# Veeam Data Center Availability Report 2014

## Le défi de « l'Always-On Business »

VEEAM
IT JUST WORKS!™

AVAILABILITY™
for the Modern Data Center

# Contenu

# Résumé

Le Veeam Data Center Availability Report 2014 examine les exigences croissantes auxquelles les entreprises font face pour assurer la « continuité de l'activité », les actions qu'elles mènent pour répondre à ces exigences et le degré de réussite de ces actions. Faisant suite aux précédents rapports de Veeam sur la protection des données, ce rapport examine la capacité des solutions existantes à fournir la disponibilité en continu que les entreprises exigent au 21e siècle.

En particulier, ce rapport prouve qu'il existe des besoins clairs d'accès 24/7 aux services et aux applications informatiques, avec plus de 90 % d'entreprises rehaussant leurs exigences pour réduire au minimum les temps d'arrêt et garantir l'accès aux données. Il montre également comment les entreprises modernisent l'infrastructure de leur data center afin de répondre à ces exigences.

Malgré les investissements dans le data center moderne, il existe un « écart de disponibilité » entre les exigences de la continuité d'activité et ce que les solutions de sauvegarde traditionnelles peuvent offrir en termes d'objectifs de temps de restauration (RTO) et de délais optimaux de reprise d'activité (RPO). En effet, pour répondre aux exigences de la continuité d'activité, les entreprises devraient récupérer leurs données stratégiques en 60 % du temps qu'il leur faut actuellement et effectuer leurs sauvegardes 1,5 fois plus souvent.

Ce rapport montre l'étendue de cet écart et son incidence financière pour l'entreprise. Actuellement, les entreprises souffrent de temps d'arrêt sur les applications 13 fois par an, avec un coût total relatif à ces temps d'arrêt et aux pertes de données s'élevant jusqu'à 10 163 114 $. En outre, les entreprises connaissent deux échecs de restauration par an. À cause de cela, elles perdent au moins 2 millions de dollars par année, ce qui s'explique par la perte de données et d'autres facteurs tels que les chutes de productivité et les opportunités manquées.

La conclusion de ce rapport donne le détail des raisons pour lesquelles les solutions de sauvegarde traditionnelles ne satisfont toujours pas aux exigences en matière de RTO et de RPO. Les répondants soulignent que ces solutions manquent de fonctionnalités telles que la restauration ultra-rapide (souhaitée par 60 % des entreprises), la prévention contre les pertes de données (53 %), la protection vérifiée (47 %), l'utilisation des données de sauvegarde en tant qu'environnement de test similaire à l'environnement de production pour les nouveaux correctifs et les mises à jour (38 %), et la visibilité complète avec supervision et alertes proactives en ce qui concerne les problèmes avant toute incidence opérationnelle (36 %).

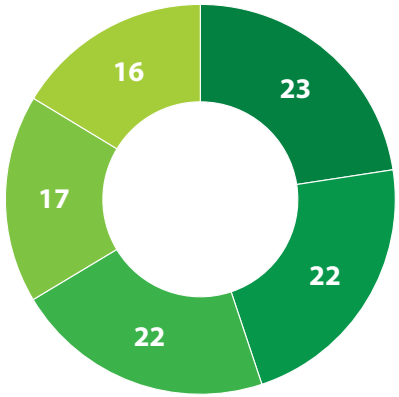
Il indique ensuite quelles actions les entreprises mettent en œuvre pour assurer la disponibilité de leurs data centers modernes. Eu égard au manque de capacités mentionné ci-dessus, il n'est pas surprenant que 78 % des entreprises projettent de changer de solution de sauvegarde dans les 2 prochaines années.

Le présent rapport se fonde sur une enquête en ligne menée en août et septembre 2014 par Vanson Bourne, société d'études de marché indépendante, auprès de 760 décideurs informatiques issus d'entreprises des États-Unis, du Royaume-Uni, d'Allemagne, de France, d'Italie, des Pays-Bas, de Suisse, du Brésil, d'Australie et de Singapour employant plus de 1 000 personnes.

# Contexte de l'étude

Les personnes interrogées ont été choisies sur une palette diversifiée de secteurs d'activité, à savoir : vente au détail, distribution et transport (23 % des répondants), fabrication (22 %), services financiers (22 %), services aux entreprises (17 %) et autres secteurs commerciaux (16 %). En conséquence, les résultats de l'étude ont été distribués de manière homogène sur diverses entreprises et divers secteurs, réduisant ainsi les risques de voir un secteur particulier biaiser les statistiques (Figure 1).

**Figure 1 : Industries des personnes interrogées (%)**



# Partie 1 :
# Le data center moderne

# Partie 1 : Le data center moderne

Les exigences des entreprises ont changé de manière considérable en relativement peu de temps. L'informatique est devenue stratégique pour chaque entreprise, et les exigences professionnelles qui y sont relatives ont changé de manière significative. Aujourd'hui, pour rester concurrentielles, les entreprises doivent produire des services informatiques plus rapidement, renforcer la sécurité et le contrôle, diminuer les coûts d'exploitation et augmenter leur flexibilité. Pour répondre à ces exigences, les entreprises mettent en place des data centers modernes en investissant dans des technologies modernes telles que la virtualisation, le stockage moderne et le cloud. Actuellement, 81 % des entreprises modernisent ou ont déjà modernisé leurs data centers, avec 16 % de plus prévoyant de le faire au cours des 2 prochaines années (fig. 2).

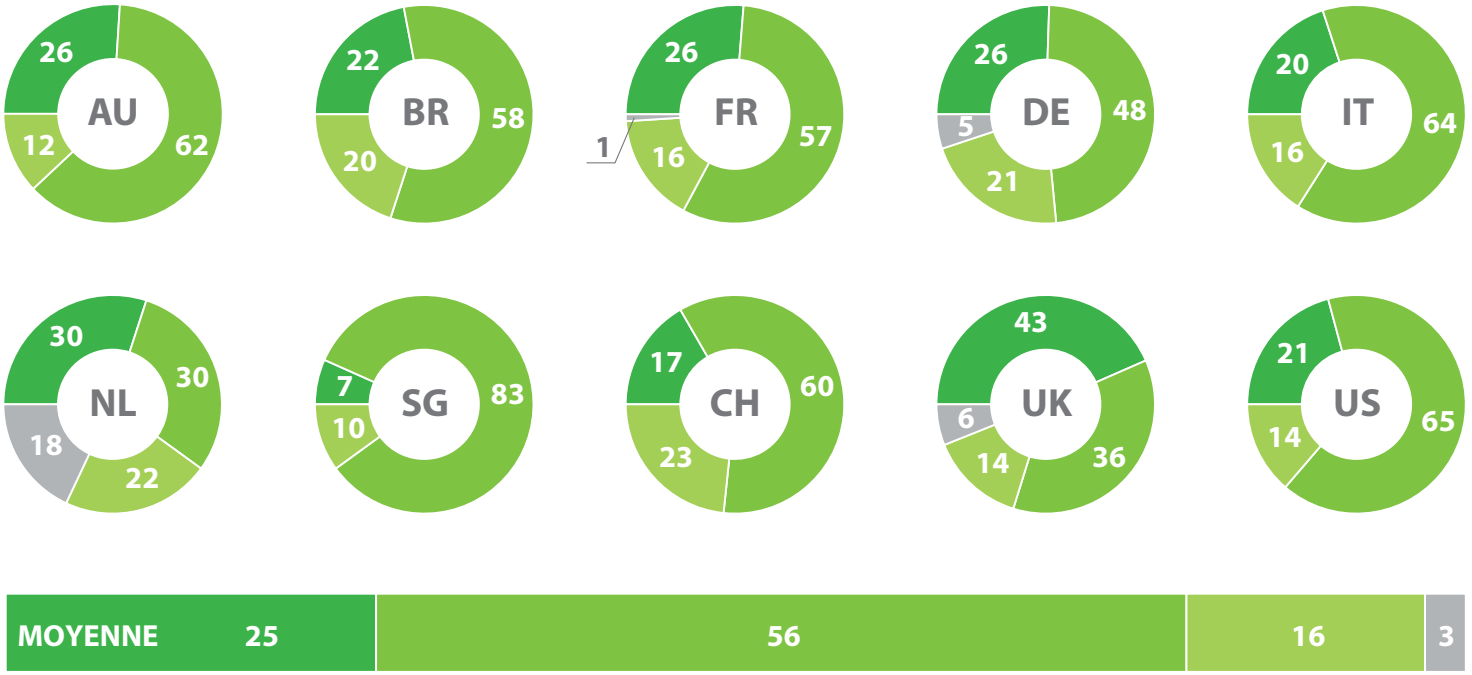



**Figure 2 : Entreprises ayant modernisé, modernisant ou prévoyant de moderniser leurs data centers (%)**

- Le centre de données a déjà été modernisé
- Le centre de données est en train d'être modernisé
- Modernisation prévue dans les 2 ans
- Aucune modernisation du centre de données prévue

68 % de ces entreprises modernisant leurs data centers le font pour permettre une continuité 24/7 de leur activité (fig. 3). Il semble exister un consensus sur la technologie requise pour moderniser entièrement un data center. 97 % des entreprises engagées dans la modernisation du data center investissent ou prévoient d'investir dans la virtualisation de leurs serveurs. Les autres technologies visées sont les mises à niveau du stockage (95 %), les mises à niveau du système d'exploitation (94 %), ainsi que la protection des données et la récupération après incident (93 %, fig. 4).

