EQUIFAX®

Rapport annuel sur la sécurité

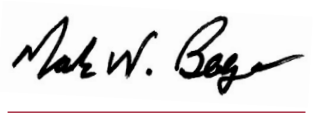
2025

Table des matières

Nous croyons qu'une meilleure communication, une plus grande collaboration et davantage de transparence entraînent une sécurité plus robuste.

Un message du PDG d'Equifax

Mark W. Begor



Président-directeur général
Equifax

2025 a été une année stimulante de croissance et d'innovation. Notre transformation mondiale des technologies et de la sécurité de 3 milliards de dollars — ainsi que la création du nuage EFXMC — étant pour l'essentiel achevées, l'IA.EFX propulse l'avenir de la nouvelle Equifax. Nous accélérons le déploiement de la technologie brevetée IA.EFX dans nos produits, en tirant parti des données exclusives et uniques qui distinguent Equifax dans l'industrie. Cette évolution a conduit à un nombre record d'innovations de nouveaux produits (INP) qui fournissent l'intelligence décisionnelle dont nos clients mondiaux ont besoin pour créer de nouvelles opportunités plus rapidement que jamais. De plus, nous gagnons en efficacité en tirant parti de l'intelligence artificielle (IA) à l'interne pour passer moins de temps sur les tâches de routine et plus de temps sur les défis complexes, créatifs et collaboratifs qui font avancer notre entreprise.

Notre engagement inébranlable envers la sécurité établit une base solide pour cette innovation.

Lorsque je me suis joint à Equifax en 2018, j'ai pris l'engagement personnel d'établir Equifax comme chef de file de l'industrie en matière de sécurité des données, et de bâtir une culture où chaque personne chez Equifax est responsable de la sécurité. Nous avons transformé chaque aspect de notre organisation pour tenir cette promesse, en faisant de la sécurité une partie de l'ADN de notre équipe mondiale. Avec la publication de notre sixième rapport annuel sur la sécurité, notre engagement inlassable envers la primauté en sécurité est clair : notre niveau de maturité de la sécurité a surpassé toutes les principales références de l'industrie pendant six années consécutives, et notre pointage de la posture de sécurité a dépassé les moyennes de l'industrie des technologies et des services financiers pour une cinquième année consécutive.

En même temps, nous reconnaissons que notre travail en matière de sécurité n'est jamais terminé.

L'année 2025 a vu une foule de nouvelles menaces pour l'infrastructure mondiale de cybersécurité, définies par une convergence de volume, de vitesse et de sophistication propulsée par l'IA. Nous avons vu des agents autonomes et l'IA industrialisée amplifier les attaques traditionnelles, en élargissant la portée de ce que nous devons défendre. Equifax était prête. Guidés par notre volonté d'optimisation inlassable et la maximisation de notre infrastructure nativement infonuagique, nous nous sommes défendus contre plus de 19,8 millions de menaces à la cybersécurité chaque jour tout en effectuant plus de 240 000 simulations pour tester notre main-d'œuvre mondiale et nous préparer à ce qui nous attend.

Alors que de nombreuses entreprises devraient être bouleversées ou désintermédiées par l'IA, Equifax tire parti de l'IA pour révolutionner l'industrie et accélérer notre primauté en sécurité. Nous sommes fiers que l'IA ait fondamentalement changé notre façon de fonctionner, avec près de 90 % de notre équipe mondiale tirant parti des outils d'IA en 2025. À mesure que nous habilitons notre entreprise à innover avec l'IA, nous avons mis en place des garde-fous rigoureux — des filtres de sécurité de contenu automatisés aux cadres de codage sécurisés — garantissant que nos modèles sont explicables et sûrs, et que nos données exclusives restent protégées.

Nous continuerons de tirer parti de l'IA pour améliorer nos défenses, sécuriser l'utilisation de l'IA par l'entreprise pour l'innovation et nous défendre contre les menaces liées à l'IA. Surtout, nous maintiendrons non seulement notre priorité absolue sur la sécurité, mais nous continuerons également d'aider nos clients, nos partenaires et les consommateurs à renforcer leurs propres postures de cybersécurité au profit de l'ensemble de l'industrie.

Un message du RSI d'Equifax

Jeremy Koppen

Chef principal de la sécurité de l'Information
Equifax

J'ai commencé ce poste avec une perspective distincte sur le parcours de sécurité d'Equifax. Avant de me joindre à l'entreprise en tant que RSI en mai 2025, j'étais directeur général chez Mandiant, où j'ai eu le privilège de travailler aux côtés de cette équipe lors des premières étapes cruciales de sa transformation. Et pendant des années par la suite, j'ai admiré leurs progrès continus de l'extérieur.

Je savais qu'Equifax était reconnue comme un chef de file de l'industrie en matière de sécurité. Mais quand j'ai franchi la porte, je n'ai pas trouvé une équipe en train de faire un tour d'honneur. J'ai trouvé une équipe avec une motivation et une concentration qui se sont immédiatement démarquées.

Cette intensité est essentielle car le paysage des menaces de 2025 a été défini par une convergence de volume, de vitesse et de sophistication. Nous avons vu des agents autonomes et une IA industrialisée amplifier les attaques traditionnelles, élargissant radicalement la portée de ce que nous devons défendre. Dans cet environnement, faire simplement plus n'est pas une stratégie. Nous devons évoluer de manière proactive pour garder une longueur d'avance.

