



Rapport annuel 2021 sur les titres

Accélérer notre leadership
en matière de sécurité

La sécurité ne devrait pas être un secret commercial. Nous croyons qu'une meilleure communication, une plus grande collaboration et une plus grande transparence sont synonymes d'une plus grande sécurité. C'est pourquoi notre équipe a élaboré ce rapport et c'est pourquoi nous collaborons activement avec les clients, les décideurs et d'autres organisations au sujet des défis et des possibilités en matière de cybersécurité.

- 3** Notre impact
- 4** Lettre du PDG Mark W. Begor
- 5** Lettre du CISO Jamil Farshchi
- 6** État des lieux
- 7** Nos actions
- 9** Poursuivre notre transformation en matière de sécurité
- 10** Analyse comparative indépendante
- 11** Résumé des résultats
- 14** Il n'y a pas de limite à la sécurité

Notre impact

Sécurité d'Equifax en 2021

- 35 millions +** Cybermenaces défendues en moyenne chaque jour
- 370,000 +** Simulations lancées pour tester notre effectif mondial en sécurité
- 11,000 +** Employés et plus ont reçu une formation personnalisée sur la sécurité
- 1000 +** Analyses de risques approfondies réalisées sur les partenaires de la chaîne d'approvisionnement numérique
- 800 +** Organisations soutenues par les services de brèches d'Equifax
- 600 +** Professionnels de la cybersécurité protégeant les données des consommateurs
- 160 +** Contrôles de sécurité en nuage automatisés surveillés en temps réel
- 150 +** Nouveaux produits Equifax mis sur le marché en toute sécurité
- 50 +** Forums ont participé pour relever les défis cybernétiques mondiaux
- 20** Attestations et autorisations obtenues de vérificateurs externes
- 14** Exercices de simulation pour préparer les scénarios de crise
- 8** Acquisitions évaluées au moyen d'évaluations robustes des risques
- 0** Vulnérabilités critiques et à périmètre élevé hors SLA



Mark W. Begor

Président-directeur général

Equifax

Nous sommes un nouveau Equifax.

Au cours des quatre dernières années, nous avons transformé notre organisation à tous les niveaux en investissant 1,5 milliard de dollars dans la technologie et la sécurité pour construire le nuage Equifax. Nous sommes vraiment une entreprise de données, d'analyses et de technologie diversifiée qui a pris de l'expansion bien au-delà d'un bureau de crédit traditionnel – et nous ne faisons que commencer.

Lorsque je me suis joint à Equifax en 2018, je me suis personnellement engagé à faire d'Equifax un **leader de l'industrie en matière de sécurité** des données et à bâtir une culture où la sécurité fait partie de l'ADN de notre entreprise. Depuis, presque tous les aspects de notre programme de sécurité ont été complètement remaniés, et les résultats sont éloquentes. Dans de multiples évaluations indépendantes, nos capacités de sécurité dépassent maintenant toutes les principales références de l'industrie. Nous sommes extrêmement fiers des progrès incroyables que nous avons réalisés pour intégrer la sécurité dans tout ce que nous faisons – de notre infrastructure technologique, de notre tissu de données et du développement de produits à nos stratégies de fusion et d'acquisition, en passant par nos plans de rémunération incitative.

Notre engagement à l'égard d'une sécurité de calibre mondial est l'une des principales priorités de notre stratégie environnementale, sociale et de gouvernance (ESG), et nous croyons que notre accent sur les facteurs ESG

permettra à notre entreprise de mieux se positionner pour assurer sa durabilité à long terme et de créer de la valeur pour les actionnaires. L'engagement en matière de sécurité couvre tous les niveaux de notre organisation : chaque employé d'Equifax reçoit une formation personnalisée sur la façon de repérer les menaces et a une visibilité sur son propre rendement en matière de sécurité. Et chaque employé admissible à une prime a une mesure de rendement en matière de sécurité incluse dans le calcul de sa rémunération incitative annuelle, ce qui l'aide à comprendre comment il contribue à protéger nos systèmes et à traiter la sécurité comme une priorité personnelle. Cela renforce notre culture et harmonise nos employés avec les progrès réalisés par rapport aux objectifs de notre programme de sécurité.