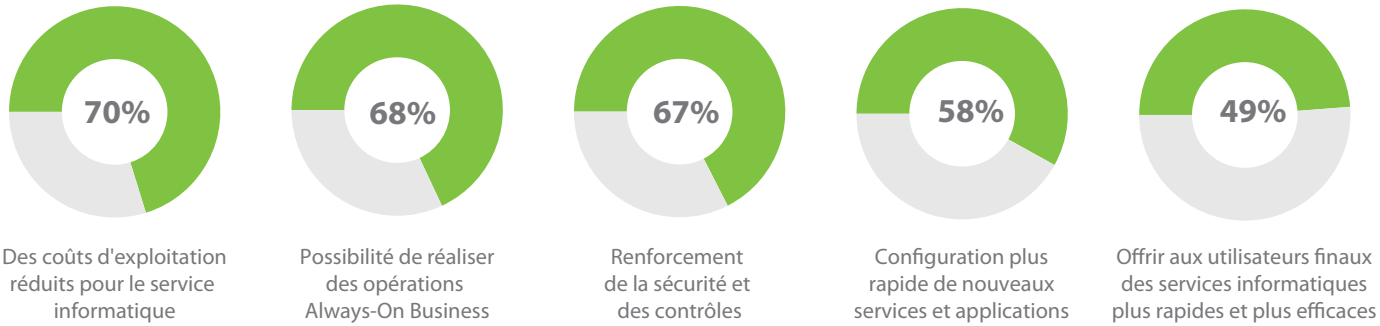



**Figure 3 : Forces motrices de la modernisation du datacenter (%)**

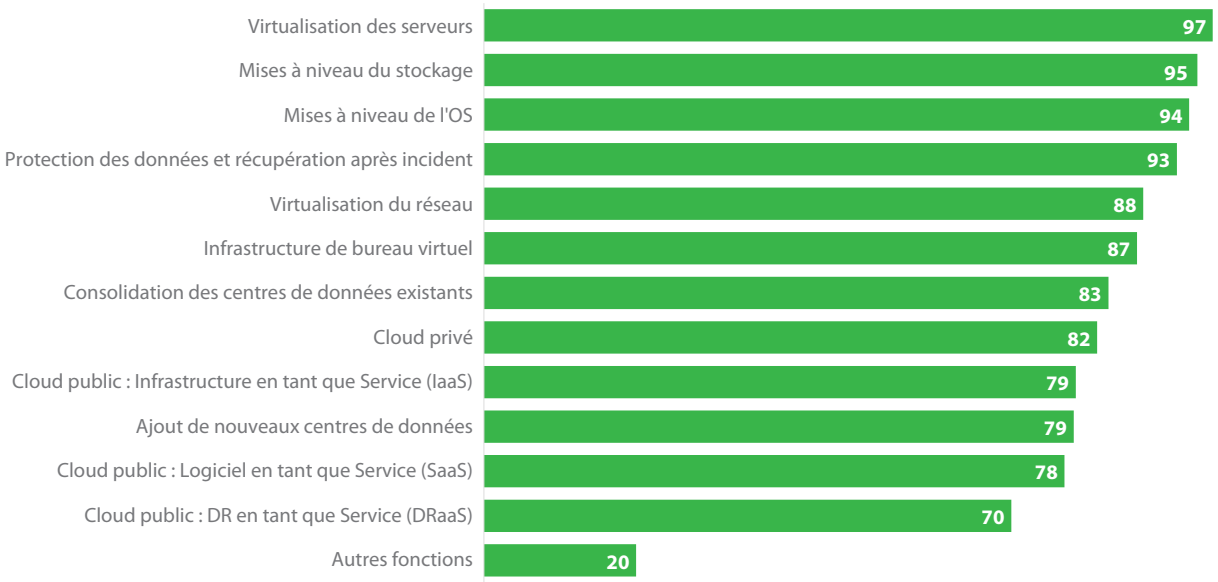
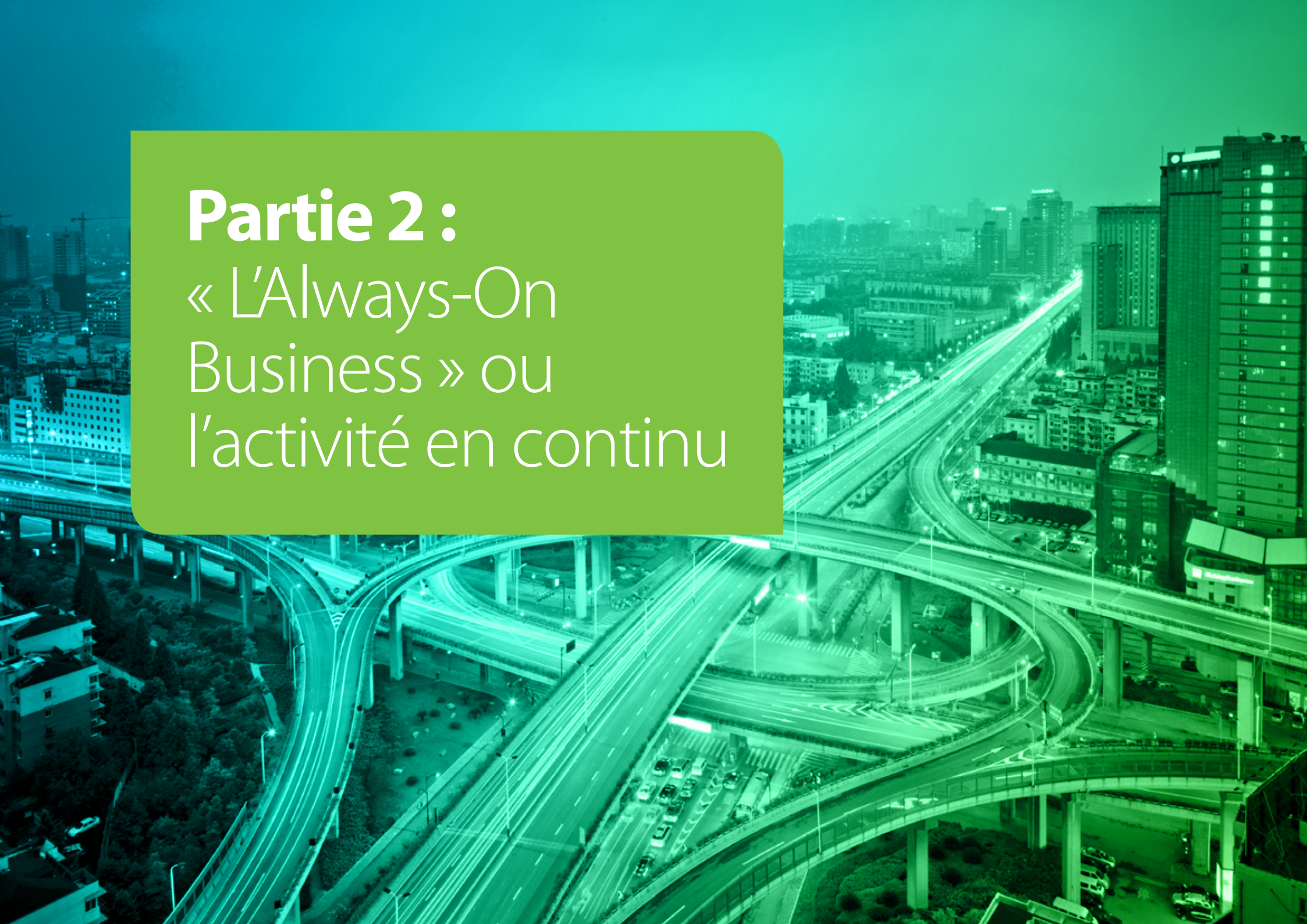



**Figure 4 : Technologies dans lesquelles les entreprises investissent ou prévoient d'investir (%)**



# **Partie 2 :**
# « L'Always-On Business » ou l'activité en continu

# Partie 2 : « L'Always-On Business » ou l'activité en continu

Au cours des 10 dernières années, les entreprises ont vu les utilisateurs finaux exiger un accès croissant aux données et aux applications pour de nombreuses raisons, dont :

- horaires de plus en plus flexibles ;
- mondialisation permettant aux entreprises d'établir des filiales sur de nombreux fuseaux horaires ;
- clients consommant en ligne à tout moment ;
- intégration et automatisation de la chaîne logistique exigeant l'accès constant aux systèmes opérationnels et aux données ;
- avènement de l'Internet des objets signifiant que les périphériques sont connectés et contrôlés de manière permanente.

Considérées en groupe, ces exigences signifient que les entreprises doivent fonctionner « en continu ». Plus de données et d'applications sont maintenant considérées comme stratégiques et les entreprises ont moins de patience pour les temps d'arrêt, ce qui entraîne un besoin accru de disponibilité des data centers modernes.

Plus de 90 % des entreprises étudiées se trouvaient en phase de hausse de leurs exigences de disponibilité afin de répondre aux besoins de continuité de leur activité. Plus spécifiquement, 93 % des répondants haussent leurs exigences pour minimiser les temps d'arrêt, alors que 92 % le font pour garantir l'accès aux données (fig. 5)

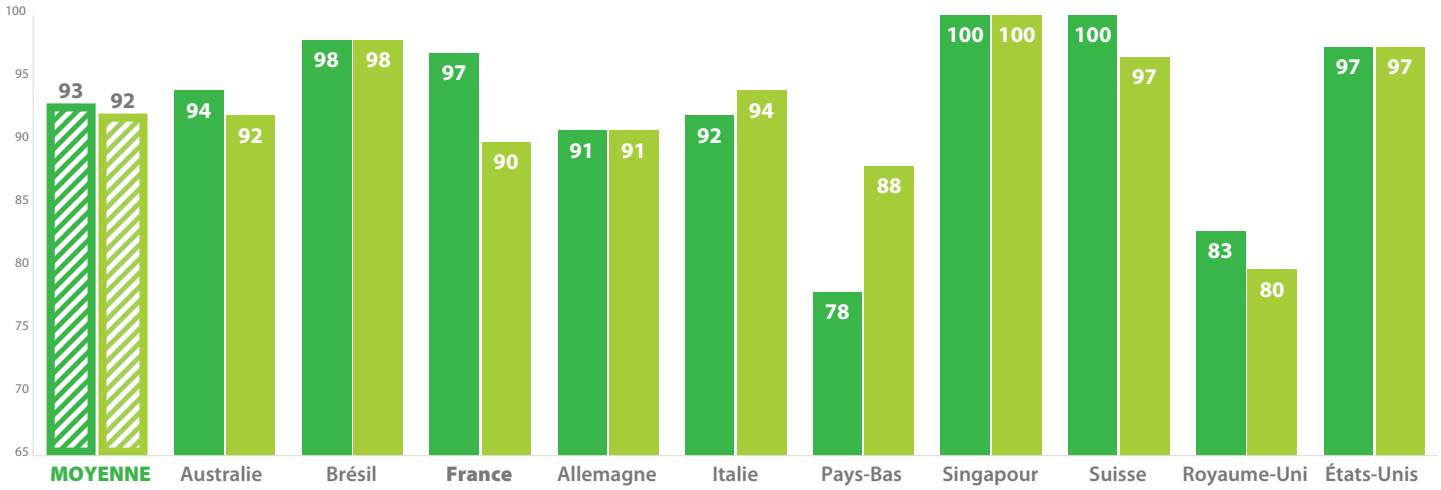



**Figure 5 : Entreprises renforçant leurs exigences de protection des données au cours des 2 dernières années (%)**

- Pourcentage des organisations qui ont augmenté leurs exigences pour minimiser les temps d'indisponibilité d'application
- Pourcentage des organisations qui ont augmenté leurs exigences pour garantir l'accès aux données

Ce processus est alimenté par les exigences des utilisateurs, la plus commune étant des interactions plus fréquentes et en temps réel entre clients, partenaires, fournisseurs et employés (65 %). Le besoin d'accéder aux applications sur plusieurs fuseaux horaires (56 %), l'adoption progressive des périphériques mobiles (56 %), la plus grande flexibilité des horaires (54 %) et un niveau croissant d'automatisation en ce qui concerne la prise de décision et les transactions (53 %) ont été également indiqués en tant qu'exigences importantes (fig. 6).

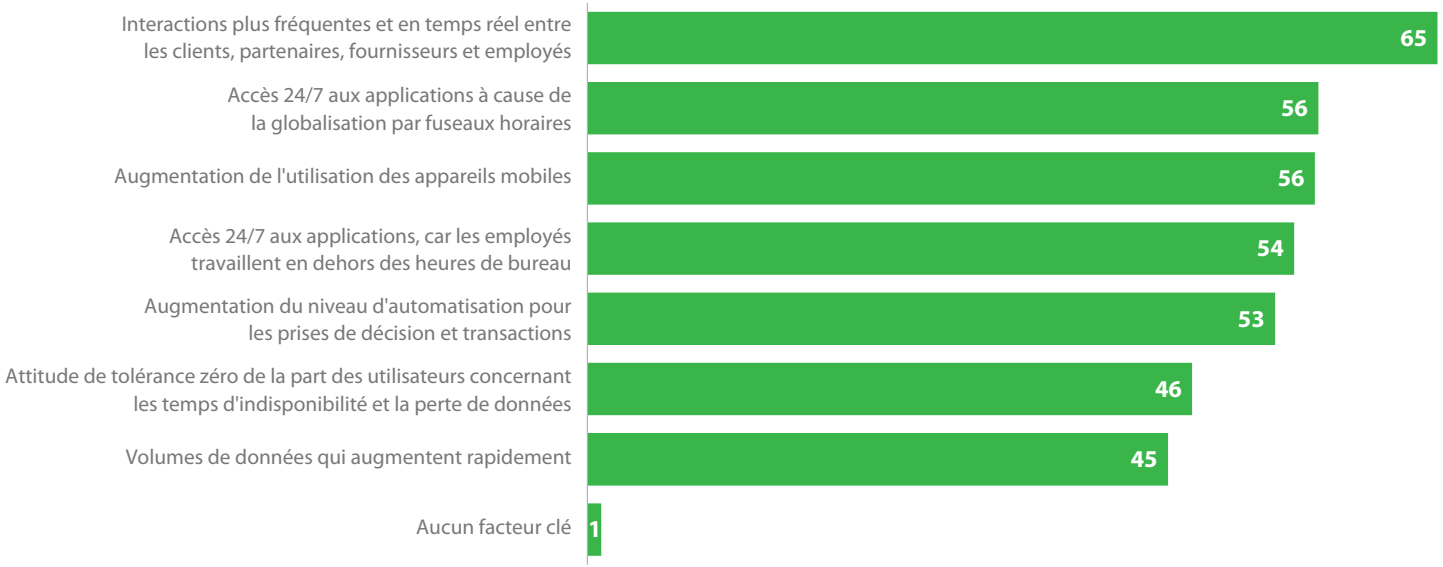



**Figure 6 : Facteurs de minimisation des temps d'arrêt et de garantie d'accès aux données (%)**

# Partie 3 :
# L'écart de disponibilité

# Partie 3 : L'écart de disponibilité

La modernisation du data center n'a pas comme conséquence automatique une plus grande disponibilité de toutes les données et applications. En fait, malgré les investissements dans la virtualisation, les stockages évolués et le cloud, beaucoup d'entreprises restent incapables de satisfaire les RPOs et RTOs de leurs contrats de niveau de service (SLA). Ceci creuse un « écart de disponibilité » entre les exigences de disponibilité de la continuité de l'activité et ce que les solutions de sauvegarde des sociétés peuvent réellement permettre.

