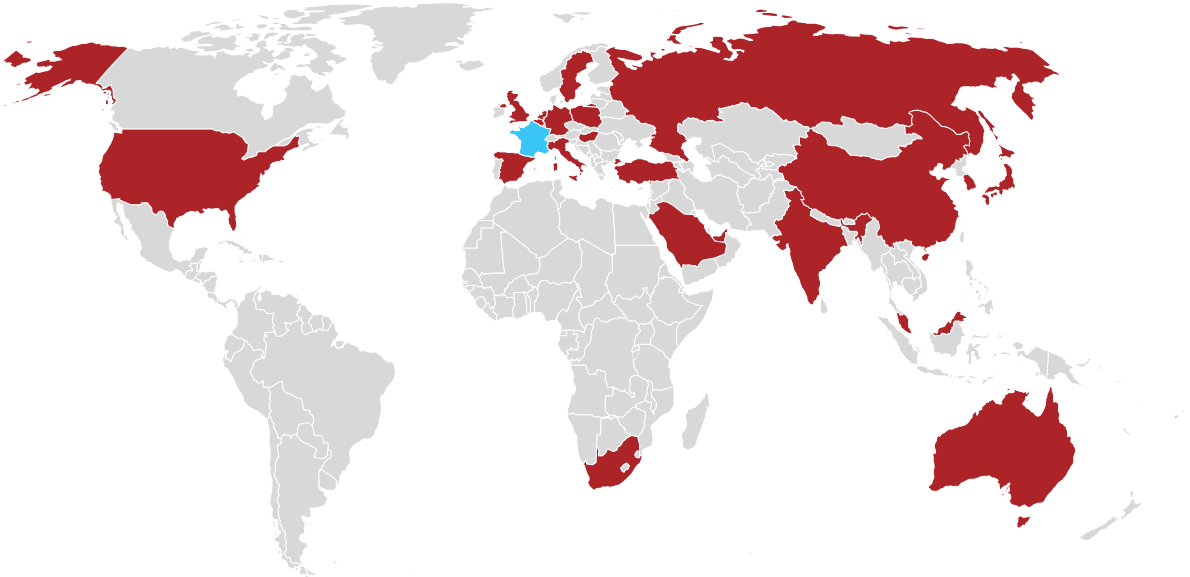
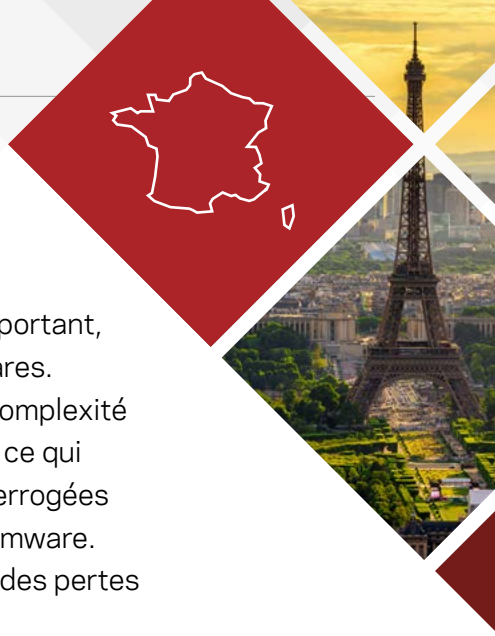
Étude Veritas sur la résilience contre les ransomwares en France

Synthèse générale

La transformation numérique, et en particulier l'adoption du cloud, s'est accélérée avec la pandémie mondiale. Pour soutenir la généralisation du télétravail, les entreprises créent plus de données et sont confrontées à la nécessité de transférer leurs applications depuis leurs propres datacenters vers le cloud. Une nouvelle étude mondiale, menée par Wakefield Research pour Veritas Technologies, a été réalisée auprès de plus de 2 700 leaders et professionnels du secteur informatique dans 21 pays. Elle conclut que ce changement s'accélère mais que les stratégies de reprise n'évoluent pas en conséquence, ce qui crée un décalage important. Cela est dû à plusieurs facteurs, mais la raison principale réside dans le fait que pour les entreprises, le cloud est une plate-forme facile à adopter pour l'exécution d'applications et le stockage d'informations, mais qu'il s'avère bien plus difficile de mettre en place une plate-forme complètement résiliente. Il existe un besoin urgent pour les entreprises de combler ce manque en accélérant la mise en œuvre d'une stratégie de résilience correspondant aux besoins actuels et à la complexité informatique croissante.



