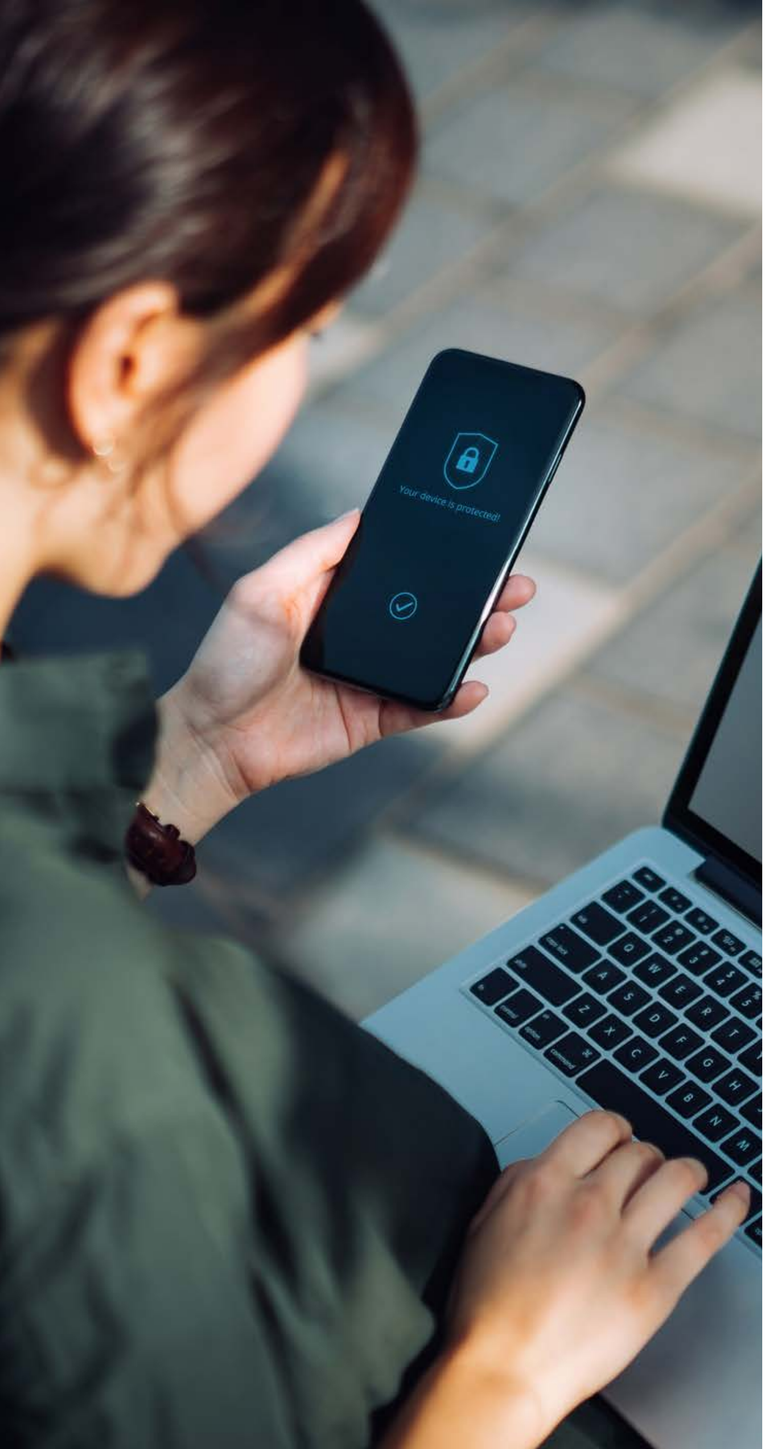
Enterprise Strategy Group | Getting to the bigger truth.™

Créer une entreprise cyber-résiliente prête à innover et à prospérer

Adam DeMattia, directeur senior des études personnalisées

MARS 2022

SOMMAIRE



Objectifs et méthodologie de l'étude

OBJECTIFS :

Cet eBook explique si et dans quelle mesure l'adoption par une organisation d'une stratégie de cyber-résilience solide constitue un facteur de prévisibilité IT, d'innovation métier et de réussite. Les corrélations établies s'appuient sur des données provenant d'organisations homologues. Grâce à cet eBook :

- Découvrez comment nous définissons et mesurons la cyber-résilience et déterminez les performances de votre organisation en la matière.
- Quantifiez les avantages obtenus par les organisations hautement résilientes par rapport à leurs homologues, à la fois en matière de performances IT et métiers.
- Enfin, en découvrant les pratiques des organisations cyber-résilientes, vous saurez comment votre organisation doit faire évoluer ses pratiques et ses priorités pour devenir un leader du marché.

