REPORT

Panorama de la cybersécurité en France

Vulnérabilités de la supply chain cyber et menaces croissantes

SecurityScorecard

Avant propos

Les plus grandes entreprises françaises restent exposées aux risques cyber au travers de leur écosystème de fournisseurs.

L'ampleur des vulnérabilités ayant affecté des tiers et quatrièmes parties au cours des douze derniers mois révèle en effet des problématiques récurrentes de sécurisation et surveillance de la chaîne d'approvisionnement numérique.

Ce rapport présente une analyse indépendante réalisée par SecurityScorecard sur la posture cybersécurité des 100 plus grandes entreprises françaises (Classées par capitalisation boursière).

Il met en évidence les vulnérabilités sectorielles persistantes, les incidents ayant affecté des services essentiels ainsi que les axes d'amélioration prioritaires .

Cette analyse met ainsi en exergue l'importance de renforcer le contrôle sur les risques liés aux tiers et d'exiger un meilleur niveau de sécurité, notamment pour les fournisseurs critiques.

Principaux constats

SecurityScorecard a évalué les 100 plus grandes entreprises françaises selon plusieurs critères de cybersécurité tels que la sécurité du réseau, les infections par des logiciels malveillants, la sécurité des terminaux, la fréquence d'application des correctifs, la sécurité applicative et la santé du DNS. Les résultats de ces analyses révèlent des vulnérabilités préoccupantes :

98 % des entreprises ont subi une violation de données au sein de leur écosystème de tiers au cours des douze derniers mois, un chiffre identique à celui du rapport précédent.

100 % travaillent avec au moins un fournisseur de quatrième niveau ayant subi une violation de données.

.

4 % ont subi une violation de données directe au cours des 12 derniers mois, en baisse par rapport aux 7% du rapport de l'année précédente.

Les **25 premières entreprises**, par capitalisation boursière, ont été deux fois plus impactées par des violations liées aux tiers que les 25 dernières entreprises.

94 % des entreprises notées A n'ont subi aucune violation de données au cours des 12 derniers mois (soulignant la corrélation entre note élevée et résilience).

29 % des entreprises ont une note entre C et F (en baisse par rapport aux 40% du dernier rapport), contre une moyenne européenne de 31%.

Le **secteur industriel** est le plus robuste avec 87% des entreprises obtenant une note B ou supérieure. A l'inverse, dans le secteur de la construction, 100% ont une note entre C et F, et toutes ont été exposées à une violation de données au sein de leur écosystème de tiers.

Introduction

L'année 2024 a été marquée par des défis significatifs sur le plan cyber en France.

Le rapport annuel de SecurityScorecard des 100 plus grandes entreprises françaises révèle que 98% d'entre elles ont subi des attaques au sein de leur écosystème de tiers. Ce constat confirme ainsi le niveau de vulnérabilité persistante affectant la chaîne d'approvisionnement numérique.

Si l'ampleur des vulnérabilités liées aux tiers reste inchangée par rapport au dernier rapport, la part d'entreprises touchées directement diminue légèrement (de 7 % à 4 %), indiquant des progrès relatifs en matière de défenses cyber internes.

Le secteur de la construction et des infrastructures s'est révélé particulièrement vulnérable, toutes les entreprises évaluées recevant une note entre C et F, signalant des faiblesses de sécurité généralisées.

En revanche, le secteur industriel a démontré une nette amélioration, avec une baisse de 42% à seulement 13% des entreprises obtenant une note entre C et F - **un signe prometteur en matière de résilience.**

En août 2024, l'Université Paris-Saclay a été ciblée par le groupe de ransomware RansomHouse. Le groupe a revendiqué la responsabilité de l'infiltration des systèmes de l'université et de l'exfiltration d'environ un téraoctet de données sensibles, y compris des informations personnelles telles que des CV et des relevés de notes de 44 candidats en master.

L'université a réagi rapidement en informant les personnes concernées et en refusant de payer la rançon. Cet incident a non seulement perturbé les opérations, mais a également mis en évidence la montée des menaces cybernétiques auxquelles sont confrontés les établissements d'enseignement et le secteur public dans son ensemble.

Par ailleurs, durant les Jeux olympiques d'été de Paris 2024, une attaque par ransomware sur le réseau du Grand Palais a provoqué d'importantes perturbations opérationnelles, entraînant la fermeture des systèmes internes afin d'enrayer toute propagation.

Ces développements soulignent l'urgence, pour les organisations de tous les secteurs en France, de renforcer le contrôle de leur écosystème cybersécurité.