Ainsi, cette année, nous nous sommes concentrés sur **une optimisation implacable.**

L'IA a fondamentalement changé notre façon de fonctionner. En tirant parti de notre infrastructure en nuage natif, nous avons utilisé l'IA pour rationaliser notre Centre des opérations de sécurité et accélérer les tâches routinières afin que nos experts puissent se concentrer sur les menaces qui comptent le plus. Nous avons également atténué l'IA adverse, en déployant des contrôles personnalisés pour bloquer les infiltrations de requête invisibles et les hypertrucages. Nous avons également sécurisé l'utilisation de l'IA au sein de l'entreprise, en organisant l'architecture de nos systèmes de manière à éliminer les obstacles, tout en mettant en place les garde-fous qui ont permis à notre main-d'œuvre de tirer parti rapidement *et* de manière responsable des capacités de l'IA dans tous les coins d'Equifax. Cette discipline a permis de garantir que la **sécurité reste un véritable accélérateur des activités commerciales.**

La preuve se trouve dans nos résultats. En 2025, Equifax a lancé en toute sécurité plus de 180 innovations de nouveaux produits (INP) — notre sixième année consécutive au-dessus de 100. Cette réussite démontre qu'une sécurité rigoureuse n'est pas un intérêt concurrent, mais un catalyseur vital d'innovation rapide et de croissance.

Mais surtout, la sécurité à Equifax est une discipline partagée. Nous le voyons en action alors que nos équipes technologiques construisent une architecture sécuritaire dès la conception, et que nos partenaires des finances et des services juridiques posent les questions difficiles sur le risque lié aux tiers. Nous le voyons également chez nos membres du personnel à travers le monde, qui agissent comme des capteurs humains en signalant de nouvelles tentatives d'hameçonnage et en renforçant nos défenses automatisées grâce à l'intuition humaine.

Sommes-nous satisfaits? Absolument pas. Nous avons encore augmenté notre maturité de sécurité en 2025, mais les menaces auxquelles nous sommes confrontés continuent d'évoluer. Nous continuerons d'adopter de nouvelles technologies, d'optimiser nos défenses et de prioriser nos efforts en fonction de l'impact, et non de la facilité.

Je suis fier de diriger une équipe avec une ambition implacable de surpasser le statu quo. Notre poursuite de la primauté en matière de sécurité n'a pas de plafond.

Notre impact :

La sécurité à Equifax en 2025

Plus de 19.8 millions
de cybermenaces bloquées chaque jour — près de 230 tentatives hostiles chaque seconde, une augmentation de 30 % par rapport à l'année dernière.

Plus de 240 000
simulations lancées pour tester notre main-d'œuvre mondiale sur divers scénarios de sécurité.

Près de 22 000
employés permanents et contractuels formés par le biais de modules de sécurité personnalisés, en augmentant la difficulté des simulations pour refléter l'environnement de menace en évolution.

Plus de 4 000
utilisateurs externes ont accédé à notre cadre de contrôles de sécurité et de confidentialité dans plus de 70 pays.

Plus de 3 700
questionnaires clients et demandes de preuves complétés pour renforcer la confiance envers notre posture de sécurité.

Plus de 2 280
analyses de risques approfondies sur des fournisseurs tiers critiques et à haut risque, en identifiant les failles de sécurité potentielles avant qu'elles ne puissent être exploitées.

Plus de 400
professionnels dédiés à la cybersécurité qui protègent les données des consommateurs 24 heures sur 24.

Plus de 330
vérifications de sécurité infonuagique automatisées surveillées en temps réel, alimentant une réponse aux menaces plus rapide et une connaissance quasi instantanée de la posture.

Plus de 180
innovations de nouveaux produits mis sur le marché en toute sécurité — notre sixième année consécutive au-dessus de 100, prouvant que la vitesse et la sécurité ne sont pas incompatibles.

52
certifications et autorisations obtenues auprès d'auditeurs externes, validant notre approfondissement et notre rigueur.

43
évaluations de sécurité physique réalisées pour protéger nos gens, nos données et nos actifs.

Plus de 35
forums auxquels nous avons participé à l'échelle mondiale pour partager des renseignements et renforcer les défenses collaboratives.

18
exercices de table simulant des scénarios de crise aux niveaux de la haute direction et des secteurs régionaux.

6
années consécutives à atteindre un pointage de maturité lié à la sécurité qui surpasse tous les principaux critères de référence de l'industrie.

2
intégrations d'acquisition réalisées selon un nouveau manuel de sécurité rationalisé.

1
minute de temps moyen pour détecter les cybermenaces.

État d'avancement :
La cybersécurité en 2025

Pivot vers la priorisation

En 2025, les entreprises ont continué de voir une augmentation du volume, de la fréquence et de la rapidité des cyberattaques. Dans ce contexte, les équipes avancées ont adopté l'IA pour étendre ce qui pouvait être neutralisé automatiquement, de sorte que moins de menaces requièrent une intervention humaine. Simultanément, l'industrie a affiné sa définition du risque. Alors que les évaluations du risque génériques ont toujours manqué de nuance et de contexte, le paysage des menaces en 2025 les a rendues particulièrement trompeuses.