VERITAS



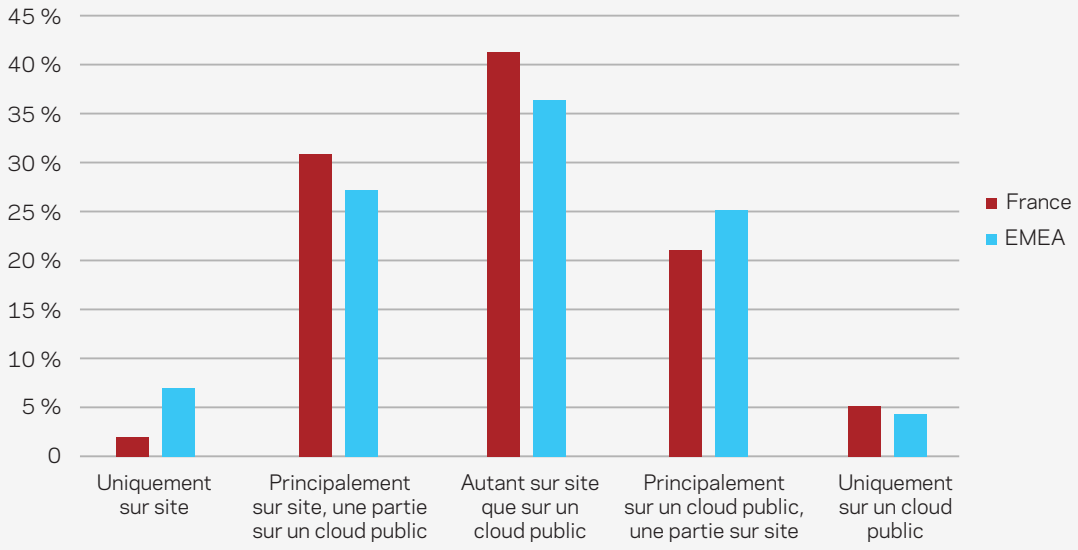
Aperçu de la situation en France

Beaucoup d'entreprises françaises souffrent d'un manque de résilience important, ce qui rend leurs données critiques vulnérables aux menaces de ransomwares. Alors qu'elles ont adopté plus de plates-formes cloud et donc renforcé la complexité informatique, elles n'ont pas su faire évoluer leurs stratégies de résilience, ce qui expose leurs données à de nombreux risques. Presque trois personnes interrogées sur dix rapportent que leur entreprise a été victime d'une attaque de ransomware. Trop d'entreprises s'exposent à de longues perturbations de l'activité ou à des pertes de données en cas d'attaque de ransomware.

Complexité informatique

- En France, les entreprises adoptent le cloud plus rapidement que la moyenne mondiale. En moyenne, une entreprise française utilise environ 13 services cloud (IaaS, PaaS, et SaaS), et un quart des entreprises en utilise plus de 20.
  - En comparaison, une entreprise moyenne en EMEA utilise environ 13 services cloud. En Asie-pacifique, environ 10.

Où votre entreprise stocke-t-elle la plupart de ses données et de ses applications ?



- Cette utilisation massive du cloud crée une plus grande complexité informatique. 69 % des personnes interrogées en France indiquent que les mesures de sécurité de leur entreprise ne sont pas adaptées à leur complexité informatique.

- Les préoccupations principales des responsables informatiques français en matière de complexité informatique couvrent tous les domaines et sont similaires à celles de leurs homologues en EMEA :

Préoccupations principales des dirigeants informatiques français en matière de complexité informatique :

35 % Coût de la maintenance plus élevé

33 % Risque accru d'attaques externes, comme des violations de données et des attaques de ransomwares

31 % Risque de perte de données

Préoccupations principales des dirigeants informatiques de la zone EMEA en matière de complexité informatique :

31 % Coût de la maintenance plus élevé

37 % Risque accru d'attaques externes, comme des violations de données et des attaques de ransomwares

35 % Risque de perte de données

- Les entreprises françaises prennent des mesures pour combler leur manque de résilience : 55 % des personnes interrogées indiquent que leur entreprise a augmenté son budget de sécurité informatique depuis le début de la pandémie de COVID-19.

