquence et en sophistication, alimentées par notre dépendance aux systèmes interconnectés. La compromission d'un seul fournisseur peut toucher des écosystèmes entiers, avec des dommages estimés à 138 milliards de dollars par an à l'échelle mondiale d'ici à 2031.[1]

Notre approche? Confiance zéro, unification du cadre de sécurité des fusions et acquisitions, et extension de la visibilité en temps réel sur les risques liés aux tiers. Nous essayons également d'aider là où Equifax est le tiers. Grâce à notre tableau de bord Contrôle infonuagique, les clients bénéficient d'un aperçu continu de la sécurité des produits du nuage Equifax[MC], leur donnant ainsi les informations dont ils ont besoin pour prendre des décisions éclairées en matière de risques.

Vol d'identifiants + piratage psychologique alimenté par l'IA

Tout au long de l'année 2024, les attaquants ont intensifié l'usurpation d'identité basée sur l'IA, comme les voix hypertruquées, l'hameçonnage réaliste et le piratage psychologique ciblé, afin d'exploiter le facteur humain. Le vol d'identifiants représente déjà la majorité des violations de données, mais l'usurpation vocale a fait de la fraude au service d'assistance une menace majeure.

Equifax a directement abordé cette problématique en déployant l'authentification sans mot de passe pour près de 22 000 employés et contractuels, éliminant ainsi un des principaux vecteurs de violations d'aujourd'hui. Nous avons également mis en œuvre un système sans mot de passe pour les appels au service d'assistance, atténuant ainsi l'une des principales cybermenaces émergentes : le clonage vocal basé sur l'IA. En combinant les principes de la confiance zéro et plus de 210 000 simulations de piratage psychologique pour notre personnel, nous nous sommes engagés à fond pour nous défendre contre les principaux risques d'aujourd'hui et de demain.

Vulnérabilités du jour zéro et exploits d'infrastructure

Avec l'essor de la découverte de vulnérabilités assistée par l'IA, les exploits de type « jour zéro » ont ciblé à la fois les piles logicielles de base et les équipements de réseau. Les criminels ont exploité des vulnérabilités récemment découvertes, souvent vendues sur des marchés clandestins, pour implanter des rançongiciels ou établir des points d'appui furtifs. De nombreuses entreprises ont eu du mal à mettre à jour les correctifs assez rapidement, renforçant ainsi l'importance de principes fondamentaux tels qu'une analyse cohérente et des protocoles de mise à jour complets.

Nous avons répondu en intensifiant la couverture de surveillance continue, en appliquant des correctifs de périmètre de manière proactive et en réduisant notre temps de réponse à quelques minutes, empêchant ainsi les attaquants de tirer parti de ces vulnérabilités.

L'évolution des rançongiciels

Les attaques par rançongiciels ont évolué au-delà du simple cryptage des données en 2024. Les pirates ont perfectionné les attaques en plusieurs étapes, arrêtant les opérations, volant des données, utilisant des techniques de double ou triple extorsion… allant même jusqu'à essayer de simuler une brèche pour forcer le paiement. Une seule attaque à grande échelle peut entraîner d'innombrables pertes et avoir un impact négatif sur les temps d'arrêt et la récupération.

Chez Equifax, nous controns les adversaires avec des mécanismes de défense superposés, une détection avancée des points d'extrémité, la priorisation automatisée des correctifs, une architecture de confiance zéro et des processus de sauvegarde robustes. Rien de tout cela n'est parfait, mais nous travaillons sans relâche pour nous améliorer continuellement dans tous les domaines.

[1] Ventures de cybersécurité. Software Supply Chain Attacks To Cost The World $60 Billion By 2025, Newswires, 3 octobre 2023. https://world.einnews.com/pr_news/659375862/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025

Nos actions

Initiatives d'Equifax et résultats en matière de sécurité en 2024

Renforcement de notre culture de la responsabilité en matière de sécurité

Nous avons optimisé les processus pour que nos employés et contractuels placent la sécurité en tête de leurs priorités, en augmentant la formation et en supprimant les points de friction.