Pour en tenir compte, les responsables de la sécurité sont passés à des pointages sur mesure qui étaient plus spécifiques aux environnements uniques de leurs entreprises — prenant en compte des variables telles que le fait qu'un système soit exposé à Internet, strictement contrôlé en matière d'accès ou qu'il détienne des données sensibles. Cela a permis aux équipes de filtrer les failles à l'aide de pointages du risque élevé, mais un faible risque pratique pour leur entreprise spécifique, et de prioriser à la place les vulnérabilités qui menaçaient réellement l'entreprise.

L'évolution du risque lié aux tiers

Les vulnérabilités de la chaîne logistique ont défié l'industrie pendant plus d'une décennie, mais en 2025, la tactique a changé. Les attaquants sont passés de l'exploitation des failles logicielles au détournement d'accès légitimes. En compromettant les fournisseurs et en volant leurs identifiants, les criminels sont effectivement « devenus » le partenaire — en utilisant des connexions autorisées pour contourner les défenses sans se faire remarquer.

Cette évolution a transformé un problème lié à la chaîne logistique en une crise d'identité, obligeant les entreprises à vérifier les partenaires de confiance aussi rigoureusement qu'elles le font pour les menaces externes.

Écart de gouvernance des agents d'IA

À mesure que l'IA a évolué des simples dialogueurs vers des agents puissants capables de se connecter aux systèmes internes pour effectuer un travail réel, il est devenu clair que bien que ces outils puissent accéder à des données sensibles, ils manquaient potentiellement de contrôles pour les garder en sécurité.

Cela a créé une division dans l'industrie. Certaines entreprises se sont précipitées, en acceptant le risque d'utiliser des outils qu'elles ne pourraient peut-être pas surveiller ou arrêter complètement en cas d'urgence. D'autres ont complètement interrompu l'adoption, par peur de voler à l'aveugle. Mais les équipes les plus efficaces ont trouvé une troisième voie. Elles ont construit leurs propres vérifications de sécurité personnalisées pour sécuriser leurs données, en utilisant leurs contrôles de sécurité fondamentaux existants, et ont simultanément travaillé avec les fournisseurs pour combler les lacunes architecturales.

Surface d'attaque en expansion sur le plan des identifiants

La surface d'attaque liée à l'identité s'est considérablement élargie en 2025, en exposant à la fois les personnes et les machines. Les attaquants ont armé l'IA pour lancer des hypertrucages hyperréalistes et des campagnes d'hameçonnage qui ont régulièrement trompé même les membres du personnel avertis, et l'écosystème d'identité machine s'est développé sans contrôle.

Alors que les entreprises se précipitaient pour automatiser, elles ont généré des milliers d'identifiants non humains (comme des clés d'API) qui manquaient de cette surveillance rigoureuse appliquée aux humains. Les attaquants ont saisi ces cibles silencieuses à haut accès, prouvant que la protection de l'identité nécessite désormais de gouverner chaque entité qui se connecte au réseau, qu'elle soit humaine ou non.

Nos actions :

Initiatives et résultats sur la sécurité d'Equifax en 2025

Modernisation de notre approche envers la culture de sécurité

Chaque employé permanent et contractuel reconnaît que la sécurité est une partie essentielle de son travail. Nous avons renforcé cela en introduisant une plateforme alimentée par l'IA qui offre une formation personnalisée et ludifiée à l'ensemble de notre main-d'œuvre.

Nous avons validé leur formation par le biais de plus de **240 000 simulations d'hameçonnage mondiales en 2025** (15 % de plus qu'en 2024), en augmentant le niveau de difficulté pour correspondre au paysage des menaces. Nous avons également élargi les cartes de pointage pour inclure six nouveaux comportements basés sur les postes, en entraînant une amélioration de 10 % par rapport à un certain comportement en seulement quatre mois, montrant que des commentaires clairs font bouger les choses.

En démontrant que la sécurité est une priorité personnelle, les employés ont utilisé nos 20 000 nouveaux outils de signalement d'hameçonnage pour signaler des menaces potentielles en seulement six mois, en repérant près de 1 500 indicateurs malveillants confirmés.

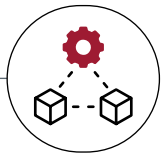
Renforcement de la sécurité comme différenciateur de marché

La sécurité est un différenciateur concurrentiel qui permet le succès commercial. Nous avons mis à l'échelle nos défenses pour permettre le lancement sécurisé d'un nombre record d'innovations de nouveaux produits en 2025, tout en obtenant 52 certifications, y compris des autorisations critiques du gouvernement américain.

Nous avons également déployé une base de connaissances spécialisées en IA qui génère des réponses aux questionnaires de sécurité basées uniquement sur notre documentation de politique officielle. Les premières mesures montrent un taux de réussite de 67 % sur les réponses de premier passage, surpassant de loin les solutions patrimoniales et nous permettant de **répondre aux besoins de la clientèle avec une rapidité sans précédent.**

En 2025, un chef de file du secteur des télécommunications nommé au palmarès de Fortune 50 a **publiquement présenté Equifax comme le modèle** à suivre dans le secteur pour « assurer la sécurité de manière appropriée », en citant notre transparence comme un élément fondamental dans la confiance qu'il nous accorde. Notre engagement en faveur de la transparence est mondial : l'année dernière, plus de 4 000 utilisateurs dans 70 pays ont accédé à notre cadre de contrôles de sécurité afin de renforcer leurs propres défenses.