La mise en place de protocoles de sécurité robustes, la conduite régulière d'évaluation des risques liés aux tiers et la promotion d'une culture de sensibilisation à la cybersécurité constituent des leviers essentiels pour atténuer les risques posés par un environnement numérique de plus en plus complexe.

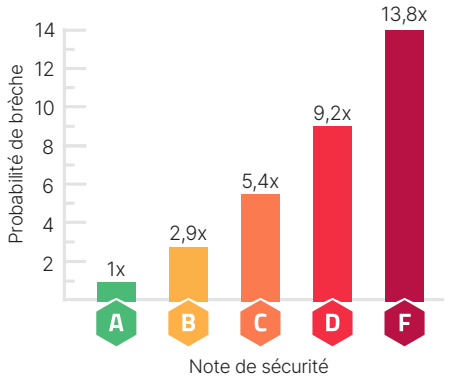
Paysage des menaces cybernétiques des 100 plus grandes entreprises françaises

Résultats

Notes globaux:

- A: 33%
- B: 38%
- C: 18%
- D: 10%
- F: 1%

Anticiper la probabilité d'une brèche



$ 4,5 M

Le coût global moyen d'une violation de données est de 4,5 millions de dollars.

IBM Security,
Cost of Doing Data Breach Report 2023

Aperçu Sectoriel

Risques cyber liés à la supply chain

Les chaînes d'approvisionnement sont devenues une cible stratégique et représentent une porte d'entrée pour les attaquants. La sécurité d'une organisation n'est jamais plus solide que celle de son fournisseur le plus vulnérable. Aucune organisation n'est à l'abri, y compris les entreprises dotées de solides systèmes de défense. Celles-ci demeurent exposées aux failles potentielles de leurs fournisseurs de troisième et quatrième partie.

La dernière analyse de de SecurityScorecard avait révélé que 98 % des entreprises travaillent avec un tiers ayant subi une violation de données.

Ce nouveau rapport confirme que les secteurs affichant les plus faibles notes de cybersécurité sont aussi ceux qui doivent gérer les écosystèmes de fournisseurs les plus complexes, augmentant ainsi leur exposition aux risques liés aux tiers, quatrièmes parties, et au-delà.

> **"Avec 98 % des plus grandes entreprises françaises affectées par des violations de données impliquant des tiers, le temps de la complaisance est révolu. Alors que les acteurs malveillants exploitent les vulnérabilités de la chaîne d'approvisionnement, les organisations doivent assumer la responsabilité de la sécurité sur l'ensemble de leur écosystème numérique. En 2025, la responsabilité ne sera plus une option Il est temps d'agir, d'évaluer, et de sécuriser. La résilience cybernétique n'est plus un avantage concurrentiel mais une exigence stratégique."**
>
> — Corian (Cory) Kennedy, Senior Manager, Threat Insights & Attribution, SecurityScorecard

Construction

Le secteur de la construction et des infrastructures enregistre les notes de cybersécurité les plus faibles, 100 % des entreprises évaluées obtenant une note entre C et F.

L'exposition numérique du secteur (plans confidentiels, contrats sensibles et données d'appels d'offres) en fait une cible de choix pour les cybercriminels. Une cybersécurité déficiente expose ces entreprises à des risques de ransomware, de fraude et de violations de données, pouvant entraîner retards de projet, pertes financières et menaces pour la sécurité physique.

En outre, les incidents de cybersécurité peuvent porter atteinte à la réputation des entreprises, entraîner des sanctions réglementaires et faire grimper les primes d'assurance

Industrie

A l'inverse, le secteur industriel affiche la meilleure performance en matière de cybersécurité, avec seulement 13 % des entreprises recevant une note entre C et F, soit une nette amélioration par rapport aux 42 % observées dans le rapport précédent.

Cependant, l'essor de l'Internet des objets (IoT), des usines intelligentes et de l'automatisation multiplie les vecteurs d'attaque. Les cyberattaques dans ce secteur peuvent provoquer des pannes d'équipements, des interruptions opérationnelles, des actes de sabotage et des fuites de données sensibles ou de secrets industriels, avec des effets potentiellement dévastateurs sur l'ensemble de la chaîne d'approvisionnement.