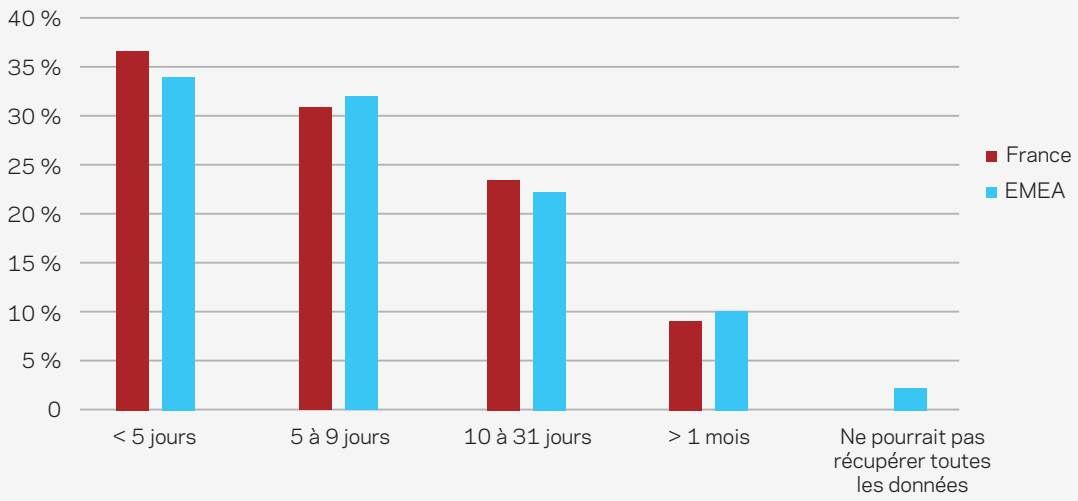
L'impact des ransomwares

- Les ransomwares constituent une menace grandissante. 29 % des personnes interrogées en France affirment qu'elles ont subi au moins une attaque de ransomware, contre 38 % en EMEA.
- Trop d'entreprises en France paient le prix de leur manque de résilience. Comme leurs systèmes de sauvegarde et de récupération ne sont pas assez robustes, lorsque les entreprises françaises sont attaquées par un ransomware, elles n'ont souvent pas d'autre choix que de payer la rançon. Parmi les entreprises victimes d'attaques de ransomware, 60 % des personnes interrogées rapportent que leur entreprise a payé l'intégralité ou une partie de la rançon, contre 49 % en EMEA.

Le manque de résilience

- En France, les entreprises seraient légèrement plus résilientes que celles situées dans d'autres pays. 63 % des personnes interrogées en France, contre 65 % en EMEA, pensent qu'il leur faudrait au moins 5 jours pour récupérer toutes leurs données en cas d'attaque de ransomware.

Combien de temps la récupération prendrait-elle après une attaque de ransomware (si vous ne payez pas la rançon) ?



- Seulement 15 % des personnes interrogées en France affirment que leur entreprise suit les pratiques d'excellence recommandées, qui consistent à posséder trois copies de leurs données, dont une hors site et une hors ligne. 39 % indiquent que leur entreprise possède au moins trois copies de leurs données sur site.
- En France, les entreprises testent leurs plans de reprise après incident plus souvent que dans les autres pays du monde : 66 % les ont testés au cours des trois derniers mois, contre 60 % à l'échelle mondiale.

Recommandations pour la France : des menaces pèsent sur les entreprises françaises. Le fait que six entreprises françaises victimes d'une attaque de ransomware sur dix ont payé la rançon indique que ces entreprises ont besoin de se concentrer davantage sur leur stratégie de résilience. Les entreprises françaises doivent combler leur manque de résilience aussitôt que possible afin de pouvoir récupérer leurs données sans avoir à payer une rançon. Elles doivent envisager l'adoption de méthodes plus robustes pour réduire l'impact des attaques de ransomwares. En voici quelques exemples :

- **Révision de leurs stratégies de bout en bout :** les entreprises françaises doivent revoir leurs stratégies de résilience pour s'assurer qu'elles s'appuient sur la visibilité en temps réel, la surveillance et l'automatisation de la récupération.
- **Sauvegardes plus robustes :** les entreprises doivent adopter une approche de sauvegarde « 3-2-1 » : elle doivent disposer d'un minimum de trois copies de leurs données dans deux emplacements distincts, avec au moins une copie hors site.
- **Tests de reprise après incident plus fréquents :** idéalement, les entreprises devraient tester leur plan de reprise après incident une fois par mois. Les environnements de données et d'applications évoluent très rapidement. Des tests moins fréquents augmentent donc le risque que leur plan de reprise après incident ne fonctionne pas lorsqu'elles en auront besoin.
- **Mises à jour de sécurité fréquentes :** les équipes informatiques doivent rester à jour dans l'implémentation des correctifs de sécurité et des nouvelles versions comportant des mises à jour de sécurité.
- **Chiffrement des données :** les entreprises doivent mettre en place un chiffrement des données en transit pour protéger les données et éviter qu'elles ne soient compromises sur le réseau.
- **Stockage immuable :** les équipes informatiques doivent utiliser des technologies de stockage immuables et ineffaçables pour éviter que les ransomwares chiffrent ou suppriment les sauvegardes.
- **Gestion de l'accès :** les entreprises doivent implémenter un contrôle d'accès basé sur les rôles et limiter l'accès uniquement aux fonctionnalités nécessaires pour les utilisateurs.