Unification de la sécurité et de l'ingénierie



En 2025, nous avons **combiné nos fonctions d'architecture de sécurité et d'architecture technologique,** en unissant les bâtisseurs et les défenseurs pour stimuler des solutions cohérentes et automatisées à travers le monde.

Grâce à cette fondation partagée, nous avons essentiellement organisé l'architecture de nos systèmes en éliminant les obstacles. En fournissant aux équipes d'ingénierie une **plateforme de développement uniformisée et automatisée** qui offre des déploiements en un clic et une intégration continue, nous leur avons permis d'expédier en toute sécurité **50 % de changements en plus** — prouvant que nous pouvons accélérer l'innovation liée aux technologies et aux produits sans compromettre la sécurité.

Cette vitesse opérationnelle s'est étendue à nos défenses. Avec une meilleure visibilité, nous avons identifié, évalué et assuré la remédiation de plus de 3 700 composants d'infrastructure critiques — **une augmentation de 164 % de la couverture** d'une année à l'autre. Malgré ce volume plus élevé, nous avons maintenu **un temps de fermeture moyen de moins de 24 heures,** démontrant que lorsque la sécurité est collective, nous résolvons les problèmes aussi vite que nous les trouvons.

Co-innovation avec les fournisseurs et partenaires

Equifax continue de faire progresser les normes de l'industrie par la co-innovation, une stratégie où nous **associons directement avec nos fournisseurs de sécurité pour façonner des améliorations de produits et de services** qui sécurisent non seulement notre environnement, mais aussi celui d'autres entreprises.

Nous avons aidé notre partenaire de protection des points d'extrémité à combler les **lacunes de visibilité** dans l'infrastructure de serveur Linux, mis au défi notre fournisseur infonuagique de **développer des contrôles d'accès plus approfondis**, pour l'IA générative, insisté pour obtenir des correctifs matériels critiques, et travaillé avec notre fournisseur de gestion des identités et des accès pour **optimiser l'infrastructure, en réduisant la latence** pour améliorer la productivité.

Cette collaboration s'est également étendue au-delà des fournisseurs de technologies jusqu'au secteur public. Par exemple, nous avons rejoint 25 partenaires et les forces de l'ordre canadiennes pour aider à **exécuter plus de 3 000 actions contre des réseaux de fraude.** Nous avons également élargi notre partenariat en Amérique latine, **en travaillant avec des organismes gouvernementaux au Salvador et au Costa Rica** pour faire progresser l'éducation en matière de sécurité de l'IA et façonner des structures de normalisation nationales.

Utiliser l'IA pour améliorer la sécurité

Nous avons appliqué de nouvelles technologies pour faire ce que nous avons toujours fait — seulement plus vite et avec une meilleure précision. En déployant l'IA comme un multiplicateur de force stratégique, nous avons amélioré notre capacité non seulement à trier et à remédier aux menaces, mais aussi à accélérer les décisions critiques en matière de sécurité qui renforcent la prestation des services d'affaires.

Nous avons commencé à utiliser l'IA agentive pour traiter les alertes de routine, libérant ainsi les analystes pour gérer les menaces complexes.

Les Centres des opérations de sécurité sont confrontés à un défi universel : la fatigue liée aux alertes, où les analystes doivent parcourir des milliers de notifications à faible risque.

Nous avons donc conçu et piloté un agent de triage spécialisé ayant un mandat strict : analyser les alertes de faible fidélité et ne les fermer que si elles répondent à une « définition de terminé » rigoureuse.

Avec une adoption complète à travers notre Centre des opérations de sécurité mondial prévue en 2026, cet outil a ajouté une nouvelle couche à la suite d'automatisation qui accélère la fermeture des problèmes, tout en aidant les experts à passer moins de temps à fermer des tickets, et plus de temps à chasser des adversaires sophistiqués.

Impact | Résolution automatique de près de **50 %** de tous les tickets d'incident du Centre des opérations de sécurité grâce à des défenses automatisées.

Nous avons considérablement réduit le temps nécessaire pour tester nos défenses contre les nouvelles menaces.

Dans le passé, tester nos défenses contre les dernières tactiques criminelles était un processus manuel. Le temps qu'un test soit conçu, l'adversaire était souvent passé à autre chose.

Pour réduire cette période, nous avons construit un moteur alimenté par l'IA qui lit des rapports de cybermenaces non structurés et les convertit instantanément en scénarios d'attaque exploitables. Cela nous permet de simuler ces attaques et de valider nos défenses contre les dernières tactiques adverses dans les jours suivant leur découverte, garantissant que notre bouclier est toujours calibré sur la menace actuelle.

Impact | Passage de la **divulgation de la menace** à **la validation de la défense** en jours, et non en mois.

Nous avons intégré des assistants IA personnalisés pour réduire les obstacles pour l'entreprise.

Pour nous assurer que nos processus de sécurité soutiennent une innovation rapide et un dialogue client sans accroc, nous avons utilisé l'IA pour uniformiser deux flux de travaux critiques.

Premièrement, un assistant consultatif en IA aide désormais les architectes à analyser les conceptions instantanément, réduisant ainsi le temps de résolution des consultations de sécurité de 46 à 18 jours.

Deuxièmement, une base de connaissances en IA accélère les questionnaires de sécurité de la clientèle en basant les réponses sur une politique validée. Cet outil a atteint un taux de réussite de premier passage de 67 %, permettant à nos équipes de répondre à la clientèle avec une plus grande rapidité et précision.