Scores par secteur

Automobile & Mobilité

40 %

40 % des entreprises ont une note entre C et F (en hausse par rapport à 33 % dans le dernier rapport

729
violations

729 violations de données de tiers au cours des 12 derniers mois

0 %
violations directe

0 % ont été victimes d'une violation de données directe (inchangé par rapport au rapport précédent)

100 %
violations de tiers

100 % sont en relation avec un tiers ayant subi une violation de données

Construction

100 %

100 % des entreprises ont une note entre C et F

846
violations

846 violations de données de tiers au cours des 12 derniers mois

0 %
violations directe

0 % ont été victimes d'une violation de données (inchangé par rapport au rapport précédent)

100 %
violations de tiers

100 % sont en relation avec un tiers ayant subi une violation de données

Scores par secteur

Biens de consommation & Distribution

22 %

22 % des entreprises ont une note entre C et F (en baisse par rapport à 42 % l'an dernier)

1506
violations

1506 violations de données de tiers au cours des 12 derniers mois

0 %
violations directe

0 % ont été victimes d'une violation de données (inchangé par rapport au rapport précédent)

100 %
violations de tiers

100 % sont en relation avec un tiers ayant subi une violation de données

Énergie & Services publics

40 %

40 % des entreprises ont une note entre C et F (en hausse par rapport à 29 % l'an dernier)

743
violations

743 violations de données de tiers au cours des 12 derniers mois

0 %
violations directe

0 % ont été victimes d'une violation de données (en baisse par rapport à 14 % dans le dernier rapport)

100 %
violations de tiers

100 % sont en relation avec un tiers ayant subi une violation de données

Finance

19 %

19 % des entreprises ont une note entre C et F (en baisse par rapport à 33 % l'an dernier)

1280
violations

1280 violations de données de tiers au cours des 12 derniers mois

0 %
violations directe

0 % ont été victimes d'une violation de données (inchangé par rapport au rapport précédent)

93,75 %
violations de tiers

93,75 % sont en relation avec un tiers ayant subi une violation de données

Scores par secteur

Industrie

13 %

13 % des entreprises ont une note entre C et F (en baisse par rapport à 42 % l'an dernier)

1325
violations

1325 violations de données de tiers au cours des 12 derniers mois

13 %
violations directe

13 % ont été victimes d'une violation de données

93,75 %
violations de tiers

93,75 % sont en relation avec un tiers ayant subi une violation de données

Technologie & Services informatiques

33 %

33 % des entreprises ont une note entre C et F (en baisse par rapport à 44 % l'an dernier)

1076
violations

1076 violations de données de tiers au cours des 12 derniers mois

33 %
violations directe

33 % ont été victimes d'une violation de données (en hausse par rapport à 22 % l'an dernier)

80 %
violations de tiers

80 % sont en relation avec un tiers ayant subi une violation de données

Concentration des risques cyber : Une préoccupation croissante

Le rapport Global Cyber Resilience Scorecard met en lumière une tendance préoccupante : dix groupes de cybercriminels sont à l'origine de 44 % des incidents mondiaux, avec le groupe C10p en tête des violations de données liées aux tiers. Cette concentration de l'activité malveillante représente une vulnérabilité systémique majeure.

Le rapport Redefining Resilience: Concentrated Cyber Risk in a Global Economy, élaboré en partenariat avec McKinsey & Company, révèle un autre facteur aggravant : 15 entreprises seulement contrôlent 62 % du marché technologique mondial. Cette domination crée une forte interdépendance et accroît le risque de propagation en cas d'attaque.

Du fait de leur envergure et de leur présence mondiale, ces entreprises technologiques peuvent involontairement servir de vecteurs aux risques tiers, touchant potentiellement des milliers d'organisations. Leur vaste empreinte numérique en fait des cibles privilégiées, et lorsqu'elles sont attaquées, les conséquences peuvent être considérables.

L'attaque de février 2024 contre Change Healthcare en est un exemple marquant. En tant que l'un des principaux gestionnaires de réclamations médicales aux États-Unis, l'entreprise a été contrainte de mettre plus de 100 systèmes hors ligne. Cette paralysie a perturbé les services de santé, amenant certains prestataires au bord de la fermeture.

Risque de quatrième niveau : un angle mort croissant

Si les tiers occupent souvent le devant de la scène dans les évaluations des risques liés à la supply chain, les fournisseurs de quatrième niveau - autrement dit les fournisseurs des fournisseurs - peuvent représenter des menaces tout aussi sérieuses.

Selon ce rapport ,98 % des entreprises ont au moins une entité compromise dans leur écosystème de tiers, faisant écho aux conclusions d'un autre rapport de SecurityScorecard selon lequel 98 % des grandes entreprises européennes travaillent avec un fournisseur de quatrième niveau ayant subi une violation de données.