Pour mieux mesurer leur disponibilité, les entreprises regardent leurs RPOs et RTOs pour les applications critiques et non critiques. Les entreprises doivent avoir l'assurance que leurs applications les plus stratégiques resteront disponibles 24/7. Actuellement, 46 % de charges de travail sont stratégiques, et l'on s'attend à voir ce chiffre atteindre 53 % d'ici 2016 (fig. 7).

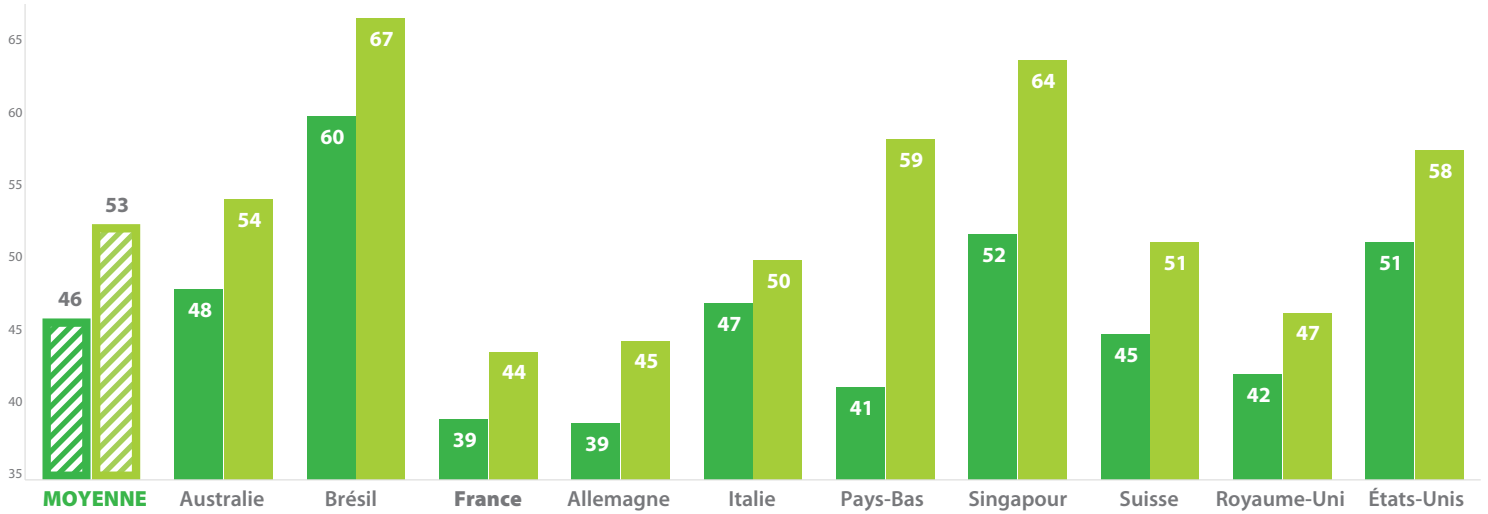



**Figure 7 : Proportion de charges stratégiques (%)**

Pourcentage stratégique actuel de la charge de travail

Pourcentage stratégique prévu de la charge de travail dans deux ans

Le premier niveau de service critique en matière de continuité de l'activité est le RTO, à savoir la vitesse à laquelle les applications peuvent être restaurées. Une restauration plus rapide des applications signifie des temps d'arrêt et une incidence sur l'activité moindres en termes de ventes et de productivité perdues. Actuellement, la restauration des applications stratégiques nécessite une moyenne de 2,86 heures, contre un RTO de 2,69 heures (fig. 8), alors que la restauration des applications non stratégiques demande 8,45 heures en moyenne contre un RTO de 10,02 heures (fig. 9). Comme nous pouvons le voir, l'entreprise moyenne respecte (ou presque) ses niveaux de service en matière de restauration des données.

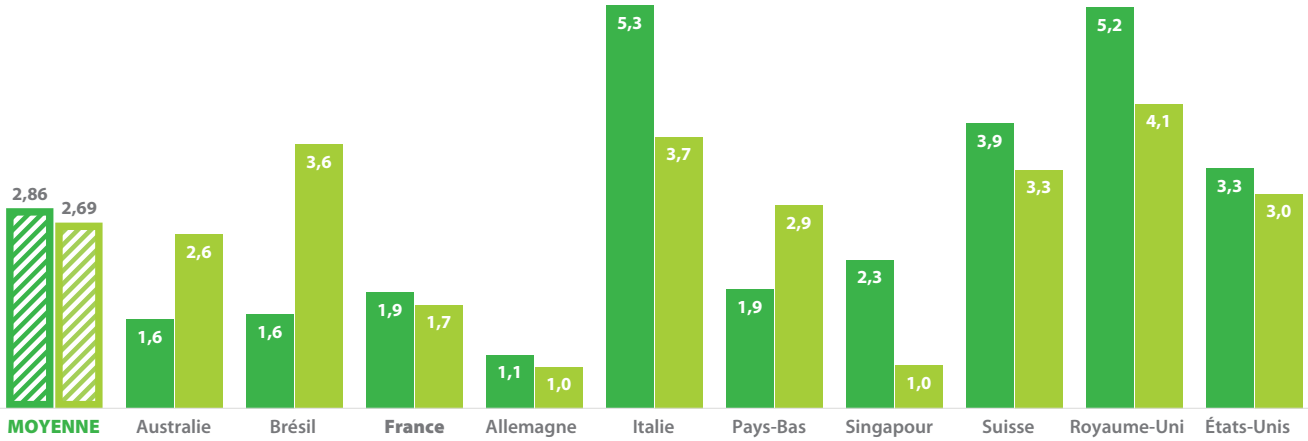



**Figure 8 : Temps de restauration moyen et RTO – applications critiques (en heures)**

Temps de restauration moyen

Actuelle RTO

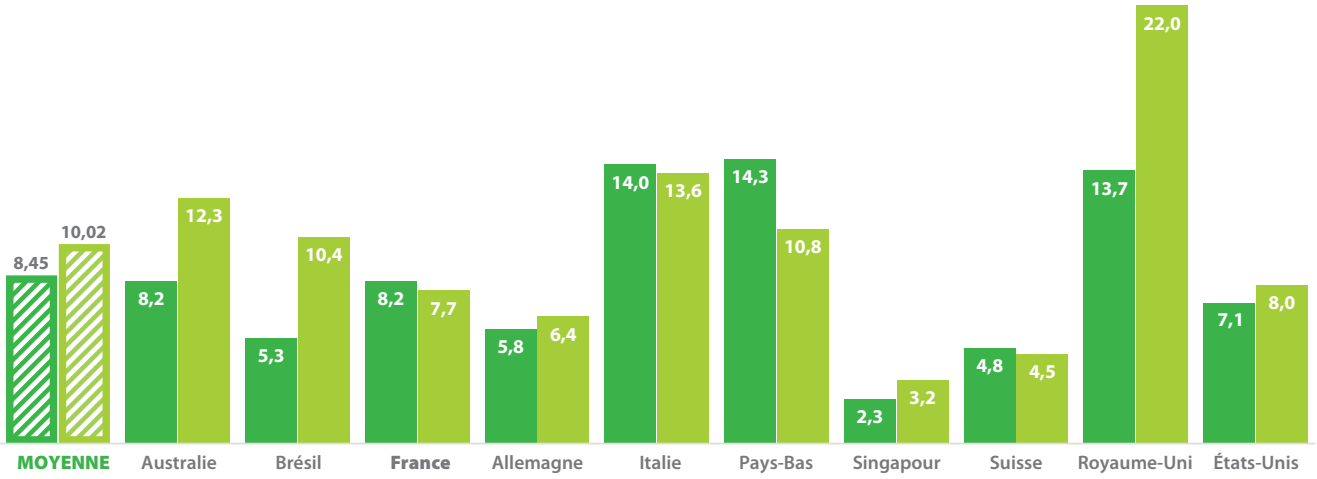



**Figure 9 : Temps de restauration moyen et RTO – applications non critiques (en heures)**

Temps de restauration moyen

Actuelle RTO

Le deuxième niveau de service critique est le RPO, c.-à-d. les données les plus récentes récupérables et la quantité de données irrécupérables en cas de panne informatique. Plus une entreprise sauvegarde ses données souvent, plus son RPO est réduit, ainsi que son exposition aux pertes de données. Actuellement, les entreprises parviennent moins bien à respecter leurs RPOs, ce qui leur fait courir un risque de pertes de données excessives.

Les applications stratégiques sont sauvegardées toutes les 4,81 heures contre un RPO de 3,53 heures (fig. 10). Les applications non stratégiques sont sauvegardées toutes les 14,46 heures contre un RPO de 11,53 heures (fig.11). En comparant les chiffres des RPOs et RTOs, il est clair que les entreprises peuvent restaurer leurs applications dans les temps convenus, mais courent le risque de pertes de données excessives.