Nos employés et nos contractuels excellent dans la reconnaissance et l'évitement des liens suspects. Nous avons effectué plus de 210 000 simulations mondiales d'hameçonnage, atteignant notre taux de clics le plus bas jamais enregistré pour les courriels d'hameçonnage simulés.

Nous avons rendu les connexions chez Equifax plus rapides et plus sécurisées que jamais en déployant une authentification sans mot de passe auprès de nos près de 22 000 employés et contractuels dans le monde, atténuant ainsi l'un des principaux vecteurs de menace pour la sécurité.

La sécurité est l'affaire de tous chez Equifax. Nous sommes tous responsables de la sécurité, et chacun de nos employés et contractuels est habilité et encouragé à en faire une priorité personnelle, ce qui favorise la confiance et la rapidité d'action.

Partenariat amélioré en matière de technologie et de sécurité

En 2024, nous avons tout mis en oeuvre pour renforcer le partenariat entre nos fonctions Technologie et Sécurité.

Nous avons fusionné l'infrastructure technologique avec les opérations de sécurité, ainsi que la continuité des activités et la reprise après sinistre avec la gestion des crises de sécurité, **unifiant ainsi notre capacité d'exécution et de réaction.**

Contrairement au mythe selon lequel la sécurité étouffe l'innovation, nous avons lancé plus de 100 INP en 2024, avec une sécurité intégrée dès la conception.

Ces optimisations, ainsi que d'autres, ont assuré une **exécution plus transparente et plus efficace,** libérant des synergies qui permettent à la sécurité d'accélérer (au lieu de ralentir) les lancements de produits.

Excellence opérationnelle avancée

Nous avons continué à affiner nos outils, nos données et nos ressources pour maximiser leur impact.

Grâce aux améliorations basées sur l'IA, nous avons accéléré les tests d'intrusion, les examens des applications et l'analyse des journaux pour une meilleure détection des menaces, tout en maintenant une surveillance humaine.

L'accent que nous avons mis sur l'amélioration continue a donné des résultats significatifs. Notre équipe de cybersécurité a **réduit les temps de réponse aux menaces de 60 à 99 % d'une année à l'autre,** mesurés par le temps nécessaire pour détecter les incidents, y répondre et les résoudre.

De même, notre Centre de gestion de la sécurité physique a rationalisé les processus et tiré parti de l'automatisation pour obtenir une amélioration de **33 % du temps de réponse aux alarmes locales hautement prioritaires,** qui est désormais inférieur à deux minutes en moyenne.

Suite

Initiatives d'Equifax et résultats en matière de sécurité en 2024

Réduction des risques liés à la chaîne d'approvisionnement

Nous avons amélioré la sécurité de notre chaîne d'approvisionnement à tous les niveaux.

Nous avons inclus des indicateurs de la chaîne d'approvisionnement dans les aperçus mensuels de sécurité de nos employés, pour montrer leur importance d'une évaluation rigoureuse des liens et des relations avec les fournisseurs pour protéger Equifax.

De plus, nous avons réorganisé les validations de sécurité de nos fournisseurs en mesurant de nouveaux points de données qui révèlent comment les tiers gèrent les risques émergents.

Afin d'améliorer l'accès des clients aux produits d'Equifax et leur visibilité, nous avons lancé la version mobile de notre tableau de bord Contrôle infonuagique, une solution unique en son genre qui fournit de l'information continue sur la posture de sécurité des produits du nuage Equifax[MC].

Collaboration externe à grande échelle

En 2024, nous avons continué à faire pression pour faire de la transparence et de la collaboration entre les entreprises et les gouvernements une norme mondiale.

Jamil Farshchi, chef des technologies et de la sécurité de l'information d'Equifax, a coanimé la nouvelle minisérie sur la cybersécurité du FBI avec le responsable de la division cybernétique du FBI, démystifiant ainsi le soutien des forces de l'ordre.