Ces chiffres soulignent l'urgence de cartographier, surveiller et évaluer la posture de sécurité de tout son écosystème, et non uniquement des fournisseurs directs. En effet, plus l'écosystème est vaste, plus la surface d'exposition s'accroît.

Les conséquences sont bien réelles. La vulnérabilité MOVEit, découverte au printemps 2023, continue d'entraîner des perturbations à grande échelle. Son impact financier, désormais estimé à plus de 65 milliards de dollars US, démontre qu'une seule faille peut déclencher des effets en chaîne d'une ampleur considérable.

Sécuriser les infrastructures critiques est essentiel

De nombreuses entreprises mentionnées dans ce rapport opèrent dans des secteurs essentiels, notamment les services publics, les télécommunications, les transports et la finance. Ces secteurs constituent l'épine dorsale de la société moderne, où la confiance du public doit rester inébranlable.

Face à cet enjeu, ces organisations doivent prendre des mesures proactives pour identifier les risques numériques au sein de leur supply chain, renforcer les contrôles et bâtir une véritable résilience. Pour découvrir des stratégies détaillées et des recommandations concrètes, nous vous invitons à consulter l'édition 2025 du Global Third-Party Breach Report de SecurityScorecard.

Recommandations et conclusion

En France, les questions de cybersécurité se trouvent à un tournant critique. Avec 98 % des plus grandes entreprises du pays exposées à des failles liées aux tiers et 100 % exposées via leur écosystème de fournisseurs de quatrième niveau, il est évident que les approches actuelles en matière de gestion des risques liés à la chaîne d'approvisionnement numérique ne sont plus adaptées.

Renforcer la cybersécurité est désormais une priorité pour de nombreuses entreprises françaises. Si beaucoup affichent des notes relativement élevées, l'exposition quasi généralisée aux risques liés aux tiers et aux quatrièmes parties met en évidence des vulnérabilités structurelles qu'il est urgent d'adresser.

Pour réduire ces risques et bâtir une résilience durable, SecurityScorecard recommande la mise en oeuvre d'un ensemble d'actions stratégiques et opérationnelles :

- **Sécurité des applications et des réseaux :** toutes les entreprises devraient prioriser l'amélioration de la sécurité des applications et des réseaux. Ces deux aspects sont fondamentaux pour se prémunir contre un large éventail de menaces cyber.

Pour les entreprises à haut risque, une attention particulière doit être portée sur :

- **Intégrité du DNS**
  Assurez la santé et l'intégrité de vos configurations du DNS. Une mauvaise configuration de ce composant critique peut être une source de vulnérabilités.
- **Sécurité des terminaux**
  Renforcez la sécurité de tous les terminaux, notamment des ordinateurs portables, ordinateurs de bureau, appareils mobiles et appareils informatiques personnels (BYOD). Ces équipements non sécurisés sont des points d'entrée fréquents pour les attaquants.
- **Fréquence des correctifs**
  Mettez en place un programme de gestion des correctifs pour vos systèmes, vos logiciels et votre matériel. Des mises à jour fréquentes permettent d'atténuer les vulnérabilités connues.

Le risque cyber doit être considéré comme un enjeu stratégique. Il doit être pleinement intégré aux processus d'achat, aux évaluations de fournisseurs et à la planification de la résilience opérationnelle.

Ce rapport constitue un signal d'alarme pour les dirigeants, les professionnels de la cybersécurité et les décideurs politiques.

SecurityScorecard appelle toutes les organisations à :

- Prendre immédiatement la responsabilité de leurs écosystèmes numériques en assurant une surveillance continue des risques liés aux tiers et quatrièmes parties.
- Exiger davantage de transparence et de responsabilité de la part de leurs fournisseurs critiques.
- Utiliser la notation cyber comme indicateur de performance continue, non seulement pour répondre aux exigences de conformité, mais également pour mettre en place des améliorations concrètes et durables.
- Se mesurer aux secteurs les plus performants et adopter les meilleures pratiques.

La confiance, la continuité opérationnelle et la résilience économique reposent sur une chaîne d'approvisionnement sécurisée et transparente. En sécurisant l'ensemble de leur écosystème, les organisations françaises peuvent montrer l'exemple : transformer la vulnérabilité en vigilance et bâtir une cybersécurité solide, à la hauteur des défis de demain.

La résilience commence par la visibilité. Le moment d'évaluer, d'agir et de sécuriser, c'est maintenant.

Méthodologie

Les menaces sont en perpétuelle évolution, il est donc indispensable de mettre en place une évaluation en temps réel. Les risques cyber doivent être évalués sur la base de données. SecurityScorecard recueille des quantités considérables de données de façon non intrusive sur l'hygiène cyber des entreprises du monde entier. Ces données nous permettent d'évaluer les défenses des entreprises contre les menaces cyber.