Impact | Réduction des temps de consultation de sécurité de **61 %** et accélération des réponses liées aux ventes.

Nous sommes passés de la recherche de failles à leur correction automatique.

Les outils de sécurité traditionnels s'arrêtent à la détection — alertant les développeurs d'une vulnérabilité et l'ajoutant à leur carnet de commandes. Nous avons franchi une étape supplémentaire en déployant des agents d'IA pour non seulement trouver les problèmes, mais aussi les résoudre.

À l'aide d'une architecture d'IA personnalisée, notre système analyse les vulnérabilités des conteneurs et inscrit automatiquement le correctif de code. Il soumet ensuite une « demande d'extraction » pour que le développeur l'examine et la fusionne. Cela fait passer la sécurité d'un gardien qui ralentit les choses à un partenaire qui nettoie le code.

Impact | Traitement de **plus de 213 000 constatations** par an sans ralentir la livraison des produits.

Sécuriser l'utilisation de l'IA dans l'entreprise

Alors que notre main-d'œuvre et nos développeurs ont adopté l'IA pour stimuler l'innovation, notre priorité était de garantir qu'ils pouvaient le faire en toute sécurité. Nous nous sommes concentrés sur la construction des garde-fous nécessaires (des filtres de sécurité de contenu automatisés jusqu'aux structures de codage sécurisé) qui ont permis à nos équipes d'adopter de nouveaux outils puissants, sans exposer l'entreprise à une fuite de données potentielle ou à un risque non géré.

Nous avons conçu des modèles d'IA plus sûrs sur le plan de l'utilisation de données d'entreprise.

Nous avons conçu notre architecture de manière à ne jamais compter uniquement sur un fournisseur de modèles pour protéger nos données. Au lieu de cela, nous avons mis en œuvre une couche de contrôle agnostique qui se situe entre nos employés et l'IA.

Cette couche assainit les requêtes et les réponses, vérifiant les fuites de données sensibles ou les attaques par infiltration malveillante avant qu'elles ne touchent un modèle d'IA. Cela garantit que même si un modèle externe est compromis, nos données restent protégées.

Impact | Fourniture d'une **couche de contrôle unifiée** pour l'infiltration de requêtes et la protection des données personnelles.

Nous avons conçu les protocoles qui permettent à chaque employé d'être un bâtisseur d'IA.

Pour mettre l'IA à l'échelle en toute sécurité à Equifax, nous nous sommes éloignés du contrôle d'accès manuel pour passer à la Politique en tant que code. Nos portes d'évaluation testent automatiquement chaque nouvel agent avant la production, et une surveillance continue détecte si un modèle commence à dériver ou à se comporter de manière imprévisible.

Cela nous positionne pour répondre aux réglementations évolutives en matière d'IA en garantissant que, pour les cas d'utilisation à enjeux élevés, nous appliquons des approbations avec intervention humaine et des interrupteurs d'arrêt automatisés avec des capacités de retour en arrière instantané. Ce cadre nous permet de démocratiser les outils d'IA avec l'assurance que les filets de sécurité sont toujours actifs.

Impact | Déploiement sécurisé d'outils d'IA générative pour **~22 000 employés permanents et contractuels** dans le monde.

Nous avons remplacé l'« IA fantôme » par un contrôle de précision et un accès organisé.

Nous avons rejeté l'approche « activé par défaut » des grands fournisseurs. Lorsque de nouvelles fonctionnalités introduisaient des risques potentiels pour les données, nous les avons mises en pause de manière sélective jusqu'à ce qu'elles puissent répondre aux normes et contrôles de sécurité d'Equifax.

Simultanément, nous sommes passés du blocage de l'innovation à son orientation. Nous avons appliqué une liste de refus stricte pour les modèles externes à haut risque, tout en offrant un accès instantané à une liste pré-approuvée d'outils prêts pour l'entreprise. Cela garantit que nos développeurs construisent sur une fondation de confiance.

Impact | Réduction du risque grâce à **l'activation sélective et conforme des fonctionnalités**.

Nous avons mis en œuvre des connexions de code sûres pour les agents d'IA.

À mesure que l'IA passe de simples dialogueurs à des agents autonomes capables de modifier le code, le risque d'un agent « sur-privilégié » augmente. Pour répondre à cela, nous avons défini un cadre de sécurité rigide pour le Protocole de contexte de modèle (MCP).

En permettant aux développeurs d'utiliser des serveurs MCP distants pour accéder au code en direct en toute sécurité, nous garantissons qu'ils peuvent tirer parti de la dernière assistance de l'IA sans donner à une machine un accès non contrôlé à l'ensemble de la base de codes.

Impact | Opérationnalisation **de la connectivité sécurisée IA-vers-Code**.

Se défendre contre les menaces liées à l'IA

Nous avons reconnu que les criminels adoptaient également des outils compatibles avec l'IA pour créer des usurpations d'identité hautement réalistes et lancer des attaques plus rapides et plus complexes. Nous avons donc recalibré nos défenses pour détecter et nous protéger contre ces menaces, garantissant que nos contrôles restent efficaces contre une nouvelle génération de fraude et de cyberattaques compatibles avec l'IA.

Nous avons intercepté avec succès une attaque par hypertrucage ciblant notre équipe de direction.