Notre équipe s'est associée aux gouvernements du Costa Rica et du Chili pour les aider à renforcer leur sécurité, comblant ainsi les écarts entre le public et le privé à l'échelle internationale.

Nous avons aussi continué à prôner une communication ouverte pour garder une longueur d'avance sur la prochaine génération de menaces mondiales.

Augmentation des résultats

Une bonne sécurité est bénéfique pour les résultats, et en 2024, nous avons contribué à la réalisation des objectifs de l'entreprise à tous les niveaux.

La sécurité n'est plus seulement une question de conformité de base. Elle contribue à générer de nouveaux revenus, car les **clients citent notre leadership en matière de sécurité comme l'une des principales raisons pour lesquelles ils ont choisi Equifax.**

Nous avons obtenu la certification du Data Privacy Framework, affirmant ainsi notre engagement à faciliter en toute sécurité les transferts internationaux de données de l'Union européenne vers les États-Unis.

Un plan pour éliminer les identifiants

Deuxième semestre 2023

Appel d'assistance technique

Norme de l'industrie	Notre approche
Contexte : L'industrie a observé une augmentation des attaques par piratage psychologique ciblant l'accès aux centres d'assistance Les cybercriminels ciblent les entreprises en se faisant passer pour des employés pour obtenir un accès privilégié. Ils trompent le personnel de soutien technique au téléphone et exploitent des questions de sécurité aux réponses facilement accessibles (par exemple, le nom de jeune fille de la mère). **Pas de solution unifiée prête à l'emploi** Il n'existait aucune solution unique permettant de remédier de manière fiable et durable à cette vulnérabilité.	**Nouvelle façon de s'authentifier pour les appels au soutien technique** Nous avons trouvé un fournisseur novateur et travaillé avec lui pour mettre au point la meilleure solution pour remédier à cette vulnérabilité : une solution de réponse vocale interactive (RVI) basée sur une application qui a permis aux employés de s'authentifier automatiquement lorsqu'ils appelaient le soutien technique d'Equifax. **Faciliter la transition des utilisateurs vers l'authentification sans mot de passe** Nous avons d'abord déployé cet outil pour l'accès au service d'assistance, afin de minimiser les interruptions de travail et d'éliminer un vecteur de risque important. Il sera ensuite utilisé pour les applications Web sans mot de passe et l'accès au RPV.

Premier semestre 2024

Ordinateurs portables et ordinateurs de bureau

Norme de l'industrie	Notre approche
Connexions basées sur un mot de passe Les utilisateurs accèdent aux ordinateurs portables et de bureau en s'identifiant avec la méthode traditionnelle du nom d'utilisateur et du mot de passe. **Aucune application tierce** Les connexions aux appareils dépendent entièrement des mécanismes d'authentification intégrés aux systèmes d'exploitation, sans l'intervention de solutions tierces. **Biométrie non activée** Les contraintes d'infrastructure empêchent l'utilisation généralisée de la fonctionnalité d'authentification biométrique.	**Modifications de la configuration de connexion à l'appareil** Nous avons aidé les utilisateurs à activer les connexions sans mot de passe aux postes de travail par authentification biométrique. **Déploiement progressif** Nous avons déployé cette méthode auprès de quelques centaines d'utilisateurs à la fois sur plusieurs mois, ce qui a permis un dépannage itératif et des communications personnalisées. **Fondation pour les composants ultérieurs** Ces changements de configuration étaient essentiels aux *futures* mises en œuvre d'applications sans mot de passe (applications Web et RPV).

Suite

Un plan pour éliminer les identifiants

Deuxième semestre

2024

Applications Web et RPV

Norme de l'industrie

Accès centralisé aux applications Web (SSO)
Les utilisateurs accèdent aux applications Web (comme la messagerie électronique, les outils de collaboration et d'autres systèmes critiques pour l'entreprise) au moyen d'un système central d'authentification unique (SSO).