Nous attribuons un score global (de A à F) sur la base de dix facteurs prédictifs d'une violation de données.

Ce rapport étudie le niveau de cybersécurité des 100 plus grandes entreprises françaises en termes de capitalisation boursière entre le 18 mars 2024 et le 18 mars 2025.

Annexe – qu'est-ce qu'une notation de sécurité ?

SecurityScorecard fournit aux organisations une vision complète de leur posture de sécurité, y compris les risques liés aux fournisseurs de tiers et de quatrièmes niveaux.

Les notations de sécurité sont entièrement fondées sur des preuves concrètes ; chaque note repose sur une observation sous-jacente et transparente, issue de l'analyse de l'ensemble de l'espace IPv4. Corrélés avec des données d'incident, les facteurs analysés par SecurityScorecard permettent aux organisations de cibler les domaines à renforcer pour réduire leur exposition au risque. Voici les dix facteurs :

- La sécurité du réseau vérifie les ports ouverts (tels que SMB et RDP), les certificats SSL non sécurisés ou mal configurés, les vulnérabilités des bases de données et les vulnérabilités IoT.
- L'intégrité du DNS vérifie les mauvaises configurations, telles que les Resolvers ouverts, ainsi que les configurations recommandées pour DNSSEC, SPF, DKIM et DMARC.
- La fréquence des correctifs mesure la fréquence des mises à jour des services, logiciels et matériels identifiés au sein d'une entreprise.
- La sécurité des terminaux mesure les versions et l'exploitabilité des ordinateurs portables, ordinateurs de bureau, appareils mobiles et appareils BYOD qui accèdent aux réseaux de l'entreprise.
- Les signaux liés à la réputation IP sont collectés par le système sinkhole de SecurityScorecard, qui ingère des millions de signaux de logiciels malveillants provenant d'infrastructures de commande et contrôle (C2) du monde entier. Les adresses IP infectées identifiées sont mises en correspondance avec les entreprises concernées.
- Les échanges entre hackers sont recueillis sur des sites Web illégaux et le dark Web où ils discutent des entreprises et des adresses IP ciblées.
- Les fuites d'informations sont des informations d'identification compromises qui ont été exposées dans le cadre d'une violation ou d'une fuite de données, de vidages de keylogger, de vidages de pastebin, de vidages de bases de données et d'autres référentiels d'informations.
- Les scores Cubit sont calculés à l'aide de l'algorithme de menace exclusif de SecurityScorecard qui mesure un ensemble de problèmes critiques de sécurité et de configuration, tels que les panneaux de commande administratifs exposés.
- La sécurité des applications s'appuie sur des renseignements de vulnérabilité provenant de bases de données CVE (white hat et black hat) et de moteurs de recherche spécialisés.

Pour en savoir plus et créer un compte gratuit, visitez le site SecurityScorecard.com

À PROPOS DE SECURITYSCORECARD

SecurityScorecard a révolutionné la cybersécurité avec une solution de Supply Chain Detection and Response (SCDR), transformant la manière dont les organisations se protègent face aux attaques sur la chaîne d'approvisionnement, l'un des vecteurs de menace à la croissance la plus rapide.

Nos notations de sécurité, pour lesquelles nous sommes reconnus leaders du secteur, constituent le socle de cette approche. La solution SCDR surveille en continu les risques liés aux tiers grâce à des des évaluations automatisées, des notations basées sur des critères précis, et des données propriétaires de threat intelligence , afin d'éliminer les risques avant qu'ils ne se transforment en violation de données.

Grâce à la plateforme **MAX**, les organisations peuvent répondre aux incidents et déployer des actions correctives en s'appuyant sur notre réseau de partenaires de service, protégeant ainsi l'ensemble de leur écosystème. Cette démarche renforce la **résilience opérationnelle**, optimise la **gestion des risques tiers**.

Aujourd'hui, plus de 3 000 organisations nous font confiance, dont les deux tiers des entreprises du Fortune 100. SecurityScorecard est également reconnue comme ressource officielle par la U.S. Cybersecurity & Infrastructure Security Agency (CISA).

Financée par des investisseurs de premier rang tels que Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, NGP, Intel Capital et Riverwood Capital, SecurityScorecard propose une sécurisation de la chaîne d'approvisionnement de bout en bout, garantissant la continuité des activités.

Pour en savoir plus, rendez-vous sur securityscorecard.com ou suivez-nous sur LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io