MÉTHODOLOGIE :

Au cours du premier trimestre 2022, ESG a mené une enquête[1] à double insu auprès de 750 décideurs des domaines IT et de la sécurité qui connaissent les technologies de cybersécurité et de résilience utilisées pour protéger les environnements de datacenter et d'appareils d'utilisateurs finaux.

Ces décideurs travaillent dans des entreprises de taille intermédiaire et de grandes entreprises issues d'une combinaison horizontale de secteurs d'activité. L'étude revêt un caractère mondial et couvre l'Amérique du Nord (187 participants), l'Europe de l'Ouest (185 participants), la région APAC (179 participants) et l'Amérique latine (199 participants).

[1] Les participants étaient anonymes et n'ont pas été informés que l'enquête était menée par ESG ou qu'elle était commandée par Dell Technologies.

Retour à la table des matières

Conclusions mises en évidence

Dans cet eBook, les organisations « préparées » sont celles qui disposent d'un niveau optimal d'investissement technologique en matière de sécurité et de dotation en personnel, et qui effectuent une inspection rigoureuse des risques liés aux tiers. L'étude montre que seules 10 % des organisations interrogées présentent actuellement ce niveau de résilience, ce qui souligne la nécessité pour les autres organisations de définir des objectifs organisationnels et de s'améliorer en la matière.

Les organisations cyber-résilientes réduisent les interruptions. Caractéristiques des organisations « préparées » :

7,3 fois plus susceptibles

d'évaluer leur capacité de résilience comme étant excellentes.

2,5 fois plus susceptibles

de fournir un temps d'activité de 99,99 % ou plus pour leurs applications stratégiques, soit un avantage estimé à 33,3 millions de dollars concernant les interruptions de service.

Beaucoup plus agiles

en matière de détection des incidents (temps moyen de détection 20 % plus court) et de réponse (temps moyen de reprise 35 % plus court).

La cyber-résilience est un facteur d'amélioration des performances métiers. Caractéristiques des organisations « préparées » :

8,5 fois plus susceptibles

de déclarer que leurs scores de satisfaction des utilisateurs finaux dépassent généralement leurs objectifs en raison d'un meilleur service et d'une meilleure expérience de l'utilisateur final.

7,7 fois plus susceptibles

que les organisations « exposées » de commercialiser de nouvelles offres et de devancer la concurrence.

Elles prévoient que leur chiffre d'affaires augmentera

2 fois plus vite

que celui de leurs homologues.

Retour à la table des matières

Définition et mesure de la cyber-résilience

Quatre caractéristiques des organisations « préparées » (ou hautement résilientes)

Pour déterminer si l'organisation d'un participant pouvait être classée dans la catégorie « préparée », nous avons examiné ses réponses à quatre questions clés relatives aux niveaux de dotation en personnel de résilience, au manque de compétences, aux investissements technologiques et aux processus d'évaluation des risques :

PERSONNES

Diriez-vous que votre équipe de cyber-sécurité compte assez d'employés ?

- ☑ Aucun poste vacant
- ☐ Personnel réduit, manque de personnel, ou adéquat

Comment décririez-vous le niveau de compétence de votre équipe de cyber-sécurité ?

- ☑ Aucun manque de compétences
- ☐ Nombreuses compétences manquantes, plusieurs compétences manquantes, ou adéquat

TECHNOLOGIE DE RÉSILIENCE

Comment définiriez-vous les investissements de votre organisation dans les produits et services de sécurisation des systèmes, applications et données ?

- ☑ Optimaux
- ☐ Faibles, à améliorer ou adéquats

RISQUES LIÉS AUX TIERS

Votre organisation réalise-t-elle des audits ou inspecte-t-elle la sécurité de ses partenaires/fournisseurs IT ?

- ☑ De façon formelle et rigoureuse
- ☐ De manière informelle, occasionnelle ou pas du tout

Organisations selon leur résilience
(Part de participants, sur un total de 750)

ESG a créé un modèle axé sur les données qui classe les organisations des participants selon trois niveaux de résilience :

Organisations préparées, organisations vulnérables et organisations exposées.