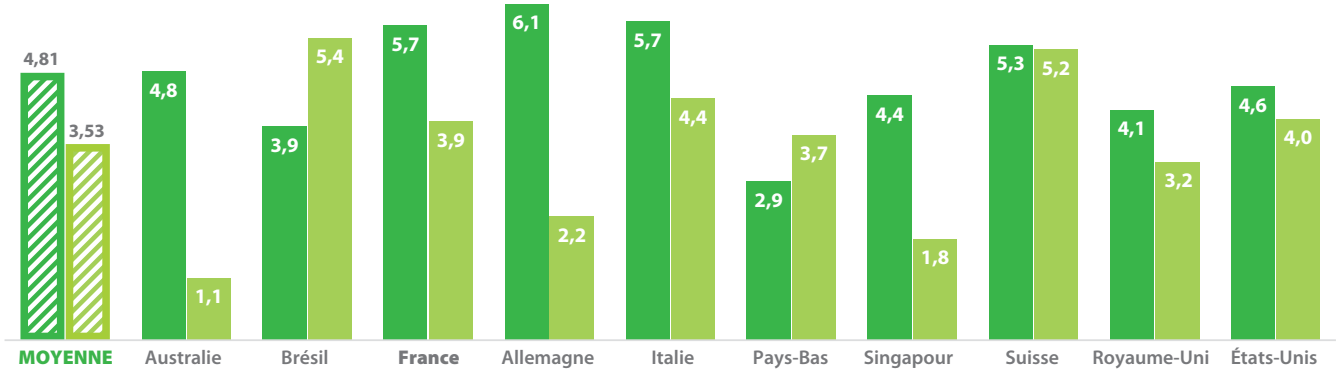



**Figure 10 : Fréquence de sauvegarde moyenne et RPO – applications stratégiques (en heures)**

Fréquence de sauvegarde moyenne

Actuelle RPO

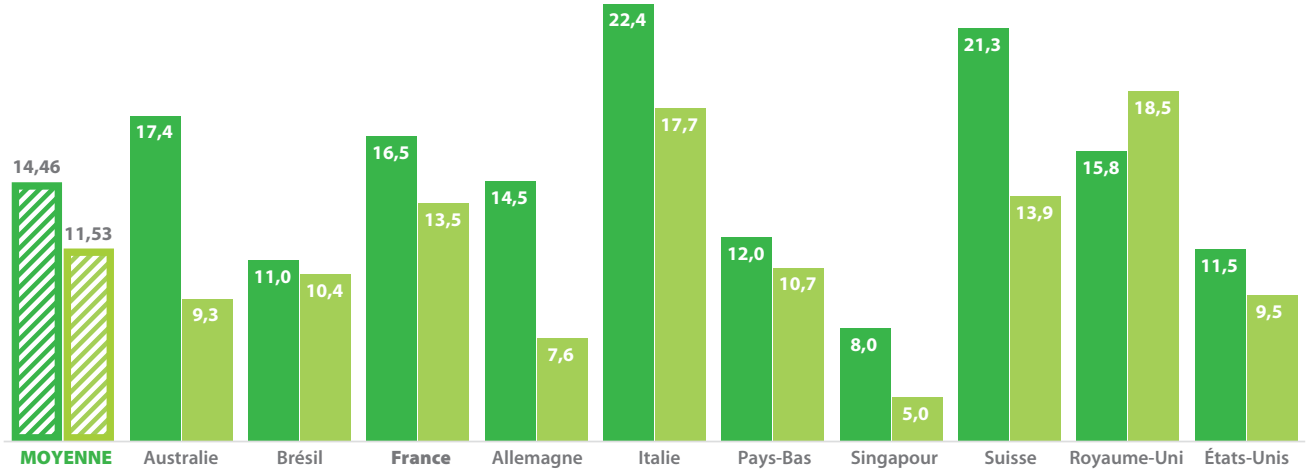
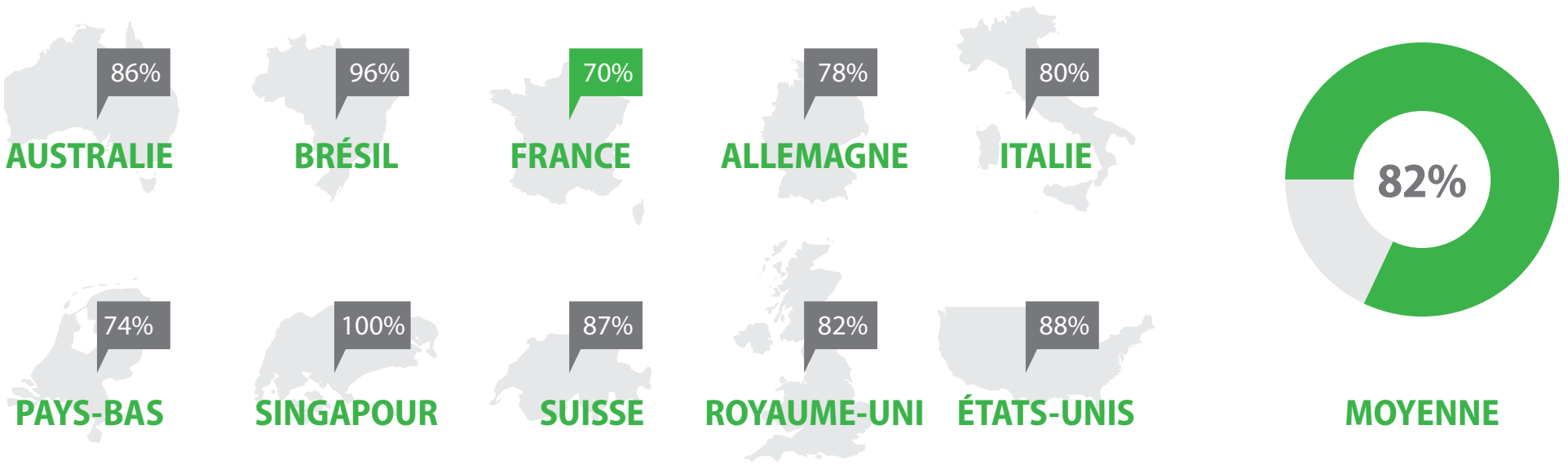



**Figure 11 : Fréquence de sauvegarde moyenne et RPO – applications non stratégiques (en heures)**

Fréquence de sauvegarde moyenne

Actuelle RPO

Figure 12 : Pourcentage d'entreprises identifiant un « écart de disponibilité » (%)




Pourtant, même ces performances ne suffisent pas à satisfaire les exigences de disponibilité d'une entreprise. 82 % de répondants disent qu'il existe un « écart de disponibilité » entre le niveau de protection des données qu'ils peuvent offrir maintenant et ce que les utilisateurs exigent afin d'assurer la continuité de l'activité (fig. 12).

Afin d'annuler cet écart, les répondants indiquent que leurs solutions de protection des données devraient offrir un RTO de 1,73 heure et un RPO de 3,19 heures. En conséquence, les entreprises devraient restaurer leurs données stratégiques en 60 % du temps nécessaire actuellement (fig. 13 à la page 14) et effectuer leurs sauvegardes 1,5 fois plus souvent qu'elles ne le font maintenant (fig. 14 à la page 14). Il est cependant très probable que les exigences continuent à tendre vers des RTO et RPO de plus en plus réduits alors que les entreprises essaieront de garantir des services informatiques 24/7. Ceci signifie qu'en dépit de leurs efforts de modernisation de leurs data centers, elles resteront en retrait par rapport aux niveaux de service que la continuité de l'activité exige.

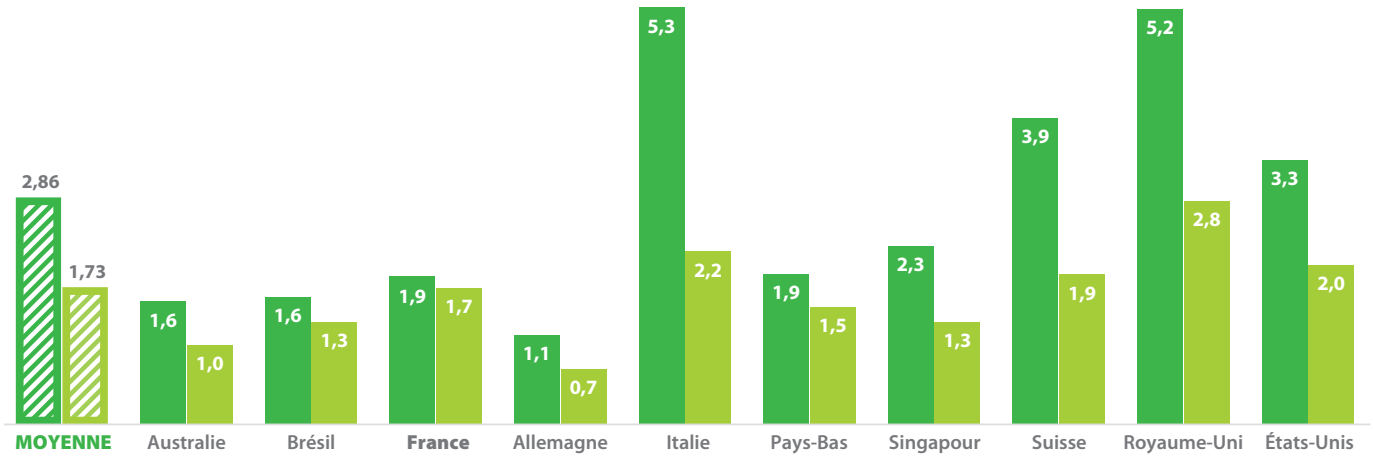



**Figure 13 : Différence entre RTO désiré et temps de restauration (en heures)**

- Temps de restauration moyen
- RTO désiré

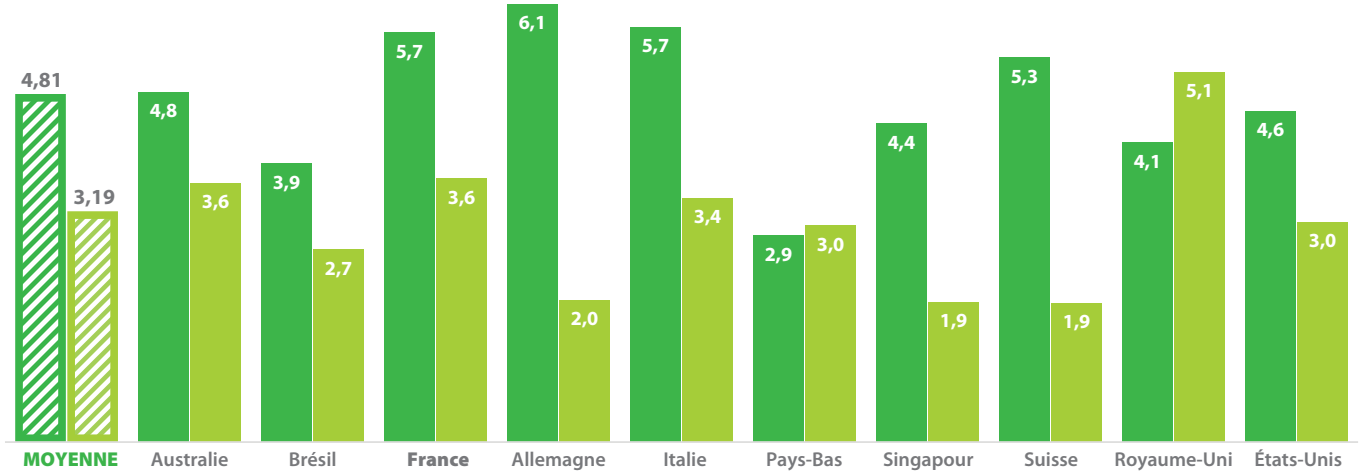



**Figure 14 : Différence entre RPO désiré et fréquence de sauvegarde (en heures)**

- Fréquence de sauvegarde moyenne
- RPO désiré


# **Partie 4 :**
# Coût financier des temps d'arrêt

# Partie 4 : Coût financier des temps d'arrêt

Effet significatif du non-respect des exigences de disponibilité des données et des applications, les entreprises sont exposées à des coûts inutiles. Par exemple, les entreprises peuvent manquer des opportunités commerciales ou doivent restructurer leur exploitation avec des frais lorsque certaines applications critiques tombent en panne.

Sans compter les coûts de productivité perdue pendant chaque temps d'arrêt. Comme il n'existe plus de période « sûre » pour les temps d'arrêt en dehors des heures de travail classiques, ces coûts sont amplifiés. En moyenne, les entreprises font l'expérience de temps d'arrêt non planifiés 13 fois par an (fig. 15).