En 2025, la menace théorique du clonage vocal par IA est devenue une réalité. Nos cyberéquipes ont détecté une attaque de piratage psychologique sophistiquée mettant en vedette un mémo vocal par hypertrucage usurpant l'identité de notre président-directeur général.

Nous n'avons pas seulement arrêté l'attaque; nous l'avons utilisée pour renforcer notre immunité. Nous avons instantanément analysé les modèles linguistiques de l'adversaire et déployé des règles de détection personnalisées sur nos passerelles de messagerie, inoculant efficacement l'organisation contre les futures tentatives de fraude générées par l'IA.

Impact | Transformation **d'une tentative d'hypertrucage en direct** en une mise à niveau permanente de la défense.

Nous avons découvert et bloqué des attaques invisibles conçues pour tromper les modèles d'IA.

Alors que nous intégrions l'IA, notre équipe de simulation d'attaques a découvert une nouvelle vulnérabilité : les adversaires pouvaient intégrer des infiltrations de requêtes textuelles invisibles (indétectables à l'œil humain) qui trompent les modèles d'IA pour qu'ils livrent des logiciels malveillants.

Nous avons réussi à faire passer cette découverte d'un cas de test à un contrôle de prévention en direct. Nous avons mis en œuvre une logique pour supprimer ces commandes cachées avant qu'elles n'atteignent notre écosystème, fermant une faille que de nombreuses organisations n'ont pas encore détectée.

Impact | Passage de la **découverte d'attaques simulées** au **contrôle de prévention** en un temps record.

Nous avons déployé des défenses adaptatives pour détecter les attaques évasives axées sur l'IA.

Les attaquants utilisent l'IA pour écrire du code qui se réécrit constamment pour contourner les filtres traditionnels. Ces attaques « polymorphes » sont conçues pour paraître différentes à chaque fois qu'elles frappent.

En réponse, nous avons déployé une logique d'évasion personnalisée dans nos défenses de points d'extrémité. Plutôt que de rechercher une signature de fichier spécifique, nos outils analysent désormais le comportement du code, nous permettant de détecter et de bloquer les logiciels malveillants générés par l'IA, quelle que soit la façon dont ils se déguisent.

Impact | Blocage des **logiciels d'IA malveillants évasifs** qui contournent les filtres traditionnels.

Nous avons renforcé nos portails pour consommateurs contre les essaims de robots logiciels axés sur l'IA.

L'automatisation permet aux criminels d'attaquer à une échelle que les humains ne peuvent égaler, utilisant des « essaims » de robots pour extraire des données ou tester des identifiants volés contre nos portails pour consommateurs. Pour protéger les cibles de haute valeur, nous avons déployé des profils de mode de blocage avancés.

Ces défenses identifient et neutralisent les tactiques pilotées par l'IA comme le « culbutage d'adresses courriel » (modifier rapidement une adresse unique pour contourner les filtres), garantissant que nos données restent accessibles aux personnes, mais pas aux robots logiciels.

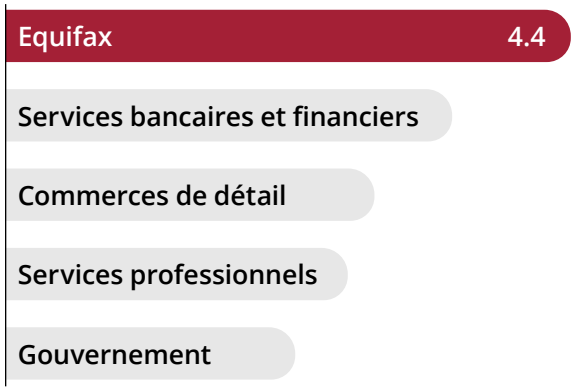
Impact | Neutralisation des **campagnes sophistiquées d'extraction d'identifiants** en temps réel.

Analyse comparative indépendante

Maturité liée à la sécurité

La maturité liée à notre programme de cybersécurité, qui a obtenu en 2025 un pointage relatif au cadre de sécurité de 4.4 attribué par le National Institute of Standards and Technology (NIST), s'est améliorée en 2025, surpassant tous les principaux points de référence de l'industrie pour une sixième année consécutive.

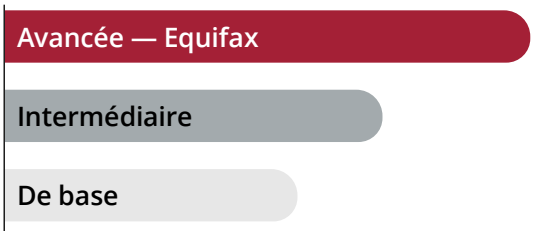
Pointage de maturité lié à la sécurité



Position en matière de sécurité

Le pointage de notre posture de sécurité a surpassé les moyennes de l'industrie des technologies et des services financiers pour une cinquième année consécutive.

Note de posture de sécurité



Ce sont les catégories de notation attribuées par le service de production de rapports qui surveille notre posture. Equifax maintient une note qui nous place dans la catégorie la plus élevée.

Qu'est-ce que la maturité liée à la sécurité?

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

Nous associons à un cabinet mondial de recherches et de conseils de premier plan pour mener une analyse approfondie de la maturité de l'ensemble de notre programme de sécurité.

Qu'est-ce que la posture de sécurité?