Le modèle utilise les quatre questions de l'enquête (à gauche) pour déterminer le statut d'une organisation. Chacune de ces questions concerne une caractéristique des organisations « préparées » (c'est-à-dire un attribut des organisations hautement résilientes) sur les équipes chargées de la protection de l'entreprise, le financement des technologies d'atténuation des risques ou l'importance accordée à la réduction des risques tiers. Plus l'organisation présente de caractéristiques, plus sa résilience est importante, comme indiqué ci-dessous :

Retour à la table des matières

Les organisations cyber-résilientes réduisent les interruptions

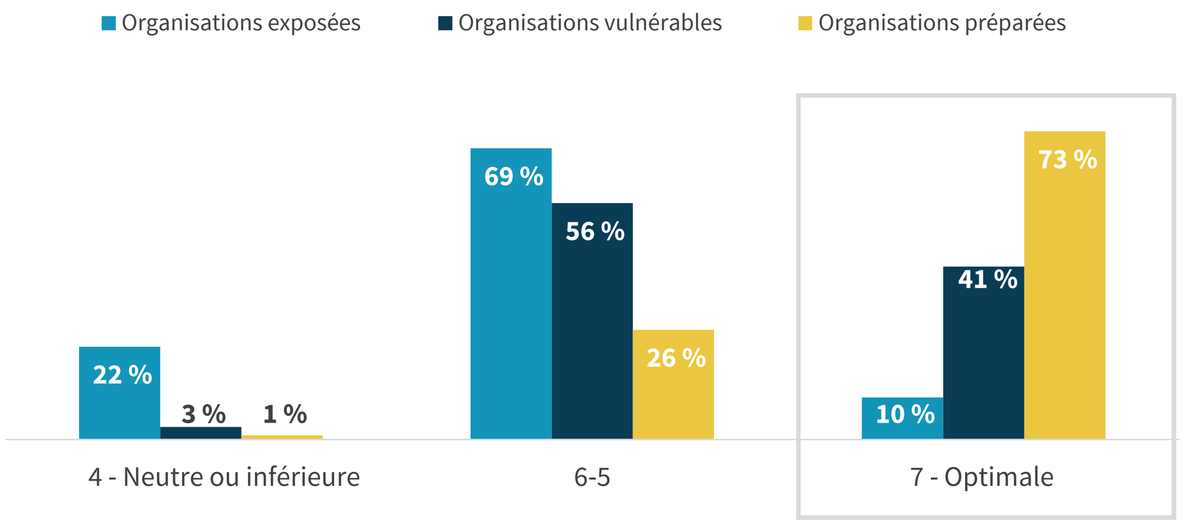
Les organisations « préparées » sont beaucoup plus confiantes dans leur niveau de cyber-résilience que leurs homologues

Bien qu'il s'agisse d'une évaluation qualitative, il est important de mesurer la confiance des responsables IT et de la cybersécurité dans les capacités de résilience de leur organisation. Ces responsables façonnent et dirigent les stratégies de leur organisation et sont les mieux placés pour évaluer la réussite de leur exécution.

Pour mesurer la confiance, nous avons demandé aux participants d'évaluer leur cyber-résilience sur une échelle allant de 7 (excellente) à 1 (médiocre). Les réponses des participants étaient généralement positives, mais seuls 24 % ont évalué la cyber-résilience de leur organisation comme étant « excellente », ce qui reflète un optimisme prudent dans l'ensemble.

Toutefois, la confiance varie considérablement en fonction du niveau de résilience des organisations. Près des trois quarts des responsables des organisations « préparées » (73 %) évaluent leur résilience comme étant excellente.

Comment évalueriez-vous la cyber-résilience globale de votre organisation (c'est-à-dire sa capacité à résister à une cyberattaque et à maintenir ses activités) ? (Pourcentage de personnes interrogées)



Les participants des organisations « préparées » sont

7,3 fois plus susceptibles

que ceux des organisations « exposées » d'évaluer leurs capacités de résilience comme étant « excellentes ».