Chez Equifax, **nous croyons fermement que la sécurité ne devrait pas être un secret commercial.** Nous reconnaissons qu'une partie du rôle de leader de l'industrie en matière de sécurité des données consiste à faire preuve de transparence au sujet de nos apprentissages et à partager activement les pratiques exemplaires que nous recueillons alors que nous travaillons à mettre en œuvre le changement. Nous demeurons déterminés à travailler ouvertement avec nos pairs, nos clients, nos partenaires et les organismes de réglementation pour relever les nouveaux défis en matière de sécurité et documenter les pratiques exemplaires. Fournir un leadership éclairé essentiel en matière de sécurité des données et travailler ensemble pour offrir des solutions qui profitent à la fois à la communauté de la sécurité et à nos clients. C'est pourquoi nous publions ce rapport annuel sur la sécurité.

Les progrès que nous avons réalisés dans le domaine de la cybersécurité – en particulier ceux de la dernière année que vous lirez dans ce rapport – ne pouvaient pas arriver à un moment plus crucial. Les attaques contre les entreprises, les gouvernements et les particuliers sont plus répandues, plus complexes et plus percutantes que jamais. Parallèlement, chaque organisation accélère sa dépendance à l'égard de la technologie, et les consommateurs utilisent des points de contact numériques à des niveaux jamais vus auparavant.

Tout cela augmente les enjeux pour la sécurité des données, mais Equifax est prêt. Nous sommes fiers d'avoir mis en place l'un des programmes de cybersécurité les plus avancés et les plus efficaces dans le monde des affaires aujourd'hui, en nous défendant avec succès contre environ 35 millions de cybermenaces par jour l'an dernier, soit environ sept fois plus qu'en 2018. L'incident cybernétique que nous avons vécu en 2017 a été un catalyseur de transformation, et il nous a menés là où nous en sommes aujourd'hui, en nous faisant reconnaître comme une autorité de premier plan en matière de sécurité. **Chez Equifax, la sécurité est devenue un point fort et un avantage concurrentiel.** Mais nous n'en avons pas fini. Nous considérons la sécurité comme un facteur de différenciation clé et nous continuerons d'investir dans le leadership en matière de sécurité.



Jamil Farshchi
Dirigeant principal de la
sécurité de l'information
Equifax

Choisir l'action.

2021 a été une année charnière en matière de cybersécurité. Nous avons été témoins d'un nombre record d'atteintes à la sécurité des données, d'une vague d'attaques par rançongiciel, de la pénétration des chaînes d'approvisionnement numériques et de la perturbation de nos infrastructures essentielles.

Pour couronner le tout, nous avons conclu l'année avec une vulnérabilité Log4j historique et la menace imminente d'un conflit entre la Russie et l'Ukraine.

Ajoutez à cela la dépendance technique croissante de la société, l'innovation dans des domaines comme l'intelligence artificielle, le Web3 et la 5G, et les retours financiers incroyables que les cybercriminels génèrent, et il est indéniable que des niveaux sans précédent de risque cybernétique sont relâchés sur nous.

C'est la réalité d'aujourd'hui. Le risque évolue et s'accélère, et il est clair que le maintien du statu quo en matière de cybersécurité est intenable.

Les options ne manquent pas. Nous avons devant nous une liste urgente de mesures à prendre en matière de cybersécurité : nouvelles politiques et réglementation, meilleure technologie et innovation, plus d'investissements

et de collaboration, plus de formation et de perfectionnement. Et pourtant, beaucoup trop d'organisations ont choisi de rester dans le statu quo... pour simplement attendre et voir, pour espérer le meilleur.

