

# Rapport 2020 sur la sécurité des paiements

Fiche d'information

**Trop peu d'entreprises comprennent les raisons qui les empêchent d'atteindre et de maintenir un niveau prévisible et satisfaisant de conformité et de protection des données. Le rapport Verizon 2020 sur la sécurité des paiements (PSR) – la dixième édition de cette série d'études – aborde les difficultés que les RSSI doivent surmonter pour concevoir, implémenter et maintenir une stratégie et un programme de sécurité efficaces et pérennes.**

## Nouvelle baisse du taux de conformité

La conformité au standard PCI DSS (Payment Card Industry Data Security Standard) continue de perdre du terrain. Le rapport PSR 2020 évalue la capacité des entreprises à maintenir des contrôles dans le temps, et non à prouver leur conformité une fois par an seulement.

Par exemple, pourquoi donner la priorité aux solutions technologiques quand le développement des capacités et processus laisse à désirer ? Comment les leaders peuvent-ils s'adapter, innover et évoluer afin de renforcer leur culture de la sécurité ? Dans notre rapport, nous présentons les principaux pièges à éviter et proposons des solutions aux problématiques des RSSI en matière de conformité de la sécurité des données. Nous explorons les éléments indispensables pour créer un programme de conformité insensible aux bouleversements externes en ces temps difficiles.

**L'appât du gain restait la principale motivation des cybercriminels puisqu'il était à l'origine de près de 9 compromissions sur 10 (86 %). Dans le retail, les attaques à visées financières représentaient 99 % des incidents, dans un contexte où les données de paiement sont encore et toujours les plus convoitées et lucratives. Par ailleurs, les applications web ont remplacé les systèmes de points de vente au titre de principal vecteur d'attaque dans ce secteur.<sup>1</sup>**

## Au sommaire du rapport PSR 2020 :

- Nouvelle baisse du taux de conformité PCI DSS
- Difficultés fréquentes des RSSI à obtenir l'implication de leur direction
- Top 7 des pièges à éviter en matière de gestion de la sécurité des données
- Cinq éléments clés d'un environnement de sécurité des données ultraperformant
- Calendrier type de la mise en conformité PCI DSS

## Principales conclusions

Si de nombreuses entreprises peinent à assurer leur conformité et la sécurité de leurs données, c'est parce qu'elles manquent de ressources ou que leurs dirigeants ne s'impliquent pas suffisamment. Dans beaucoup d'entre elles, la stratégie de sécurité des données est en décalage complet avec la stratégie d'entreprise et les opérations.

Quant aux RSSI, ils doivent composer avec des restrictions budgétaires, un vivier de recrues limité et nombre de problèmes à régler en urgence. C'est ainsi qu'ils privilégient une approche court-termiste : ils implémentent des technologies en guise de solution rapide plutôt que de développer des plans stratégiques de long terme avec le concours de leur direction. Lorsque ces solutions de fortune atteignent leurs limites, les RSSI quittent leur poste, dans les deux ans qui suivent pour la plupart. Et trop souvent, leur successeur adopte la même démarche.

Résultat : une baisse continue du taux de conformité PCI DSS depuis plusieurs années. D'après le rapport PSR 2020, seuls 27,9 % des entreprises étaient 100 % conformes lors de leur audit intermédiaire en 2019, ce qui équivaut à une baisse de 8,8 points par rapport à 2018. Entre 2017 et 2018, ce chiffre avait déjà perdu 5 points de pourcentage. L'appât du gain restait la principale motivation des cybercriminels puisqu'il était à l'origine de près de 9 compromissions sur 10 (86 %). Dans le retail, les attaques à visées financières représentaient 99 % des incidents, dans un contexte où les données de paiement sont encore et toujours les plus convoitées et lucratives. Par ailleurs, les applications web ont remplacé les systèmes de points de vente au titre de principal vecteur d'attaque dans ce secteur.<sup>1</sup>

---

Notre rapport PSR décortique les problématiques des RSSI et leur impact sur la conformité des entreprises à travers les 7 grands pièges à éviter en matière de gestion de la sécurité des données. Pour ses auteurs, puisque les problèmes ne sont pas d'ordre technologique, il ne rime à rien d'acquérir de nouveaux outils, matériels et applications pour les résoudre. Il s'agit plutôt de défis organisationnels nécessitant des compétences de gestion avancées :

- Création de processus formels
- Conception d'un business model pour la sécurité
- Définition d'une stratégie de sécurité bien pensée, adossée à des frameworks et modèles opérationnels
- Développement de programmes et projets de sécurité pour la maturation des capacités et processus

### **Pour aller plus loin**

Pour lire le rapport Verizon PSR 2020 dans son intégralité, rendez-vous sur [verizon.com/paymentsecurityreport](https://verizon.com/paymentsecurityreport). Pour découvrir comment renforcer la sécurité de vos paiements et votre gestion de la conformité, contactez votre chargé de compte Verizon Business ou écrivez-nous à [paymentsecurity@verizon.com](mailto:paymentsecurity@verizon.com)

---

### **La solution Verizon**

Selon le classement établi par le PCI SSC (Payment Card Industry Security Standards Council), nous sommes l'un des plus grands groupes d'auditeurs de sécurité qualifiés (Qualified Security Assessors, ou QSA) au monde. À ce titre, nous aidons les entreprises à rester conformes au standard PCI et à réduire leur exposition aux risques grâce à une approche cohérente et facilitatrice de la sécurisation des données de carte de paiement.

Nos atouts :

- Services PCI déployés dans 61 pays
- Plus de 180 spécialistes de la sécurité dans 30 pays
- Plus de 18 000 évaluations réalisées depuis 2009
- Services de conseil en sécurité depuis 1999 et services de conformité PCI depuis 2003