Sécuriser les applications Web avec l'AMF (authentification multifacteur)
La signature unique est sécurisée par un mot de passe et une authentification multifacteur (AMF).

Sécuriser le réseau avec l'AMF
L'accès au réseau privé virtuel (RPV) est protégé par l'AMF. Les utilisateurs doivent saisir un mot de passe lors de la connexion au WiFi à distance puis de faire une vérification sur un appareil mobile.

Première étape cruciale
La connexion au RPV avec un mot de passe est la première étape pour accéder aux ressources de l'entreprise, ce qui rend les problèmes de mot de passe particulièrement perturbateurs.

Impact sur le personnel à distance
En raison de sa nature critique et de son impact sur le personnel à distance, la migration des systèmes vers un accès au RPV avec identifiants est susceptible de perturber les utilisateurs finaux.

Notre approche

Intégration d'un système sans mot de passe
Nous avons intégré notre système d'authentification unique (SSO) existant à un service d'authentification sans mot de passe, permettant aux utilisateurs de s'authentifier pour accéder au RPV et à certaines applications avec leurs appareils mobiles. Les postes de travail permettaient également des authentifications biométriques.

Choix volontaire et incitations
Nous avons commencé par offrir la possibilité aux utilisateurs de passer volontairement à l'authentification sans mot de passe. Par la suite, nous avons adopté une approche d'encouragement et de rappels avant que la méthode sans mot de passe devienne le choix par défaut.

Communication complète
La transition a été communiquée tôt et à plusieurs reprises sur de nombreux canaux (courriels, publications sur l'intranet, affichage numérique, etc.). Nos communications comprenaient des instructions techniques et une présentation des avantages. Nous nous sommes assurés que chaque employé comprend les avantages de la méthode sans mot de passe!

Collaboration

La clé pour une collaboration réussie

Les avantages d'un environnement sans mot de passe sont indiscutables. Les défis liés à la transition peuvent toutefois être intimidants. Il est difficile de changer des habitudes bien établies. La collaboration a été le multiplicateur de force qui a rendu cette transformation possible.

Co-innovation avec notre fournisseur

Nous avons vu le potentiel de la technologie sans mot de passe pour minimiser les risques et gagner en commodité. En gardant ces avantages à l'esprit, nous avons pris la décision réfléchie de soutenir le développement de cette technologie en établissant une boucle de rétroaction interactive avec notre fournisseur. Ce partenariat transformateur a permis des avancées (comme un nouveau processus de vérification par RVI pour les appels au soutien technique) qui contribuent désormais à favoriser l'adoption de la solution dans l'ensemble de l'industrie. D'autres organisations financières commencent déjà à s'engager dans cette voie, ce qui entraînera des améliorations systémiques de la sécurité tout au long de la chaîne d'approvisionnement mondiale.

Collaboration étroite des équipes de la technologie et de la sécurité

Cette initiative illustre parfaitement la valeur de l'excellente collaboration entre nos équipes de la technologie et de la sécurité. Elles ont collaboré étroitement de la planification jusqu'à l'exécution pour s'assurer que l'expérience utilisateur et la sécurité soient prises en compte à chaque étape de la transformation.

Un travail d'équipe

Chacun de nos employés et contractuels considère la sécurité comme une responsabilité personnelle, et leur engagement a été crucial pour le succès de cette transformation. Ils n'étaient pas des bénéficiaires passifs du changement : ils ont activement collaboré à sa mise en œuvre. Tout le personnel a adapté ses flux de travail quotidiens pour intégrer le nouveau système. Le changement exigeait une adaptation aux nouvelles méthodes d'authentification, l'adoption des connexions avec authentification biométrique et l'adoption de l'application d'authentification mobile. La volonté d'accepter le changement a permis une transition fluide et efficace, contribuant ainsi à renforcer notre sécurité.