Il s'agit d'une erreur de calcul fatale. Peu de risques ministériels (s'il y en a) ont à la fois la probabilité et l'incidence que les cybermenaces aient. Non seulement les attaques sont une certitude, mais elles paralysent constamment les activités commerciales, génèrent des responsabilités écrasantes et suscitent la colère des clients, des investisseurs, des organismes de réglementation et des médias. L'espoir est une stratégie dangereuse de gestion des risques.

Mais alors, **il y en a d'autres qui choisissent l'action. Ceux qui investissent, innovent et collaborent de manière à rendre leur entreprise et leur entourage plus sûrs.** Ces entreprises savent que ce qui a été fait auparavant ne freinera pas la tendance des attaques réussies. Ils savent que nous devons constamment relever la barre afin de déjouer les cybercriminels de façon intelligente, efficace et novatrice. Ils reconnaissent qu'il n'y a pas de ligne d'arrivée en matière de sécurité.

Il s'agit de l'approche d'Equifax depuis la cyberattaque de 2017 contre notre entreprise. Nous avons rehaussé la sécurité dans tous les aspects de notre activité, de la chaîne d'approvisionnement numérique aux fusions et acquisitions en passant par l'innovation en matière de nouveaux produits. Il est tout aussi important de continuer à miser sur la transparence, à prendre la parole et à aider d'autres organisations à renforcer la cybersécurité.

Malgré les défis, les menaces et l'incertitude qui existent dans le cyberspace, nous demeurons déterminés à être un leader en matière de sécurité. Nous avons choisi d'agir.

État des lieux

Menaces à la cybersécurité mondiale en 2021

Des organisations de toutes tailles et de toutes industries font face à une prolifération de problèmes de sécurité dans le monde.

C'est pourquoi nous avons créé le Cadre des conditions de menace. Notre équipe suit l'évolution rapide du contexte de cybersécurité et tient compte de ces événements réels lors de l'évaluation de notre niveau de menace à l'échelle de l'organisation.

Cadre des conditions de menace Equifax

Equifax Security gère notre niveau de menace d'entreprise qui s'ajuste en fonction d'un éventail de facteurs. Pour chaque niveau de menace – Sévère, Élevé, Élevé, Gardé – nous avons une série de processus prédéfinis qui activent diverses actions de notre équipe. Notre niveau de menace à l'échelle de l'organisation est régulièrement signalé à l'équipe de la haute direction et au conseil d'administration de l'entreprise.

Sévère

Élevé

Élevé

Gardé

Les thèmes mentionnés ci-dessous résument les principales menaces liées à la connaissance de la situation macroéconomique dont nous avons été témoins en 2021.

Enregistrer le nombre d'atteintes à la protection des données

Les atteintes à la protection des données en 2021 ont dépassé les niveaux de l'année¹ et ont prouvé une fois de plus que tout le monde est une cible. Cependant, dans une mer de brèches, on se distingue du reste : un piratage massif de Microsoft Exchange, l'un des logiciels de messagerie les plus populaires dans le monde. L'incident a sonné l'alarme à la Maison-Blanche, qui a averti que les organisations avaient « des heures et non des jours » pour corriger les vulnérabilités. La violation était si grave qu'elle a incité le FBI à obtenir une ordonnance du tribunal permettant à l'agence d'accéder proactivement et de réparer les ordinateurs infectés à travers les États-Unis.

Forte augmentation des attaques de ransomware

Les ransomwares existent depuis des décennies, mais en 2021, les attaques contre des organisations, des villes et des particuliers ont atteint des niveaux sans précédent. Le plus grand fournisseur de viande du monde, un géant du conseil, un géant de l'assurance, et un grand fournisseur de paie, ont tous été détenus pour rançon. Une entreprise a versé un montant record de 40 millions de dollars à des cybercriminels. Le volume de paiements présumés par rançongiciel signalés par les banques américaines a presque doublé par rapport à 2020. La série d'attaques a incité des responsables de plus de 30 nations à organiser un sommet international pour faire face à la crise.