Retour à la table des matières

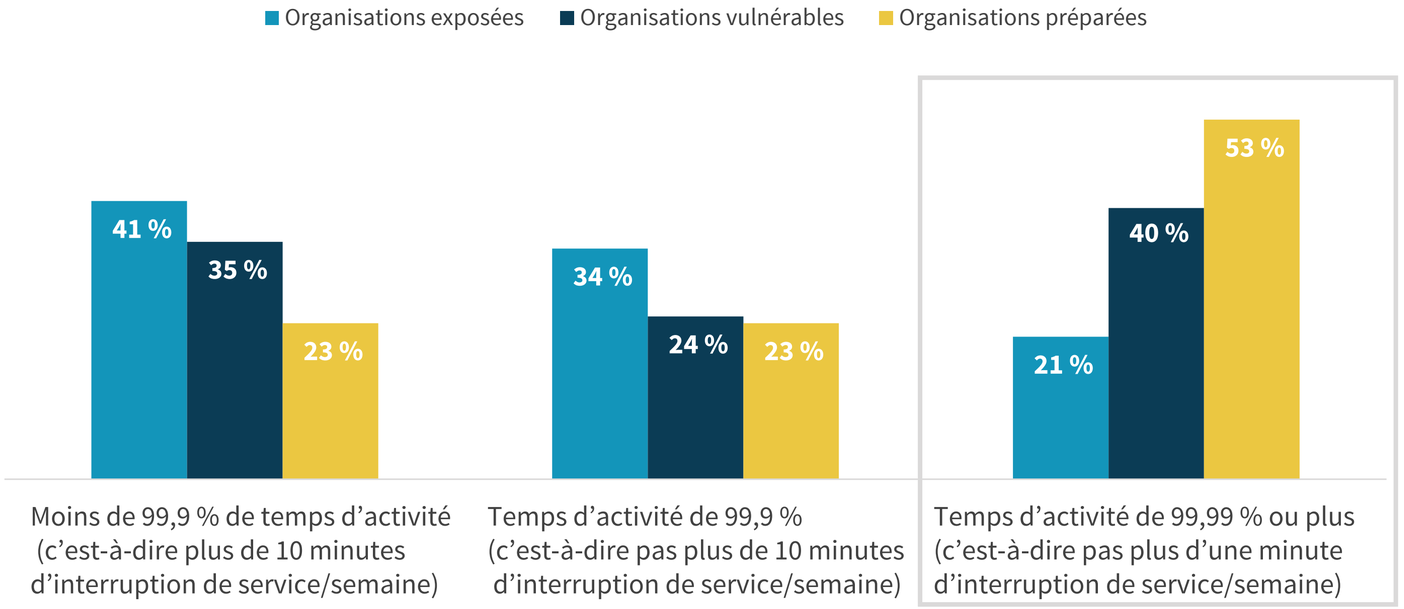
Comparaison du temps d'activité des applications stratégiques atteint pour chacun des niveaux de cyber-résilience

Tout aussi importantes, voire davantage, les mesures qualitatives de résilience sont des mesures quantitatives telles que le temps d'activité, le temps moyen de détection des incidents et le temps moyen de reprise après ces derniers. Chacune d'entre elles est soumise à une analyse comparative dans l'étude.

La protection des processus stratégiques est au cœur de la résilience organisationnelle et les équipes IT et de sécurité doivent maintenir les charges applicatives stratégiques qui sous-tendent ces processus.

Lorsque nous comparons la réussite des organisations dans ce domaine, l'écart est évident : les organisations « préparées » sont 2,5 fois plus susceptibles que les organisations « exposées » de fournir un temps d'activité de 99,99 % ou plus pour leurs applications stratégiques (soit 1 minute d'interruption de service au maximum par semaine, 53 % contre 21 %).

Quel est le contrat de niveau de service de temps d'activité standard que votre organisation fournit pour les charges applicatives stratégiques ?



Les organisations « préparées » sont

2,5 fois plus susceptibles

de fournir un temps d'activité de 99,99 % ou plus pour leurs applications stratégiques.

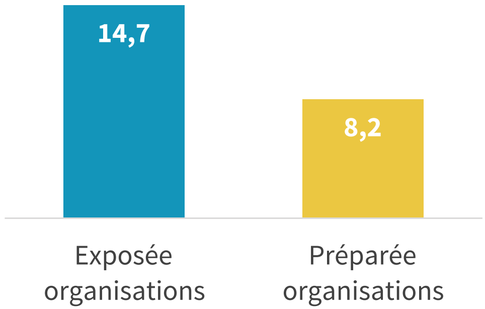
Retour à la table des matières

À combien s’élèvent les avantages des organisations « préparées » en matière d’interruption de service ?