Pas une « solution universelle »

Equifax est une entreprise mondiale et nos équipes régionales de sécurité et de technologie ont joué un rôle central. Elles ont non seulement aidé à déployer notre nouvelle technologie sans mot de passe, mais également contribué à responsabiliser l'ensemble de notre personnel. Elles ont fourni un soutien personnalisé, relevé des défis locaux uniques et proposé des programmes de formation sur mesure. Cette approche localisée a permis à chaque employé, quel que soit son emplacement, de se sentir soutenu et équipé pendant le processus de transition.

Nous sommes ravis de poursuivre cette collaboration en 2025 et pour les années à venir en organisant des séances d'échange des connaissances avec les clients et les partenaires qui souhaitent reproduire notre transformation commerciale sans mot de passe.

Analyse comparative indépendante

Maturité du système de sécurité

Nous travaillons en partenariat avec un grand cabinet mondial de recherche et de services-conseils pour réaliser une analyse objective approfondie de la maturité de l'ensemble de notre programme de sécurité.

Score de maturité de la sécurité

Qu'est-ce que la maturité du système de sécurité?

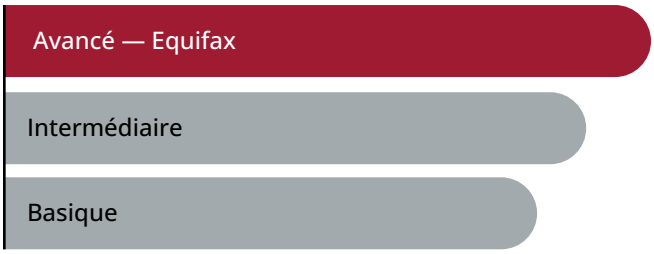
La maturité d'une organisation en matière de sécurité représente sa capacité à s'adapter aux cybermenaces et à gérer les risques au fil du temps.

Nous avons conservé notre position de chef de file en ce qui concerne la maturité de notre programme de cybersécurité en 2024, surpassant toutes les principales références du secteur pour la cinquième année consécutive.

Posture de sécurité

Un service de production de rapports sur la cybersécurité de premier plan surveille en permanence la posture de notre programme de sécurité et évalue le risque de notre écosystème de chaîne d'approvisionnement.

Évaluation de la posture de sécurité



Il s'agit des catégories de notation attribuées par le service des rapports qui effectue le suivi de notre posture. Equifax maintient une notation qui nous positionne dans la catégorie la plus élevée.

Qu'est-ce que la posture de sécurité?

La posture de sécurité d'une organisation correspond à son état de préparation et à sa capacité à détecter les menaces et les risques de sécurité, à y répondre et à s'en remettre.

Notre score en matière de sécurité a dépassé les moyennes du secteur de la technologie et des services financiers pour une quatrième année consécutive.

Résumé des résultats

La sécurité chez Equifax en 2024

Posture de sécurité et maturité

- A obtenu une cote de maturité de premier ordre pour l'exploitation d'un programme de sécurité harmonisé au cadre de cybersécurité du National Institute of Standards and Technology (NIST), surpassant toutes les principales références du secteur au cours des cinq dernières années.
- A obtenu une cote de posture de sécurité qui a dépassé les indices de référence du secteur des technologies pour une quatrième année consécutive.

Cybersécurité

- Contrôle en temps réel de 374 vérifications de sécurité dans le nuage, ce qui a permis d'améliorer la visibilité de notre posture.
- Authentification multifacteur renforcée (AMF) pour la totalité des accès à distance, réduisant ainsi les risques d'entrée non autorisée.
- Transition vers des connexions sans mot de passe pour nos près de 22 000 employés et contractuels dans le monde, neutralisant ainsi les menaces basées sur les identifiants.
- Amélioration des temps de réponse aux menaces de 60 à 99 % d'une année à l'autre, grâce à la détection basée sur l'IA, à l'optimisation des processus et à des renseignements intégrés sur les menaces.

Conformité

- Obtention de 51 certifications avec une réduction des coûts de 6 % d'une année à l'autre, ce qui a permis de réaliser des économies de 500 000 $ en 2024 seulement.