Cyberincidents sans précédent dans les infrastructures essentielles

Aucun ransomware n'a fait plus les manchettes que l'attaque contre Colonial Pipeline, l'exploitant du plus grand pipeline de carburant aux États-Unis. L'incident cybernétique a provoqué la panique sur la côte Est et a fait grimper les prix du gaz à leur plus haut niveau en sept ans. Pour la première fois, la cybersécurité est devenue une réalité pour des millions de personnes. De l'autre côté de l'Atlantique, en Irlande, une cyberattaque a paralysé tout le système de santé du pays, qui fournit des soins à 5 millions de personnes. Ce fut une attaque dévastatrice car les données des patients et les systèmes informatiques ont été rançonnés pendant des semaines.

Nouvelles vulnérabilités de logicielles qui causent des ravages

Une faille trouvée dans le code open-source largement utilisé connu sous le nom de Log4j affectait apparemment toutes les grandes entreprises, organisations et entités gouvernementales sur Terre. Cette vulnérabilité a été facilement exploitée et a mis en danger des centaines de millions de terminaux et de serveurs. Une société de sécurité a constaté qu'il y avait plus de 100 tentatives de piratage pour exploiter la vulnérabilité chaque minute. Parmi les victimes se trouvait le ministère belge de la Défense, qui a été forcé de fermer une partie de son réseau informatique après avoir découvert une cyberattaque impliquant Log4j. Un responsable de la cybersécurité des États-Unis a qualifié Log4j de « vulnérabilité la plus grave jamais vue dans sa carrière ».

¹Centre de ressources sur le vol d'identité, Rapport d'atteinte à la protection des données 2021

Nos actions

Initiatives de sécurité et résultats d'Equifax en 2021

Expansion de notre sécurité infonuagique



Nous avons amélioré notre sécurité infonuagique de premier niveau pour y inclure la validation et la surveillance automatisées. Notre migration vers le cloud nous donne une visibilité plus robuste sur la sécurité de notre entreprise, ce qui nous permet de détecter et de répondre aux menaces avec plus de rapidité et de précision.

En 2021, nous avons mis en œuvre plus de 160 vérifications de sécurité automatisées en nuage qui sont maintenant surveillées en temps réel.

Formation améliorée pour nos employés



Nous avons également personnalisé notre programme de formation sur la sécurité des employés et entièrement automatisé la prestation de l'apprentissage basé sur le comportement pour répondre aux besoins de notre entreprise mondiale. Reconnaisant la menace unique des attaques d'ingénierie sociale numérique, nous avons accéléré cette formation en ajoutant des déclencheurs émotionnels dans plus de 370 000 simulations que nous avons menées en 2021. Cela nous a permis de varier la difficulté de notre formation et de nous assurer que notre main-d'œuvre demeure compétente en matière de sécurité.

En 2021, notre cote de sensibilisation à la sécurité des employés a atteint un nouveau record de 98 sur 100, une amélioration considérable par rapport à 81 sur 100 en 2020. De plus, nos employés ont obtenu un taux de clics de simulation de 4,7 %, une amélioration de 110 % par rapport à 2020.

Renforcer la sécurité de notre chaîne d'approvisionnement numérique



Nous avons sécurisé notre chaîne d'approvisionnement numérique avec plus de détails, de rapidité et d'innovation. Malgré la complexité et l'imprévisibilité de la gestion de la chaîne d'approvisionnement de la plupart des organisations, notre équipe est en mesure d'évaluer plus efficacement les capacités de sécurité des plus de 5 000 fournisseurs qui soutiennent Equifax. Ce n'est pas la norme en matière de gestion des risques, mais c'est un excellent exemple de la façon dont nous protégeons l'ensemble de l'écosystème de notre entreprise.

En 2021, nous avons évalué la totalité des fournisseurs de notre entreprise et analysé en profondeur les risques de plus de 1 000 de nos partenaires de la chaîne d'approvisionnement numérique les plus importants.