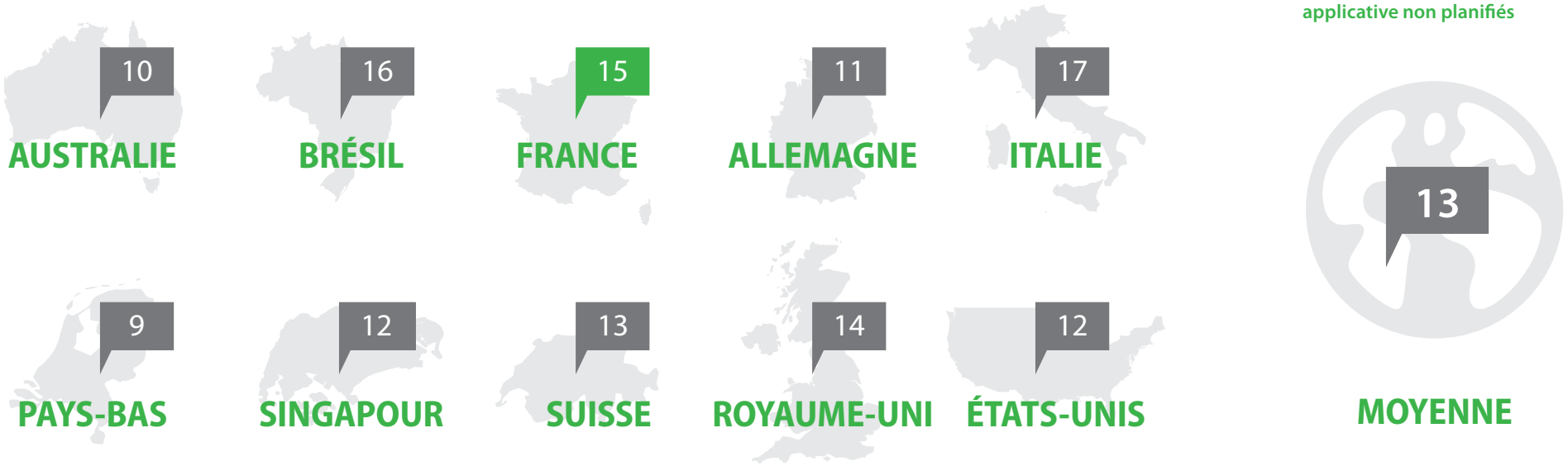



**Figure 15: Nombre d'incidents par an concernant les temps d'indisponibilité applicative non planifiés**

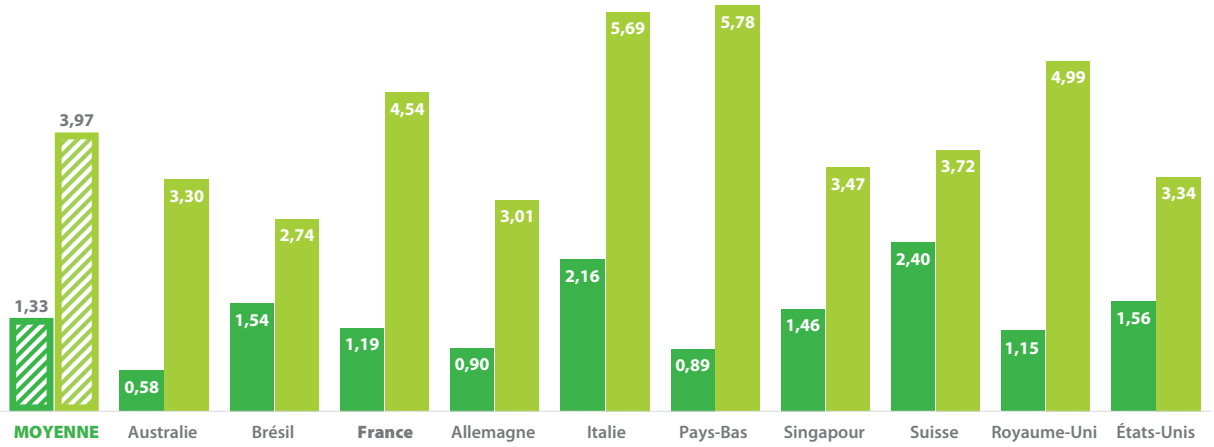



**Figure 16: Longueur des temps d'indisponibilité applicative non planifiés (heures)**

Applications stratégiques

Applications non stratégiques

Ces temps d'arrêt durent 1,33 heure pour les applications stratégiques et 3,97 heures pour les applications non stratégiques (fig. 16). Le coût moyen d'une heure de temps d'arrêt d'une application stratégique s'élève à 82 864 $, et à 43 886 $ pour une application non stratégique (fig. 17). Ceci signifie qu'un arrêt d'application stratégique coûte en moyenne 110 209 $ alors qu'un arrêt d'application non stratégique coûte en moyenne 174 227 $ (fig. 18).

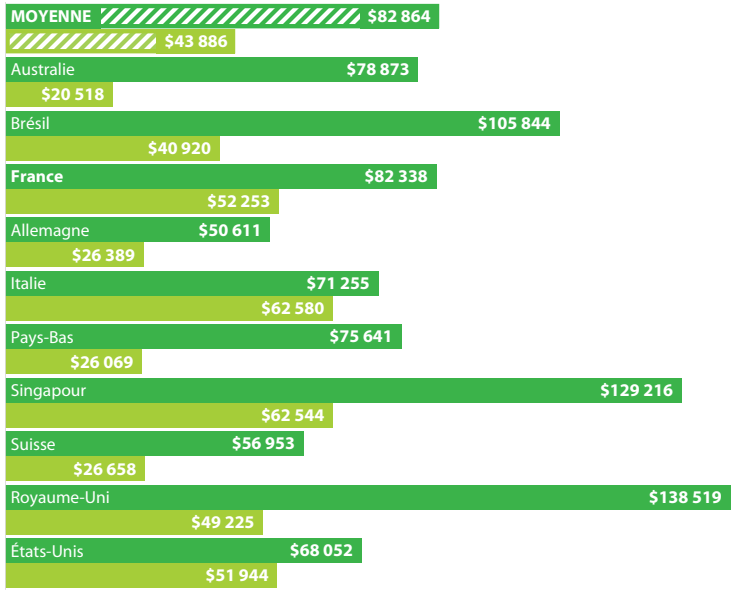



**Figure 17: Coût par heure pour les temps d'indisponibilité applicative (US$)**

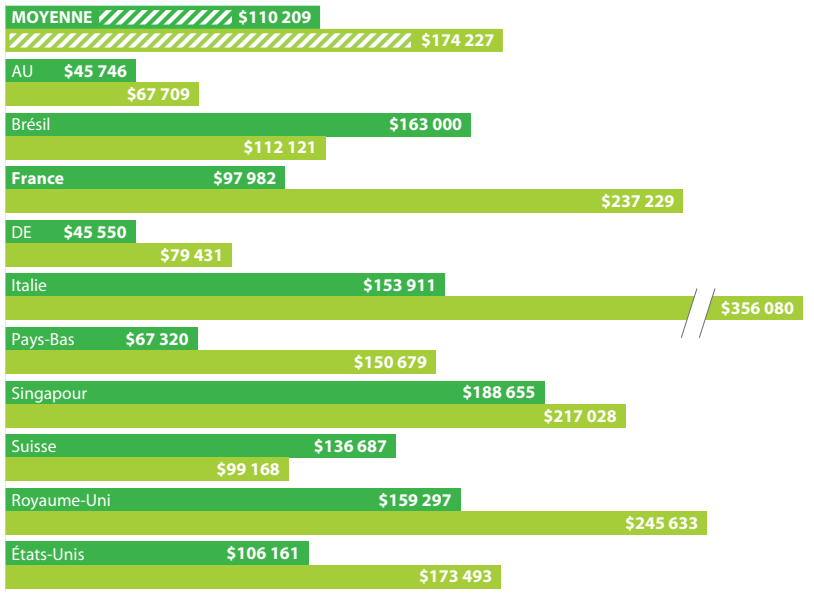



**Figure 18: Coût par incident de temps d'indisponibilité applicative (US$)**

Applications stratégiques

Applications non stratégiques

Parallèlement aux coûts directs des temps d'arrêt, il existe également des coûts liés à la perte de données, c.-à-d. aux données non sauvegardées et qui ne peuvent donc pas être restaurées en cas de temps d'arrêt. Selon l'importance des données elles-mêmes, cela peut représenter un coût énorme pour une entreprise en termes d'opportunités commerciales manquées et de productivité perdue. La perte de données pour les applications stratégiques coûte en moyenne 70 913 $ par heure de données perdues. Pour les applications non stratégiques, la perte de données coûte en moyenne 42 016 $ par heure de données perdues (fig. 19).

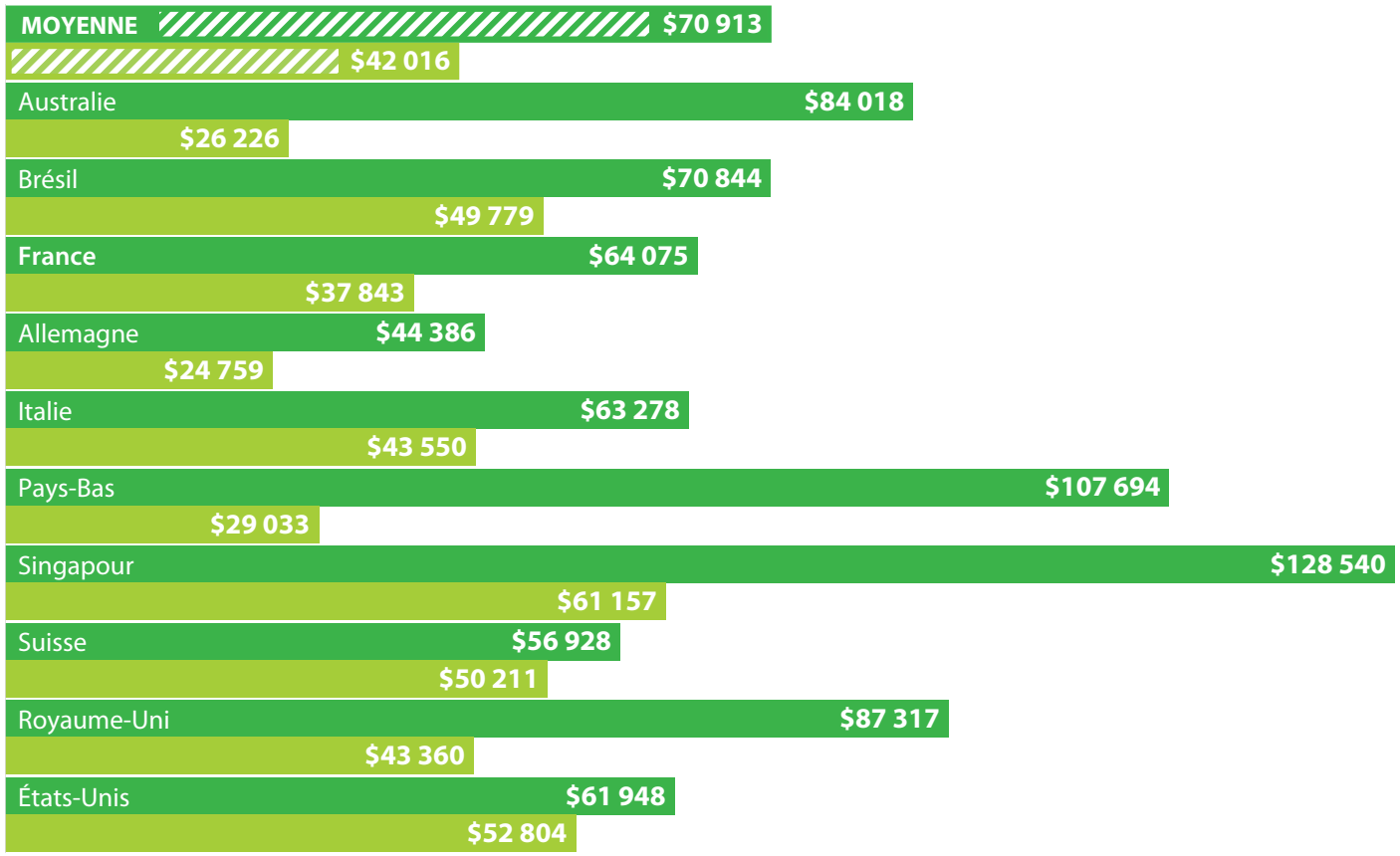



**Figure 19: Coût de perte de données par heure (US$)**

- Applications stratégiques
- Applications non stratégiques

En comparant la fréquence des sauvegardes d'applications, comme le montrent les figures 10 et 11, on voit qu'un unique incident peut coûter aux entreprises jusqu'à 341 092 $ en données perdues pour les applications stratégiques, et jusqu'à 607 551 $ pour les applications non stratégiques (fig. 20).