L’étude nous permet de répondre à cette question centrale. Il est évident que l’embauche de personnel, l’investissement dans davantage de technologies de résilience et une inspection rigoureuse des risques liés aux tiers ont un impact sur les coûts. Toutefois, les données montrent que le retour sur investissement est significatif : les organisations « préparées » réduisent les interruptions de service des applications stratégiques de 44 %. En combinant ces données avec le coût horaire moyen des interruptions de service signalé par les participants à l’étude et en multipliant cet impact économique par le nombre total d’applications stratégiques, les données montrent que les avantages en matière d’interruption de service s’élèvent à 33,3 millions de dollars par an pour les organisations « préparées » par rapport aux organisations « exposées ».

INTERRUPTION DE SERVICE

Heures moyennes d’interruption de service par application et par an



×

COÛT HORAIRE MOYEN DES INTERRUPTIONS DE SERVICE[1]

×

NOMBRE TOTAL MOYEN D’APPLICATIONS STRATÉGIQUES[1]

=

Pour les organisations « préparées »

AVANTAGE

Pour les organisations « préparées » :

33,3 millions de dollars/an

[1] Coût horaire moyen des interruptions de service signalé par les participants : 205 000 dollars, [2] Nombre moyen supposé d’applications stratégiques prises en charge : 25 (hypothèse prudente)

Retour à la table des matières

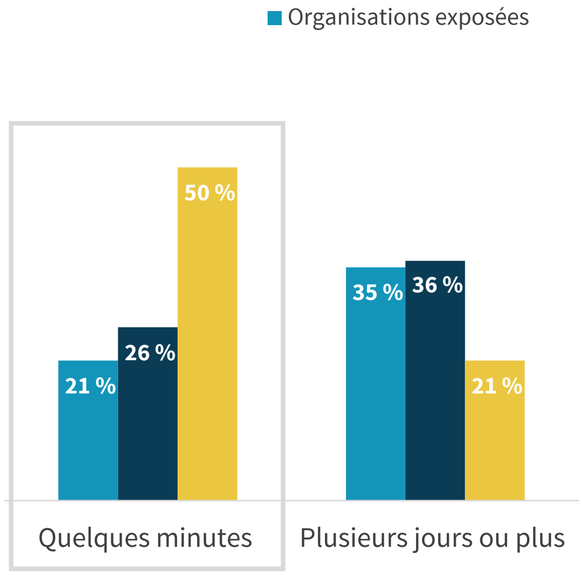
Gestion des alertes et agilité de la réponse aux incidents pour chaque niveau de cyber-résilience

Une fois de plus, en ce qui concerne le temps d'activité et la disponibilité supérieurs offerts par les organisations « préparées », les données sont claires : ces organisations sont bien plus agiles que leurs homologues lorsqu'il s'agit d'enquêter sur les incidents, de les identifier et d'y répondre.

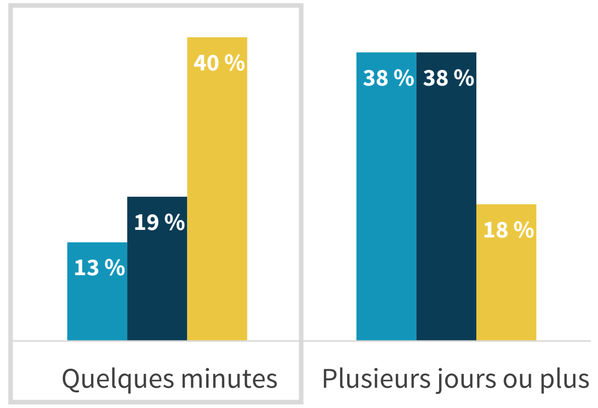
En ce qui concerne l'enquête sur les cyber-incidents et leur identification, nous avons défini le temps moyen de détection comme le temps qui s'écoule entre le moment où une alerte est générée et celui où votre organisation conduit un examen complet afin de déterminer si un incident de sécurité s'est produit. Dans un tel cas, les organisations « préparées » sont 2,4 fois plus susceptibles que les organisations « exposées » d'être en mesure d'enquêter sur les alertes en quelques minutes (ce qui se traduit par un temps de détection moyen 20 % plus court).