Nos mesures :: Initiatives de sécurité et résultats d'Equifax en 2021

Renforcement de notre posture de gestion des risques à l'échelle mondiale



Nous avons élargi notre collection de mesures de sécurité spécifiques pour chacun des pays dans lesquels nous exerçons nos activités afin de renforcer notre posture de risque mondiale. Notre équipe analyse maintenant des mesures de risque de sécurité uniques à l'échelle régionale, comme la couverture des agents, la couverture des registres, l'exactitude de l'inventaire des actifs, la numérisation des codes d'application et la gestion du cycle de vie des certificats.

En 2021, nous avons obtenu des taux améliorés de couverture de 88 % pour les agents, de 88 % pour la journalisation, de 98 % pour l'inventaire des biens, de 71 % pour les demandes inscrites à la numérisation automatique des codes et de 98 % pour la gestion du cycle de vie des certificats dans nos régions autres que les États-Unis.

Transparence avancée en matière de cybersécurité



Nous avons continué de collaborer avec des intervenants du monde entier – des dirigeants et des décideurs, des universitaires et des responsables du renseignement, des associations commerciales et des propriétaires de petites entreprises – pour promouvoir une cybersécurité plus forte. En tirant parti de notre expertise et en partageant nos pratiques exemplaires, nous aidons les autres à se préparer et à se défendre contre les menaces émergentes.

En 2021, nous avons participé à plus de 50 forums pour faire avancer des idées et des solutions aux défis mondiaux en matière de cybersécurité, y compris des engagements avec le Federal Bureau of Investigation, le département d'État des États-Unis, la National Technology Security Coalition et le Forum économique mondial.

Favoriser la croissance des entreprises



Nous avons aidé notre entreprise à stimuler l'innovation, de façon plus sécuritaire. Notre équipe Sécurité a collaboré à l'échelle de l'organisation pour commercialiser un nombre record de nouveaux produits et créer de nouvelles occasions commerciales pour notre entreprise. Ces efforts ont clairement démontré qu'une bonne sécurité ne consiste pas seulement à lutter contre les attaques, mais aussi à favoriser les résultats nets.

En 2021, nous avons contribué à commercialiser en toute sécurité plus de 150 nouveaux produits pour les clients d'Equifax, lancé un environnement de sécurité FedRAMP à la fine pointe de la technologie pour soutenir le gouvernement des États-Unis dans le nuage et lancé de nouvelles activités dans des domaines comme l'identité et la fraude.

Poursuivre notre transformation en matière de sécurité

En 2017, Equifax a fait face à l'une des cyberattaques les plus importantes de l'histoire lorsque des membres de l'armée chinoise ont eu accès à notre réseau et aux renseignements personnels de plus de 147 millions de personnes.

Aujourd'hui, il y a très peu d'aspects de notre programme de sécurité qui n'ont pas été complètement remaniés par rapport à ce qui était en place en 2017.

Peu d'entreprises ont consacré plus de temps et de ressources à la protection des renseignements des consommateurs. Mais nous ne nous arrêtons pas là. Notre équipe s'engage à relever constamment la barre en matière de sécurité en :

Investissant

des capacités de cybersécurité de premier ordre et de l'établissement d'une culture axée sur la sécurité

Innovant

de manière à rendre nos activités, nos clients et les consommateurs plus sûrs

Collaborant

avec d'autres afin d'être une force pour le bien dans la cybersécurité

Nous avons transformé notre programme de sécurité à tous les niveaux.

Investissement de 1,5 milliard de dollars pour reconstruire nos capacités technologiques et de sécurité à partir de zéro

Migration de notre entreprise vers le nuage, ce qui nous donne une meilleure visibilité des données qui entrent et sortent de notre environnement

Construction d'un centre de fusion électronique de 7,3 millions de dollars qui prend en charge la détection et l'intervention en tout temps

Embauche de plus de 600 professionnels de la cybersécurité hautement qualifiés pour réagir aux menaces avec rapidité et précision

Nous avons modifié notre structure organisationnelle en rehaussant la sécurité pour relever directement de notre chef de la direction