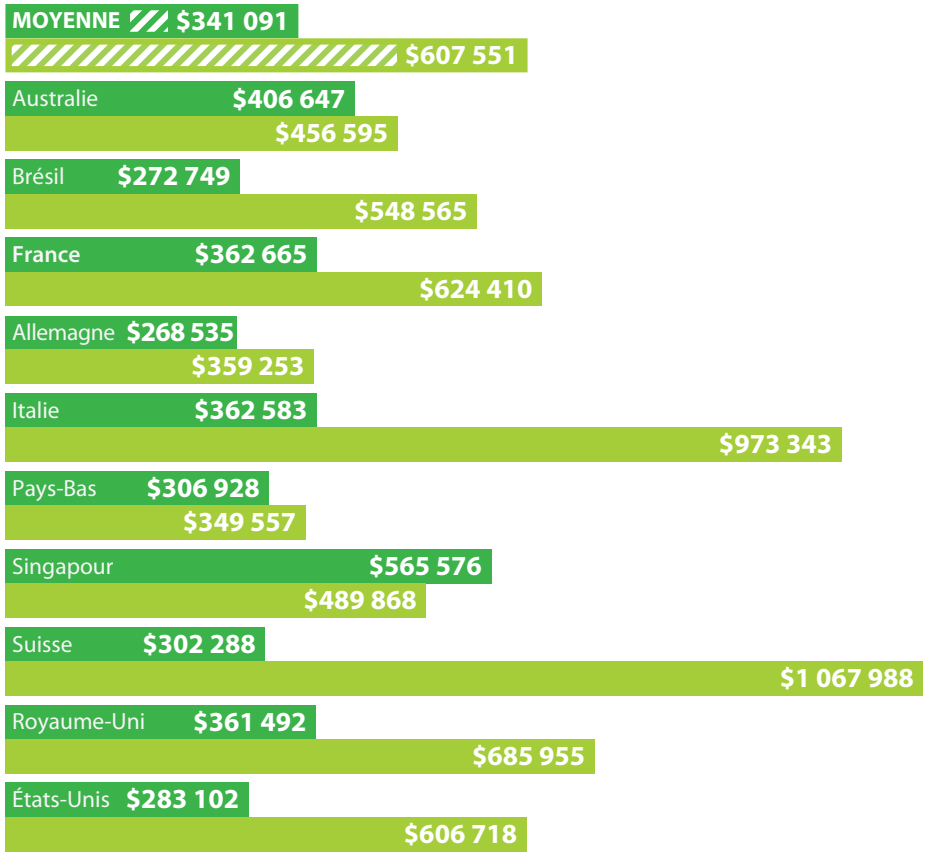



**Figure 20: Coût maximum de perte de données par incident (US$)**

- Applications stratégiques
- Applications non stratégiques

Au total, un seul temps d'arrêt peut coûter 451 301 $ pour des applications stratégiques et 781 778 $ pour des applications non stratégiques, en ajoutant les coûts du temps d'arrêt et de la perte de données (fig. 21).

Avec une moyenne de 13 incidents par an, les entreprises subissent un coût annuel moyen s'élevant jusqu'à 10 163 114 $, selon la nature de l'application concernée et la quantité de données perdue dans chaque cas (fig. 22).

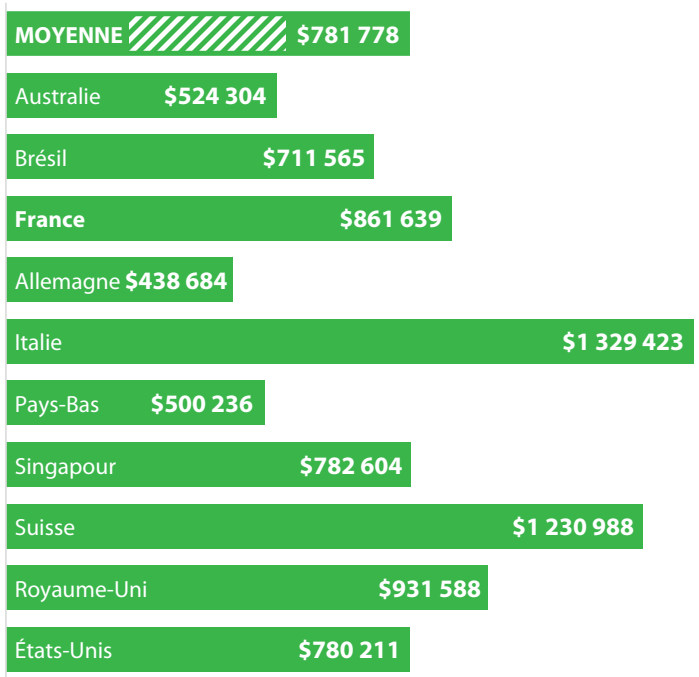



Figure 21 : Coût maximum par temps d'arrêt (en US$)

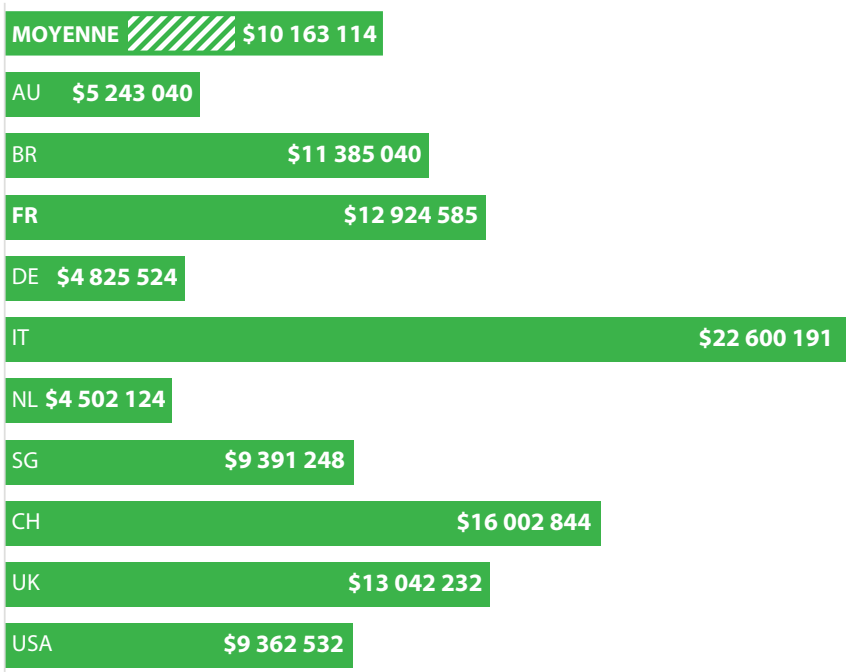



Figure 22 : Coût annuel maximum des temps d'arrêt (en US$)

Ces coûts constituent probablement une raison importante pour laquelle les entreprises exigent la disponibilité constante des services informatiques. Par exemple, si les entreprises pouvaient respecter les niveaux de service sur la perte des données actuellement exigés par la continuité de l'activité comme illustré sur la figure 14, aussi bien pour les applications stratégiques et non stratégiques, et en admettant que le coût horaire des pertes de données indiqué sur la figure 19 reste constant, le risque maximum de perte de données s'élèverait à 226 212 $ pour les applications stratégiques et à 134 031 $ pour les applications non stratégiques. Ceci représente une réduction de risque d'au moins 100 000 $ par incident, soit 1,3 million de dollars par an, par la seule amélioration du RPO (fig. 23). Et étant donné que l'amélioration des RTOs est également susceptible d'affecter les temps d'arrêt, les économies de coûts peuvent s'avérer significatives.

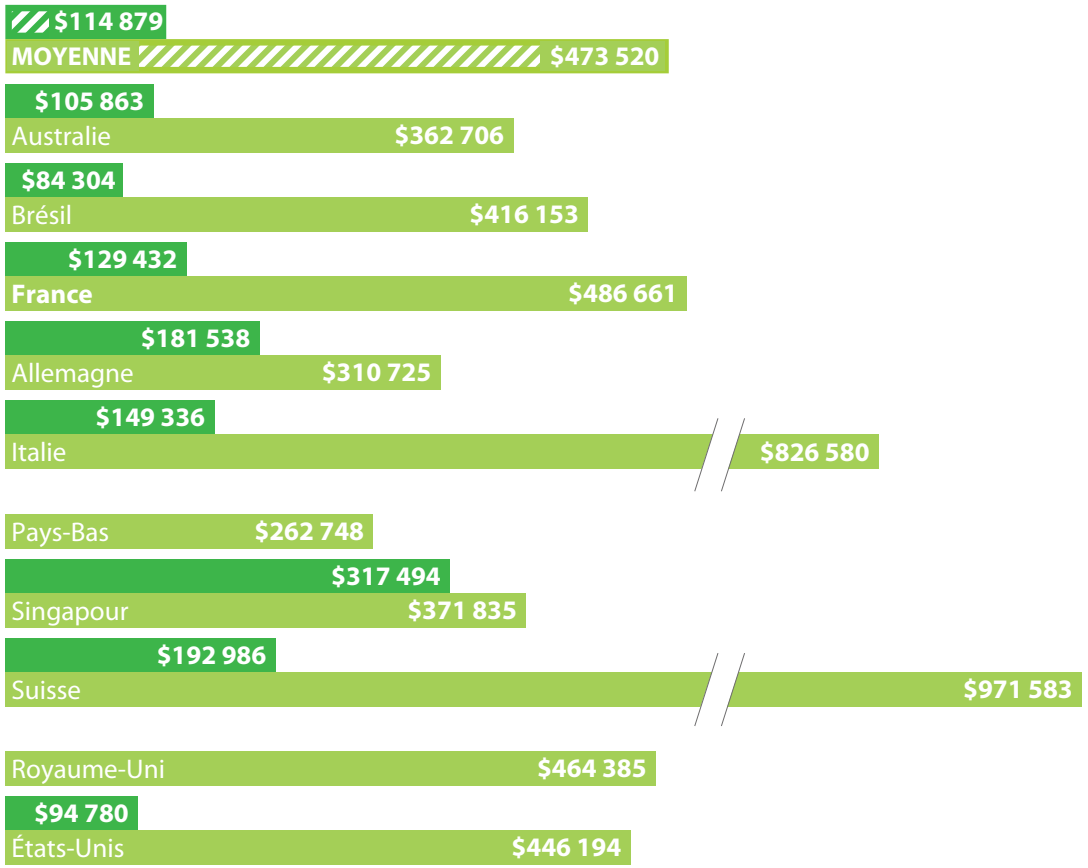



**Figure 23: Risque de perte de données réduit au minimum par incident à partir de RPO améliorés (US$)**

- Temps d'indisponibilité par incident d'application stratégique
- Temps d'indisponibilité par incident non stratégique

En effet, si les entreprises pouvaient atteindre des RTOs et RPOs cibles de 15 minutes ou moins, que les outils modernes de protection des données peuvent fournir, les économies seraient significatives. En supposant à nouveau que le coût horaire des pertes de données et des temps d'arrêt d'applications indiqués sur la figure 17 reste constant, le coût maximal d'une panne d'application s'élèverait à 38 444 $ (fig. 24). Si un temps d'arrêt inattendu se produit 13 fois par an, ceci représente un coût annuel maximum de 499 772 $ et signifie une économie de 932 945 $ au strict minimum.

Ces statistiques montrent les coûts réels de « l'écart de disponibilité ». Et ces coûts ne feront qu'augmenter avec les exigences croissantes de la continuité de l'activité. Les entreprises doivent agir immédiatement afin de s'assurer que les coûts représentés par l'écart de disponibilité ne passent pas de quelques dizaines à plusieurs centaines de milliers de dollars.