Pour mesurer l'agilité de la réponse, nous avons défini le temps de reprise moyen comme le temps moyen qui s'écoule entre la notification des cyber-incidents et la reprise complète des opérations du système d'information. Pour cette mesure, les organisations « préparées » sont 3,1 fois plus susceptibles que les organisations « exposées » d'assurer la reprise après incident en quelques minutes (ce qui se traduit par un temps de reprise moyen 35 % plus court).

Quel est le temps moyen de détection de votre organisation concernant les charges applicatives stratégiques ? (Pourcentage de personnes interrogées)



Quel est le temps moyen de reprise de votre organisation concernant les charges applicatives stratégiques ? (Pourcentage de personnes interrogées)



Les organisations « préparées » sont

2,4 fois plus susceptibles

d'enquêter sur les alertes en quelques minutes.

Les organisations « préparées » sont

3,1 fois plus susceptibles

d'assurer la reprise après incident en quelques minutes.

Retour à la table des matières

Les organisations cyber-résilientes obtiennent de meilleurs résultats opérationnels par rapport à leurs homologues

Les organisations résilientes offrent une expérience d'utilisateur final de premier ordre

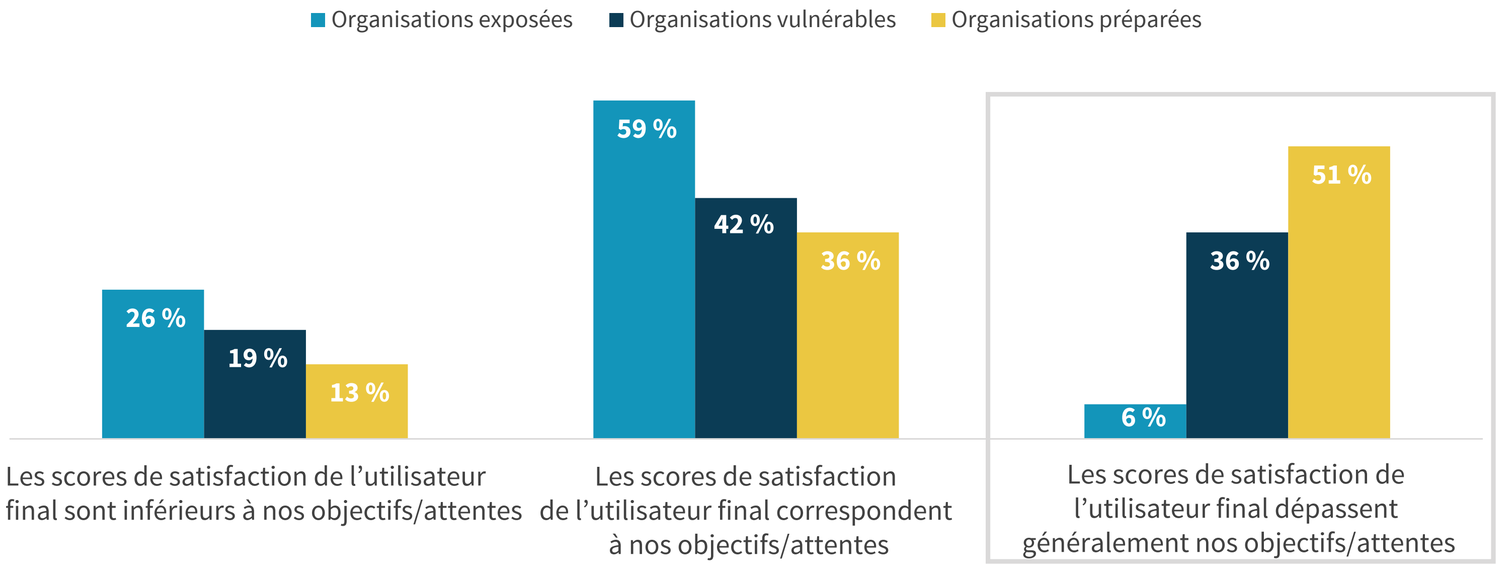
La résilience, comme de nombreux aspects IT, a pour objectif d'être invisible pour les utilisateurs finaux. Les lacunes en matière de résilience se font sentir lorsqu'un événement imprévu se produit.

Les données montrent que les organisations « préparées » sont davantage en mesure (par rapport à leurs homologues) de limiter les interruptions. Les données montrent également que cela permet d'améliorer la satisfaction de l'utilisateur final.