Renforcement de la façon dont les membres du Conseil évaluent les principaux secteurs de risque dans l'ensemble de l'organisation

Mise en place d'un programme rigoureux de formation des employés sur la sécurité avec simulations mensuelles et fiches de pointage personnalisées

Validation et surveillance automatisées intégrées de plus de 160 contrôles de sécurité en nuage en temps réel

Lancement d'un environnement de sécurité FedRAMP de pointe pour soutenir les clients du gouvernement américain dans le cloud

Inscription de plus de 3 000 fournisseurs et tiers à la surveillance continue des risques

Développé CloudControl, une plateforme qui donne aux clients une visibilité en temps réel de la sécurité de leurs produits et services Equifax Cloud

Acquisition de Appriss Insights, une source de premier plan de renseignements sur les risques et la justice pénale, et de Kount, un leader mondial des solutions d'identité numérique et de fraude

Obtention de certifications et d'autorisations, y compris PCI DSS, ISO 27001, SOC 1, SOC 2 et FISMA

Analyse comparative indépendante

Échéance du titre

Un cabinet de recherche et de conseil international de premier plan effectue chaque année une analyse approfondie de la maturité de l'ensemble de notre programme de sécurité.

2021 Score de maturité de sécurité



Qu'est-ce que la maturité des titres?

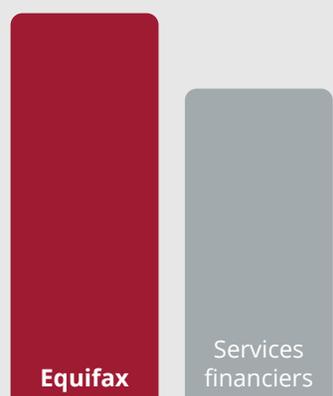
La maturité d'une organisation en matière de sécurité représente sa capacité à s'adapter aux cybermenaces et à gérer les risques au fil du temps.

À la fin de 2021, la maturité de notre programme de cybersécurité a surpassé tous les principaux indices de référence du secteur pour une deuxième année consécutive.

Posture de sécurité

Un service de signalement de cybersécurité de premier plan surveille continuellement la posture de notre programme de sécurité et évalue le risque de notre écosystème de la chaîne d'approvisionnement.

Côte de posture de sécurité 2021



Qu'est-ce que la posture de sécurité?

La posture de sécurité d'une organisation est sa préparation et sa capacité à identifier les menaces et les risques de sécurité, à y répondre et à s'en remettre.

À la fin de l'année 2021, nos capacités de sécurité se classaient dans le 1 % supérieur des sociétés de technologie et de services financiers analysées.

Résumé des résultats

Sécurité d'Equifax en 2021

Maturité et posture des titres

- Dépenses de cybersécurité optimisées en pourcentage du budget de TI à 10 %, en deçà de la moyenne de l'industrie de 10,6 %²
- Nous avons obtenu une cote d'échéance des titres qui a surpassé tous les principaux indices de référence du secteur pour une deuxième année consécutive
- Nous avons obtenu une cote de sécurité de 1 % des entreprises de technologie et de services financiers analysées.

Cybersécurité

- Mise en œuvre de plus de 160 vérifications de sécurité automatisées en nuage qui sont surveillées en temps réel
- Maintien de 0 vulnérabilité critique et à périmètre élevé en dehors de notre Accord sur les niveaux de service (ANS)
- Nous avons étendu le balayage automatisé des codes à 92 % de nos demandes (comparativement à 54 % en 2020)
- Authentification multifactorielle forcée pour 100 % de l'accès à distance à notre réseau

Conformité

- Nous avons obtenu 20 certifications et évaluations de vérificateurs externes qui valident notre conformité aux exigences commerciales, juridiques, contractuelles et réglementaires, notamment :
 - PCI-DSS : Normes relatives aux cartes de paiement
 - ISO 27001 : Contrôles de gestion de la sécurité
 - COS 2 : Rapport sur la sécurité, la disponibilité et la confidentialité
 - COS 1 : Rapport sur les contrôles de vérification