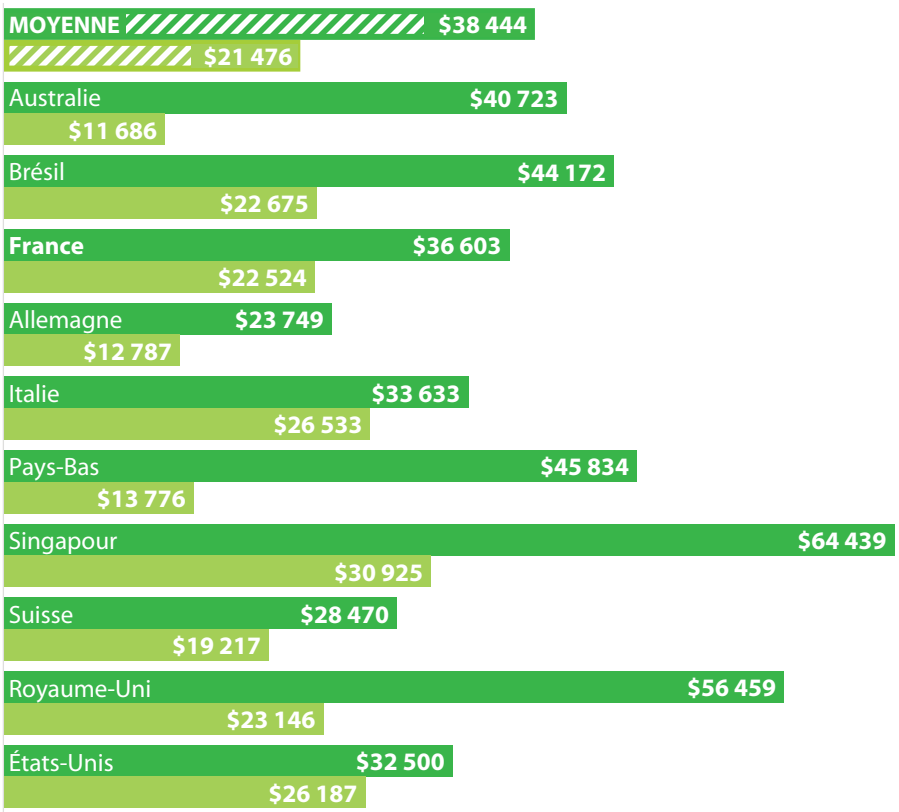



**Figure 24: Coût maximum par incident de temps d'indisponibilité en atteignant les RTPO de 15 minutes (US$)**

- Coût maximum stratégique
- Coût maximum non stratégique

# **Partie 5 :**
# Solutions et fonctionnalités pour la disponibilité (la source du problème)

# Partie 5 : Solutions et fonctionnalités pour la disponibilité (la source du problème)

L'incapacité à assurer la continuité de l'activité incombe finalement à la solution de sauvegarde traditionnelle d'une entreprise : sans capacités suffisantes, les services informatiques ne peuvent pas garantir les RTOs et RPOs exigés par l'activité.

Les entreprises le reconnaissent : 92 % des personnes interrogées identifient les fonctionnalités de protection des données dont elles souhaiteraient disposer dans leur data center, mais qu'elles ne peuvent actuellement implémenter. Ces fonctionnalités comprennent la restauration ultra-rapide, c.-à-d. la capacité de restaurer n'importe quelle application ou n'importe quel serveur en moins de 15 minutes, souhaitée par 60 % des entreprises. D'autres fonctionnalités souhaitées sont la prévention contre les pertes de données, c.-à-d. la réduction des pertes de données à 15 minutes ou moins (53 %), la protection vérifiée, c.-à-d. la restauration garantie de chaque fichier et application à chaque fois (47 %), l'utilisation des données de sauvegarde comme environnement de test similaire à l'environnement de production pour les correctifs ou les mises à jour (38 %), ainsi qu'une visibilité complète avec supervision et alertes proactives en ce qui concerne les problèmes avant toute incidence opérationnelle (36 %) (fig. 25).

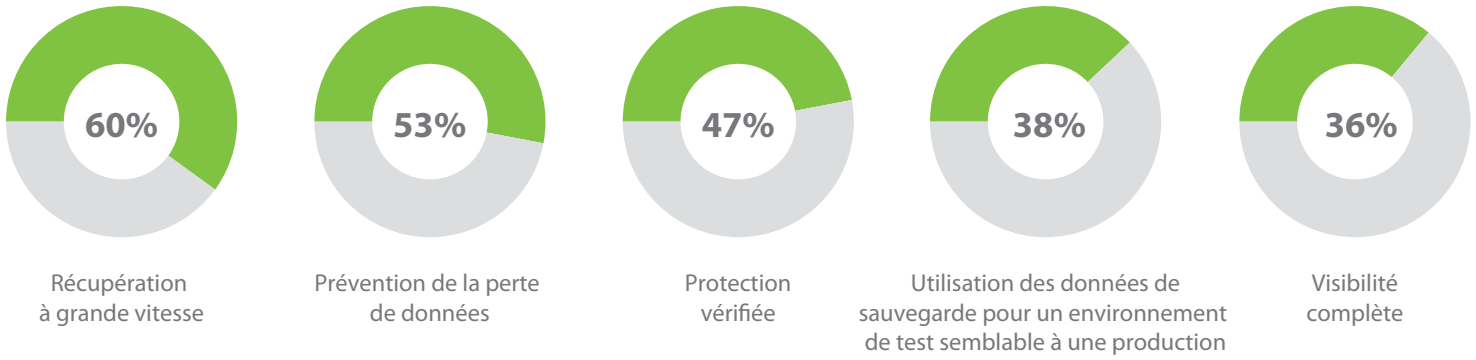



**Figure 25 : Fonctionnalités dont les entreprises voudraient disposer dans leur data center, mais qu'elles ne peuvent pas implémenter (%)**

Les entreprises ont également identifié les barrières les empêchant de mettre en œuvre ces fonctionnalités. Dans chaque cas, le coût des nouvelles technologies constitue la barrière principale. Il est suivi par la complexité du développement ou le manque d'expertise, l'absence de fonctionnalités nécessaires du produit actuel et les contraintes liées aux ressources humaines (fig. 26).

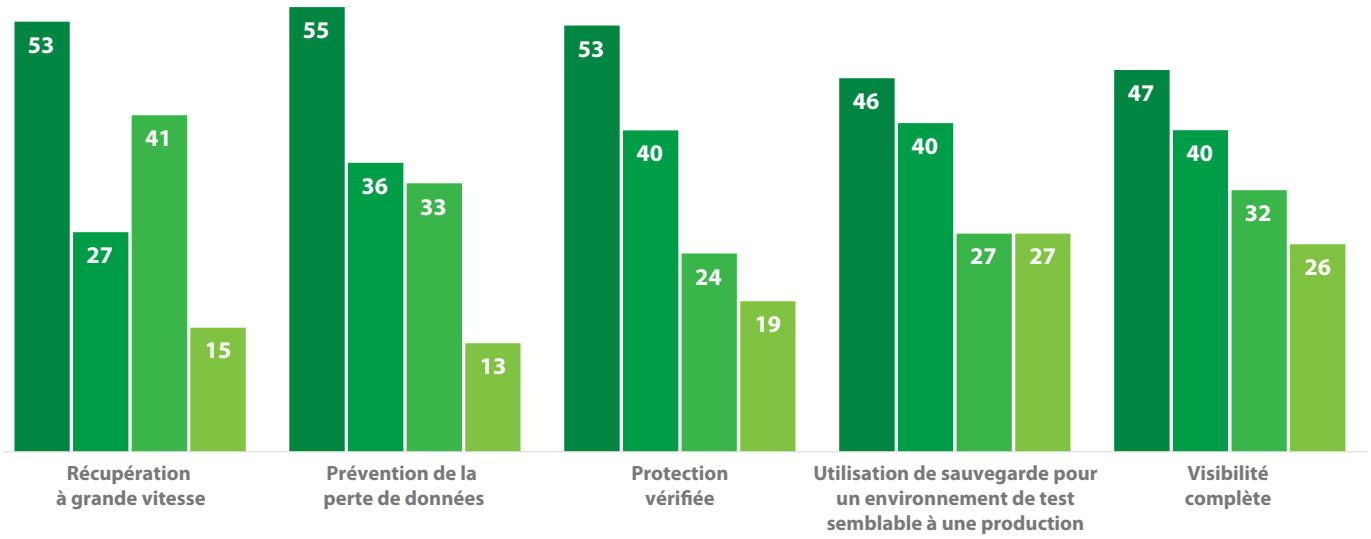



**Figure 26 : Facteurs empêchant les entreprises d'implémenter ces fonctionnalités (en pourcentage d'entreprises indiquant chaque facteur) (%)**


# Partie 6 :
# Un exemple de manque de capacités

# Partie 6 : Un exemple de manque de capacités

Un exemple de la façon dont ce manque de fonctionnalités affecte la disponibilité des données et des applications dans les entreprises se trouve dans les tests et la vérification. Quand une sauvegarde est effectuée, il existe toujours un risque qu'elle soit endommagée et irrécupérable lorsque nécessaire. En testant les sauvegardes, les entreprises peuvent vérifier qu'elles seront correctement restaurées et que rien ne sera perdu. Toutefois, sans fonctionnalités adéquates, la vérification est une tâche consommatrice de temps, ce qui signifie que seulement une fraction des sauvegardes sera vérifiée.

Les entreprises testent la restauration de leurs sauvegardes en moyenne tous les huit jours (fig. 27). Cependant, chaque trimestre, les entreprises testent seulement en moyenne 5,26 % de leurs sauvegardes (fig. 28), ce qui signifie que l'immense majorité des sauvegardes n'est pas vérifiée et peut ainsi mener à des échecs de restauration.

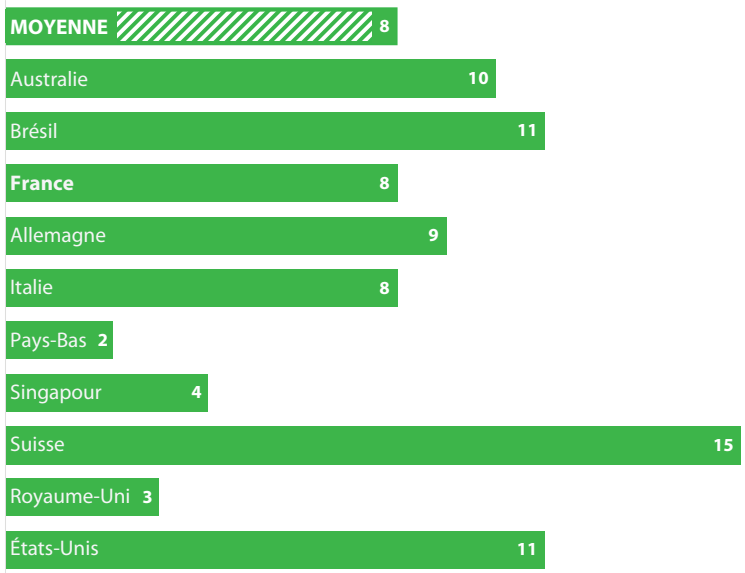



**Figure 27 : Fréquence des tests des sauvegardes (en nombre de jours)**

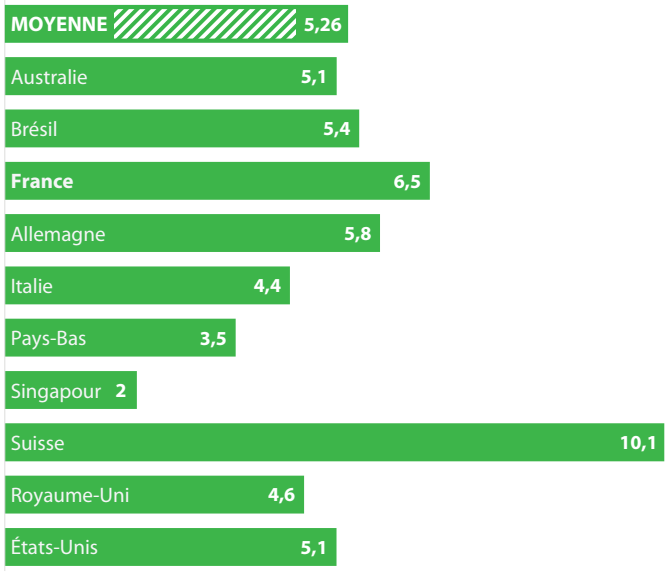



**Figure 28 : Pourcentage des sauvegardes testées chaque trimestre (%)**

Ceci est confirmé par le fait que 16,74 % des sauvegardes ne peuvent être restaurées (fig. 29). Avec des temps d'arrêt non planifiés survenant 13 fois par an, cela signifie que les restaurations effectuées par les entreprises échoueront deux fois chaque année, augmentant ainsi considérablement la durée, les pertes de données et le coût des temps d'arrêt.