La posture de sécurité d'une organisation est son état de préparation et sa capacité à identifier, réagir et récupérer lorsqu'il est question de menaces et de risques 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 relatif à la chaîne logistique.

Résumé des résultats :
La sécurité à Equifax en 2025

Maturité et posture de sécurité

- Obtention d'un pointage record de 4.4 du National Institute of Standards and Technology (NIST) en 2025 sur le plan de la maturité liée à la sécurité, surpassant tous les principaux points de référence de l'industrie pour une sixième année consécutive.
- Obtention d'une note de posture de sécurité qui a dépassé les repères de l'industrie des technologies pour une cinquième année consécutive — montrant une posture de sécurité constamment robuste aux clients et aux régulateurs.

Conformité

- Obtention réussie de 52 certifications en 2025 incluant une réduction de 2 % d'une année à l'autre du coût par certification, et une diminution de 66 % par rapport à 2018.
- Uniformisation de la conformité en lançant un portail de preuves automatisé et un nouveau tableau de bord pour mapper les constatations directement aux contrôles spécifiques — réduisant le fardeau manuel lié à la conformité.

Fusions et acquisitions ciblées

- Intégration réussie de deux acquisitions précédentes en utilisant notre cadre de fusions et acquisitions répétable basé sur le NIST — garantissant une transition plus sécurisée.
- Accélération du cycle de vie des fusions et acquisitions en combinant des évaluations d'API sans agent avec l'IA générative — réduisant les délais de diligence raisonnable de quelques semaines à quelques jours, tout en automatisant l'analyse des données pour des intégrations plus rapides et plus intelligentes.

Cybersécurité

- Identification, évaluation et assurance de la remédiation de plus de 3 700 composants d'infrastructure critiques, une augmentation de 164 % en glissement annuel, tout en maintenant un temps de fermeture moyen inférieur à 24 heures — réduisant considérablement la surface d'attaque de l'organisation.
- Construction et pilotage d'un nouvel agent de triage IA qui aide désormais à résoudre automatiquement près de 50 % de tous les tickets d'incident du Centre des opérations de sécurité.
- Maintien des connexions sans mot de passe pour nos près de 22 000 membres du personnel et contractuels dans le monde.
- Migration achevée vers la gestion des accès en nuage natif pour ~2 000 applications, améliorant le contrôle d'accès et la visibilité.
- Déploiement de l'IA pour traduire les rapports de renseignement sur les menaces non structurés en scénarios d'attaque simulée exploitables — nous permettant de tester nos défenses contre de nouvelles tactiques adverses dans les jours suivant leur découverte, et non des mois.
- Application de l'authentification multifacteur (AMF) pour 100 % de l'accès à distance, réduisant les risques d'entrée non autorisée.

Sécurité physique et enquêtes

- Réalisation de 29 tests d'intrusion physique, identifiant des domaines d'amélioration continue.
- Conduite de 43 évaluations de sécurité physique pour sécuriser le personnel, les données et les actifs.

Gestion des risques

- Établissement d'un moteur de risque quantitatif comme source de vérité faisant autorité pour les mesures de sécurité, permettant l'ingestion quotidienne et la priorisation des tâches de remédiation des vulnérabilités.
- Réalisation d'analyses de risques approfondies sur 100 % des tiers critiques et à haut risque de notre entreprise (2 289) — conduisant à des plans de remédiation exploitables là où c'est nécessaire.
- Réalisation d'évaluations de risques sur 100 % des applications d'affaires (4 022) pour établir une compréhension complète du risque lié aux actifs.
- Poursuite de l'intégration de comptes stratégiques clés, y compris certaines des plus grandes institutions financières au monde, sur Contrôle infonuagique — fournissant une visibilité en temps réel sur la sécurité de leurs produits et services Equifax.

Gestion des crises

- Conduite de 18 exercices de table avec les parties prenantes de l'entreprise, y compris :
  - PDG et équipe de direction;
  - Équipes de crise régionales et des unités d'affaires.
- Introduction de nouveaux exercices de table axés sur la menace interne, la modélisation de l'IA, les rançongiciels et les scénarios de piratage psychologique — équipant les dirigeants pour répondre aux menaces avancées.
- Mise en œuvre de plans de crise sur mesure et facilitation d'exercices de table régionaux en espagnol et en portugais pour assurer l'état de préparation des équipes locales.
- Intégration de la gestion de crise avec la continuité des activités et la reprise sur sinistre — formant une organisation unique et unifiée de gestion de crise d'affaires.

Formation à la sécurité

- Conduite de plus de 240 000 simulations d'hameçonnage (augmentation de 15 % en glissement annuel), augmentant continuellement la difficulté à mesure que le paysage des menaces évolue.
- Reciblage du personnel qui a démontré une susceptibilité à l'hameçonnage pour mieux les éduquer sur les techniques courantes des acteurs liés aux menaces.
- Introduction d'un nouvel outil de signalement des menaces, générant plus de 20 000 signalements d'hameçonnage potentiel de la part des employés permanents et contractuels en seulement 6 mois, dont près de 1 500 ont été confirmés comme incluant des indicateurs malveillants.
- Incorporation de 6 nouveaux facteurs dans les aperçus de sécurité mensuels du personnel — cette année, y compris des comportements liés à :
  - La certification d'accès, évaluant la recertification opportune de l'accès des utilisateurs, de l'utilisation des comptes et de la propriété des droits.
  - L'utilisation d'images de référence, mesurant si les ingénieurs utilisent des images dorées standardisées pour les environnements.
  - La gouvernance des problèmes, mesurant la rapidité de fermeture des problèmes de sécurité ouverts.