Fusion et d'acquisition

- Fait preuve d'une diligence raisonnable rigoureuse à l'égard de huit acquisitions, y compris une analyse exhaustive des vulnérabilités, un examen des codes et une évaluation des compromis, avant la conclusion
- Diriger les efforts de correction et d'intégration pour chaque acquisition afin de s'assurer que les nouvelles entités sont exploitées conformément à nos contrôles de base
- Il est à noter que nous avons facilité deux des cinq plus importantes acquisitions de l'histoire d'Equifax : Appriss Insights, une source de premier plan de renseignements sur les risques et la justice pénale, et Kount, un leader mondial des solutions d'identité numérique et de fraude

Gestion des risques

- Réalisation d'évaluations sur 100 % des fournisseurs de notre entreprise
- Réalisation d'analyses de risque approfondies sur plus de 1000 de nos partenaires de la chaîne d'approvisionnement numérique les plus critiques
- Nous avons intégré plusieurs nouveaux clients à CloudControl, une plateforme unique dans l'industrie qui donne aux clients une visibilité en temps réel de la sécurité des produits et services Equifax Cloud qu'ils utilisent

²IANS et ARTICO, Étude comparative du budget de la sécurité pour 2021

Résumé des résultats :: Sécurité d'Equifax en 2021

Gestion des crises

- Réalisation de 14 exercices de simulation sur table et simulations de crise en temps réel avec les intervenants de l'entreprise. Les principaux intervenants comprenaient :
 - Conseil d'administration
 - PDG et équipe de direction
 - Équipes de crise régionales et des unités opérationnelles
- Révision du cadre de notre programme d'intervention d'urgence

Formation en Matière de Sécurité

- Nous avons effectué plus de 370 000 simulations pour tester notre effectif en matière de sécurité
- Production de fiches de pointage de sécurité personnalisées pour chaque employé chaque mois afin de renseigner notre effectif sur son rendement en matière de cybersécurité
- Augmentation de la cote de sensibilisation à la sécurité des employés à 98 sur 100 (comparativement à 81 en 2020)
- Réduction du taux de clics par simulation auprès des employés à 4,9 % (amélioration de 110 % par rapport à 2020)

Services d'atteinte à la vie privée

- Soutenu plus de 800 organisations et leurs clients, les aidant à réagir aux incidents cybernétiques et à s'en remettre

Engagement Client

- Rempli plus de 1 900 questionnaires et vérifications au nom des clients d'Equifax pour assurer la conformité
- Tenue de sommets et de tables rondes sur la sécurité des clients en Australie, au Canada et au Royaume-Uni pour accroître la transparence

Produits et services

- Lancement d'un environnement de sécurité de pointe FedRAMP pour soutenir le gouvernement américain dans le cloud
- En toute sécurité, 151 nouveaux produits ont été mis sur le marché pour nos clients (comparativement à 134 en 2020)

Confidentialité

- Lancement d'un nouveau processus d'évaluation des facteurs relatifs à la vie privée axé sur les risques aux États-Unis et au Canada
- Conception et mise en œuvre d'un processus de gouvernance pour les zones de données privilégiées
- Nous avons déployé un nouvel outil pour appuyer la découverte de données à l'échelle de l'organisation, ce qui nous permet de mieux trier, gérer et protéger nos données

Fraude

- Nous avons continué de faire évoluer notre moteur d'évaluation des risques, en commençant notre transition de la logique de décision codée en dur à des modèles couplés à des attributs de risque dynamiques

Résumé des résultats :: Sécurité d'Equifax en 2021

Sécurité matérielle et enquêtes

- Réalisation de huit essais de pénétration physique pour déterminer les domaines où il y a des améliorations continues dans la prévention de l'accès non autorisé aux installations
- Réalisation de 39 évaluations de la sécurité matérielle confirmant que des contrôles appropriés sont en place pour protéger les employés, les données et les biens
- Grâce à l'amélioration des processus et de l'automatisation, notre Centre des opérations de la sécurité physique a amélioré notre délai de réponse pour :
 - Alarmes locales de haute priorité : dans les 4 minutes
 - Rapports de renseignement entrants : dans les 5 minutes
- Atténuation/suppression de 1,3 milliard de dollars de transactions frauduleuses de consommateurs et d'entreprises