Fusions et acquisitions

- L'intégration de deux acquisitions antérieures a été presque achevée en utilisant notre cadre reproductible, avec 94 % des contrôles répondant aux normes d'Equifax.

Gestion des risques

- Réalisation d'analyses approfondies des risques sur la totalité des tiers à risque critique et élevé de notre entreprise (2 253).
- Évaluations des risques réalisées sur la totalité des applications de l'entreprise (6 308).
- Lancement d'une version mobile du Contrôle infonuagique pour une visibilité continue sur la posture de cybersécurité.

Confidentialité

- Implantation d'un nouvel outil de prévention de la perte de données pour les courriels, ce qui optimise la compréhension des utilisateurs et la protection de l'information.
- Publication d'une déclaration relative à confidentialité des données personnelles pour les candidats.
- Certification du Data Privacy Framework, permettant de transférer en toute sécurité des données de l'Union européenne et du Royaume-Uni vers les États-Unis.

Suite

La sécurité chez Equifax en 2024

Gestion de crise

- Réalisation de 15 exercices théoriques sur des simulations de crise en temps réel avec les parties prenantes de l'entreprise, notamment :
  – PDG et équipe de direction;
  – équipes de crise régionales et équipes de crise des unités commerciales.
- Introduction de nouveaux exercices de simulation axés sur la sécurité au travail, la reprise après sinistre et le formulaire 8-K. Un formulaire 8-K est un rapport qui doit être déposé auprès de la Securities and Exchange Commission des États-Unis pour annoncer des événements importants.
- Mise en œuvre de plans de crise adaptés à chaque région et unité commerciale.
- Élargissement de notre empreinte en matière de préparation aux crises avec la mise en place d'équipes de crise locales pour nos activités en République dominicaine et au Brésil.

Formation sur la sécurité

- Réalisation de plus de 210 000 simulations, avec le taux de clics le plus bas jamais atteint (2,9 %) pour des tentatives d'hameçonnage simulées.
- Intégration des indicateurs de la chaîne logistique dans les portraits mensuels de sécurité des employés concernés, soulignant ainsi l'importance de leur rôle dans la protection d'Equifax grâce à une évaluation appropriée des liens avec les fournisseurs.

Services liés aux brèches

- Soutien à plus de 700 organisations en réponse à des cyberincidents; au nom de nos clients, nous avons offert une protection de l'identité à 22 millions de victimes de brèches de données dans plus de 25 pays.

Engagement des clients

- Réalisation de 3 551 questionnaires et vérifications à la demande des clients d'Equifax pour assurer la conformité.
- Mise sur le marché en toute sécurité de plus de 100 INP pour la cinquième année consécutive.

Fraude

- Amélioration de la détection des fraudes avec 41 % plus de signalements d'activités suspectes qu'en 2023, ce qui démontre une visibilité accrue et des stratégies d'atténuation plus solides.

Sécurité physique et enquêtes

- Réalisation de 12 tests d'intrusion physique pour cibler les domaines d'amélioration continue.
- Réalisation de 38 évaluations de la sécurité physique pour sécuriser les employés, les données et les actifs.

La voie à suivre

En 2024, nous avons utilisé la sécurité comme moteur de rapidité, de confiance et de différenciation sur le marché, en supprimant les identifiants, en intégrant l'IA à la détection des menaces et aux activités quotidiennes et en transformant l'adversité en avantage. Nous ne sommes pas uniquement en mode défensif : nous avançons plus vite, nous lançons de nouveaux produits et nous plaçons la barre plus haut que jamais. Et ce n'est pas terminé. En 2025 et pour les années à venir, nous nous concentrerons sur l'innovation continue. Nous continuerons à tracer de nouvelles voies en matière de sécurité et de technologie pour protéger les données de nos clients contre les acteurs malveillants et en faire profiter l'ensemble du secteur.

1550 Peachtree Street NW, Atlanta, GA 30309 • 404.885.8000 • equifax.com