Engagement client

- Réalisation de 2 599 questionnaires clients, avec un temps de réalisation moyen de 1,86 jour, fournissant une assurance de sécurité rapide aux parties externes.
- Réalisation de 1 149 demandes de preuves à la demande de la clientèle d'Equifax pour assurer la conformité.
- Mise sur le marché en toute sécurité de plus de 180 INP — notre sixième année consécutive au-dessus de 100.

Confidentialité

- Mise en œuvre d'un nouvel outil pour la prévention de la perte de données (DLP) par courriel, offrant une plus grande compatibilité avec notre ensemble d'outils existant, des analyses plus robustes et une conformité mondiale améliorée.
- Obtention de la recertification au Cadre de protection des données (DPF) pour la 2e année, permettant des transferts de données sécurisés de l'UE/R.-U. vers les États-Unis.
- Lancement d'une nouvelle plateforme de gestion du consentement à l'échelle mondiale pour respecter les choix des visiteurs du site Web.

Fraude

- Finalisation de la stratégie mondiale de surveillance de la fraude et normalisation du blocage des comptes frauduleux en une plateforme infonuagique unique, unifiant les processus entre les unités commerciales.
- Blocage de plus de 3 700 appareils suspects et 2 900 adresses IP suspectes grâce aux enquêtes sur la fraude.
- Les incidents de fraude impliquant l'exposition de données sensibles ont chuté de 18 % d'une année à l'autre, soulignant notre capacité à arrêter une activité suspecte avant qu'elle ne s'aggrave.
- Établissement d'une nouvelle équipe de fraude en Inde, offrant une couverture mondiale étendue de la fraude et une capacité sur plusieurs fuseaux horaires.

Développement de logiciels sécurisés

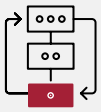
- Amélioration de l'adoption de l'Infrastructure en tant que code (IaC) de 52 %, tirant parti de blocs de code standardisés pour assurer l'alignement avec les normes de configuration d'Equifax et éliminer les mauvaises configurations manuelles.
- Lancement d'un assistant personnel alimenté par l'IA pour les flux de travaux des services consultatifs de sécurité (SAS) qui a réduit le temps moyen de résolution des consultations de 61 %, et réduit les demandes d'escalade initiales de 56 %.
- Développement d'une architecture d'IA sur mesure pour analyser les vulnérabilités des conteneurs et générer automatiquement le code de corrections, ce qui a permis de simplifier le processus de résolutions de plus de 213 000 incidents annuellement.
- Lancement de la boîte à outils de gestion automatisée des certificats afin d'automatiser le renouvellement des certificats TLS des applications (les identifiants numériques qui chiffrent les données en transit). Cet outil permet d'assurer le suivi des dates d'échéance, de mettre à jour et de tester les certificats sans intervention manuelle.

Nos priorités en 2026

Sécuriser chaque identité : L'homme et la machine

En éliminant les identifiants pour l'ensemble de notre main-d'œuvre, nous avons prouvé que l'authentification sans mot de passe est possible. En 2026, nous mettons cette révolution à l'échelle. Nous commencerons à déployer une option pour les connexions sans mot de passe à nos clients de commerce interentreprises, neutralisant les attaques par bourrage d'identifiants tout en éliminant les obstacles pour nos partenaires.

Simultanément, nous ciblons la majorité silencieuse des identités : les comptes non humains. Alors que nos agents d'IA et nos API se multiplient, nous appliquons la même vérification rigoureuse aux machines qu'aux personnes, garantissant qu'un robot logiciel ne peut pas être utilisé comme porte dérobée.



Mise à l'échelle de notre gouvernance agentique

En 2025, nous avons construit les protocoles pour sécuriser notre première génération d'agents d'IA. En 2026, nous industrialisons ce filet de sécurité. Nous élargissons notre cadre de politiques en tant que code pour couvrir chaque coin de l'entreprise, automatisant les tests de milliers d'agents pour la sécurité, la dérivation et la confidentialité stricte des données. Cette approche de gouvernance dès la conception garantit que nous gardons une longueur d'avance sur le paysage réglementaire complexe lié à l'IA.

En mettant à l'échelle ces garde-fous automatisés, nous permettrons à Equifax de passer du pilotage de flux de travaux agentiques à leur exécution en tant que moteur d'affaires standard à grand volume — sans jamais compromettre notre sécurité et notre contrôle.

Évolution du risque contextuel

Lorsqu'il s'agit d'analyser le risque de sécurité, nous sommes experts pour filtrer le bruit et prendre en compte le contexte, y compris la valeur de l'actif, l'exposition à Internet et les contrôles compensatoires. Maintenant, nous changeons la façon dont nous voyons le signal.

En 2026, nous remanions la façon dont le risque de sécurité est visualisé, transformant des calculs complexes en une carte de haute fidélité de l'exposition de l'entreprise. Nous normalisons également les évaluations pour les cas limites et validons notre inventaire d'actifs pour garantir que notre image est complète. Cette évolution convertit les données de risque abstraites en signaux d'affaires clairs et indéniables, rendant la prochaine bonne décision évidente pour chaque responsable de la prise de décisions.