Talent et la Diversité

- Continuer à accroître la diversité au sein de notre effectif en atteignant :
 - 26 % de femmes au sein de l'équipe aux États-Unis (contre 24 % en moyenne dans l'industrie³)
 - 17 % de membres noirs de l'équipe aux États-Unis (contre 9 % en moyenne dans l'industrie³)

Plaidoyer et de Partenariat

- Participation à plus de 50 forums pour promouvoir une cybersécurité plus forte pour les entreprises, le gouvernement et la société
- Renforcement des partenariats avec les organismes d'application de la loi pour lutter contre la fraude, le vol d'identité et l'identification des activités criminelles
- Collaboration avec des organisations pour faire progresser les idées et les solutions aux défis mondiaux en matière de cybersécurité, notamment :
 - Conseil de l'Atlantique
 - Fondation pour la défense des démocraties
 - Bureau fédéral d'enquête
 - National Technology Security Coalition
 - Département d'État des États-Unis
 - Forum économique mondial
- Publication du premier rapport annuel sur la sécurité, dans le cadre de notre engagement continu à accroître la transparence en matière de cybersécurité

³Aspen Institute, 2021 Diversity, Equity, and Inclusion in Cybersecurity Report

Il n'y a pas de limite à la sécurité

Nos priorités en 2022

Optimisation de notre portefeuille de fusions et acquisitions



Fusion et Acquisition reste un pilier important de la stratégie de croissance de l'EFX 2023, et Security est chargé d'évaluer le risque de sécurité de chaque cible d'acquisition. À mesure que le paysage des fusions et acquisitions évolue, nous constatons un volume de transactions plus important, une concurrence accrue et des périodes de diligence plus courtes.

Alors que nous continuons d'accélérer nos activités de suivi et d'analyse stratégiques, nous tirons parti de nouveaux outils et de processus optimisés qui nous permettent de repérer les signaux avertisseurs, de remédier aux menaces plus rapidement et de simplifier la phase d'intégration.

Renforcer la technologie de cybersécurité de la prochaine génération



Lorsqu'il s'agit de sécuriser notre entreprise, nous nous engageons à relever constamment la barre. C'est pourquoi nous travaillons avec des chefs de file novateurs dans le domaine de la sécurité en tant que partenaires de conception pour aider à rehausser encore davantage nos capacités fondamentales en matière de cybersécurité.

Cette technologie de cybersécurité de prochaine génération repose fortement sur l'intelligence artificielle, le cloud et l'automatisation. En fin de compte, cela nous permettra de recueillir de meilleurs renseignements, de détecter et d'arrêter les menaces plus rapidement et de réduire les risques pour notre entreprise.

Accélérer la sécurité sans friction



Nous intégrons le libre-service et l'automatisation à l'échelle de notre entreprise. Pourquoi? Parce que nos équipes ne devraient pas avoir à choisir entre une meilleure sécurité et une plus grande innovation. Nous pouvons avoir les deux.

En introduisant des choses comme la prise de décision en temps réel sur les risques, la numérisation simplifiée des codes et la surveillance continue de la chaîne d'approvisionnement, nous serons en mesure de maintenir notre leadership en matière de sécurité tout en réduisant le fardeau de nos employés.



[equifax.com](https://www.equifax.com)

Copyright © 2022 Equifax Inc. Tous droits réservés. Equifax et les marques Equifax utilisées dans le présent document sont des marques de commerce d'Equifax Inc. Autres marques et noms de sociétés mentionnés dans le présent document sont la propriété de leurs propriétaires respectifs. Sauf indication contraire, les renseignements sont en date de décembre 2021. 22-106647