En effet, en raison de ces pannes, la perte de données coûtera à une entreprise un minimum de 682 184 $ par an, étant donné que la meilleure situation est celle où le système sera restauré à sa dernière sauvegarde valide (fig. 30).

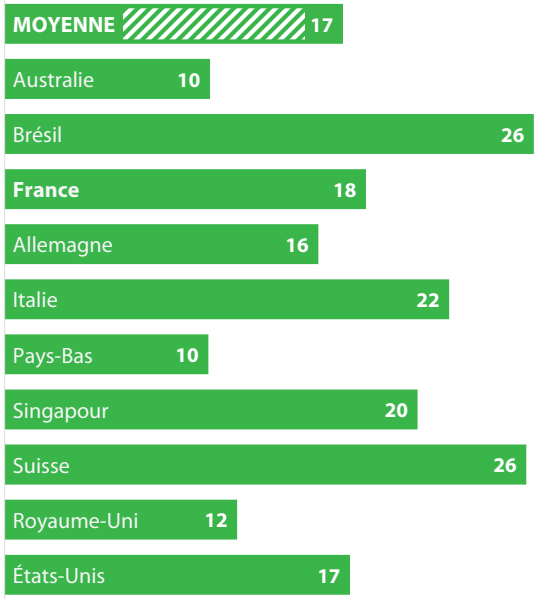



**Figure 29 : Pourcentage des sauvegardes irrécupérables (%)**

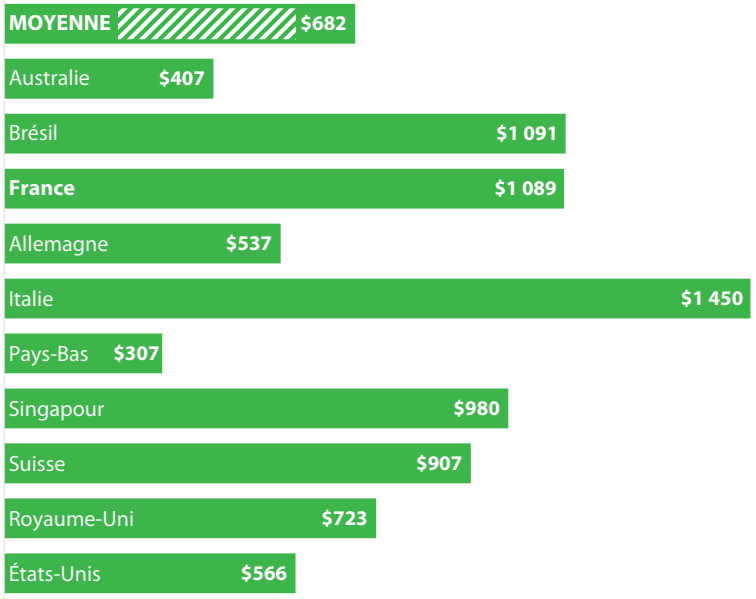



**Figure 30 : Coût annuel minimum des pertes de données inévitables (en milliers de $ US)**

En ajoutant le coût de cette perte de données au coût moyen minimum des temps d'arrêt, une entreprise perdra au moins 2 millions de dollars chaque année en raison des pannes d'applications (fig. 31).

Tester n'est pas seulement nécessaire pour valider la restauration des sauvegardes. Tester les correctifs ou les mises à jour d'applications dans un bac à sable semblable à l'environnement de production avant de les déployer en production permet également de s'assurer que ces correctifs ou mises à jour s'exécuteront comme prévu, et que l'activité ne souffrira pas de temps d'arrêt excessifs. Cependant, ce n'est actuellement pas le cas. 87 % des entreprises signalent des temps d'arrêt plus longs que prévu lors du déploiement de correctifs ou de mises à jour d'applications (fig. 32).

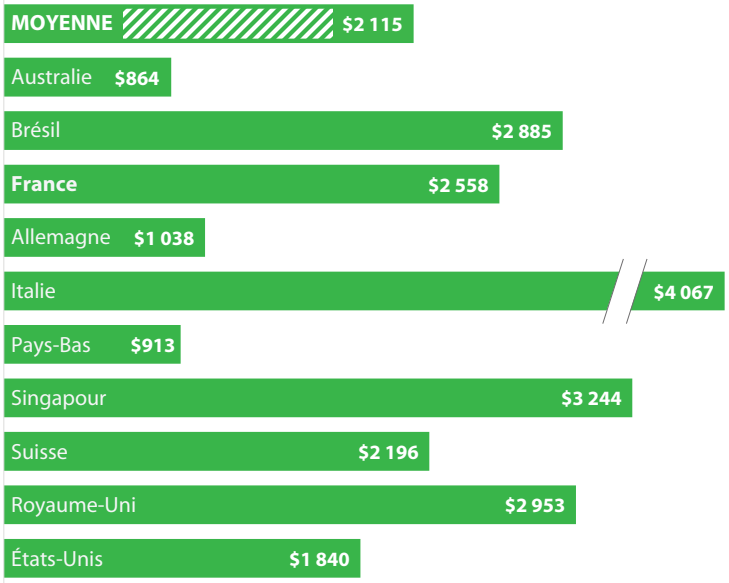



Figure 31 : Coût annuel minimum des pannes d'applications (en milliers de US$)

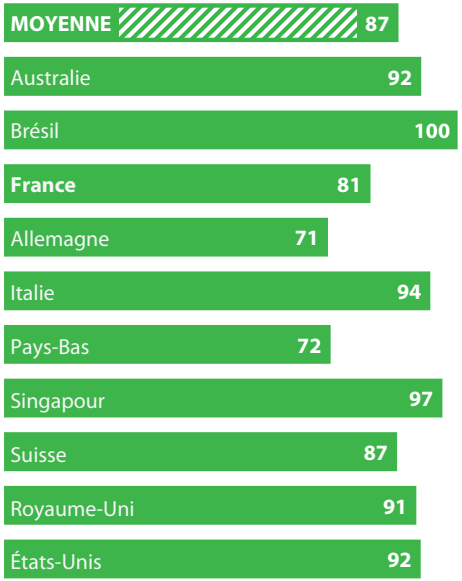



Figure 32 : Pourcentage d'entreprises indiquant des temps d'arrêt supérieurs aux prévisions lors du déploiement de correctifs ou de mises à jour d'applications (%)

# **Partie 7 :** Perspectives d'avenir

# Partie 7 : Perspectives d'avenir

Comme nous avons vu, les entreprises ont conscience de la nécessité d'assurer la disponibilité du data center moderne pour parvenir à la continuité d'activité ou « Always-On Business », et de leur inaptitude à le faire. D'ici deux ans, le paysage devrait être très différent. 78 % des entreprises prévoient de changer de produit de protection des données au cours des deux prochaines années, avec une projection moyenne à six mois (fig. 33).

Cela s'avérera essentiel pour satisfaire leurs exigences commerciales. Il est clair que la tendance actuelle de la modernisation du data center ne donne pas aux entreprises les fonctionnalités dont elles ont besoin pour faire de la continuité de l'activité une réalité. Au lieu de cela, les services informatiques doivent avoir la certitude que les temps de restauration sont aussi courts que possible, que les pertes de données sont minimisées et que les sauvegardes seront restaurées comme prévu lorsque nécessaire. Sans ces capacités, les entreprises n'auront d'autre choix que d'assumer les coûts croissants de l'écart de disponibilité.

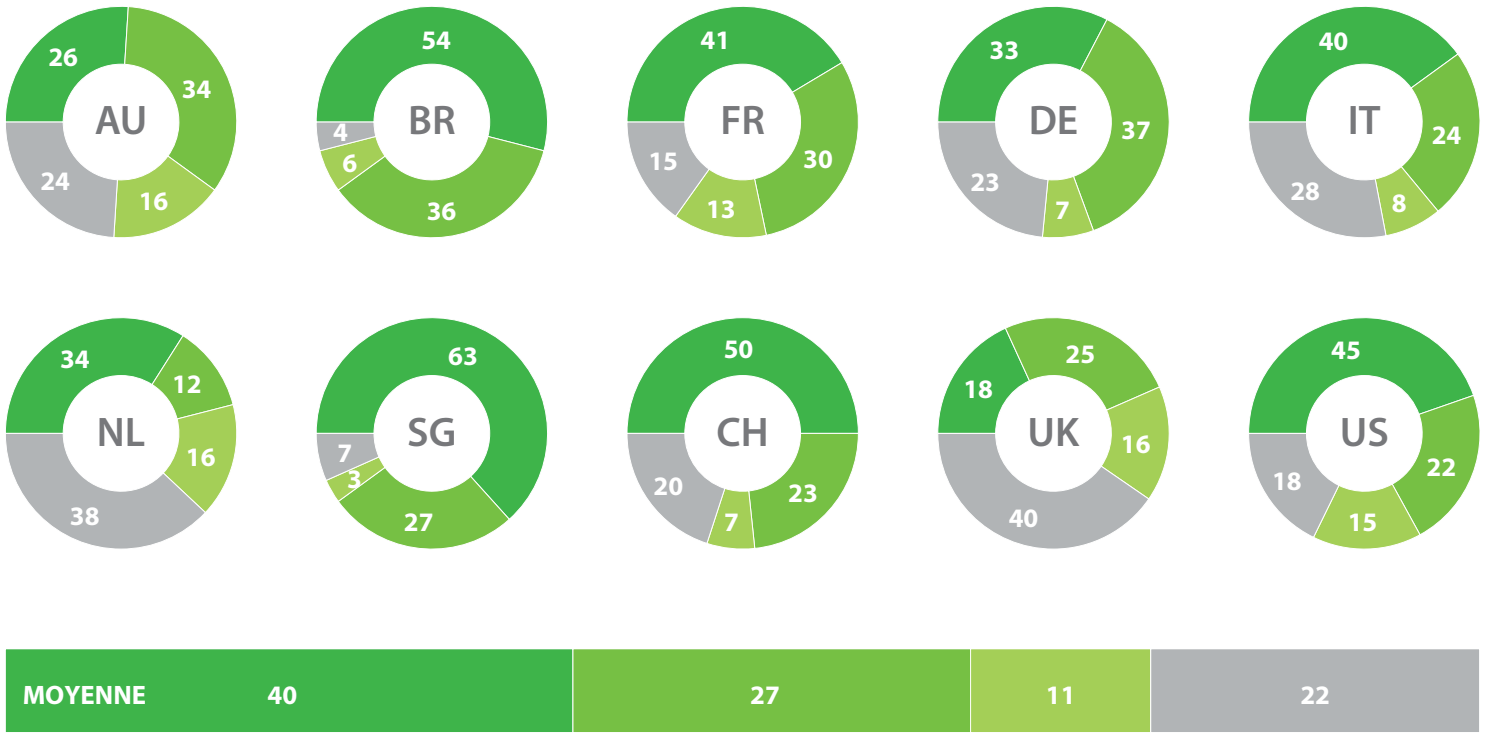



**Figure 33 : Pourcentage d'entreprises projetant de changer de produit de protection des données dans les 2 prochaines années (%)**

- Changement dans les 6 mois
- Changement dans l'année
- Changement dans les 2 ans
- Aucun projet de changement