Nous avons demandé aux participants si leur département IT avait atteint les objectifs de satisfaction de l'utilisateur final. La majorité des participants des organisations « préparées » ont déclaré que les objectifs étaient généralement dépassés. En fait, les participants des organisations « préparées » sont 8,5 fois plus susceptibles que ceux des organisations « exposées » de déclarer que les scores de satisfaction de l'utilisateur final dépassent généralement les objectifs.

Il existe une corrélation claire entre le niveau de résilience et la capacité du département IT à fournir l'expérience d'utilisateur final exigée par les utilisateurs métiers.

Dans l'ensemble, votre département IT a-t-il atteint les objectifs formels de satisfaction de l'utilisateur final ? (Pourcentage de personnes interrogées)



Les participants des organisations « préparées » sont

8,5 fois plus susceptibles

de déclarer que leurs scores de satisfaction de l'utilisateur final dépassent généralement leurs objectifs.

Retour à la table des matières

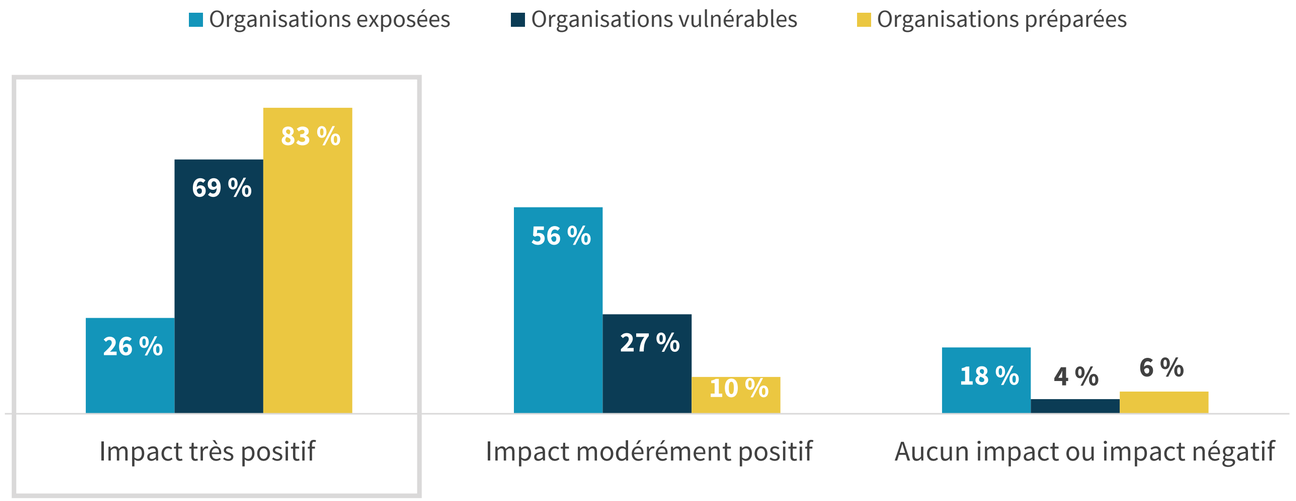
La résilience n’est pas simplement corrélée avec l’amélioration de l’expérience de l’utilisateur final : elle la favorise.

Bien sûr, « corrélation » ne signifie pas « causalité », mais l’étude fournit la preuve d’un rapport de cause à effet entre les investissements dans la résilience et l’amélioration de l’expérience d’utilisateur final.

Nous avons demandé aux participants s’ils pensaient que les investissements de leur organisation dans la résilience ont eu un impact positif, neutre ou négatif sur des éléments tels que l’agilité, l’innovation et l’expérience de l’utilisateur final, et 87 % ont signalé un impact positif.

En approfondissant davantage et en examinant les données par niveau de résilience, nous constatons que les participants des organisations « préparées » sont 3,2 fois plus susceptibles que ceux des organisations « exposées » de déclarer que leurs investissements en matière de résilience ont considérablement amélioré l’expérience des utilisateurs finaux, l’agilité et l’innovation.

Les investissements de votre organisation dans la résilience ont-ils eu un impact positif/neutre/négatif sur l’agilité, l’innovation et l’expérience d’utilisateur final ? (Pourcentage de personnes interrogées)



Les participants des organisations « préparées » sont

3,2 fois plus susceptibles

d’affirmer que leurs investissements en matière de résilience ont un impact très positif.

Retour à la table des matières

Comment l'investissement dans la résilience fait avancer les entreprises

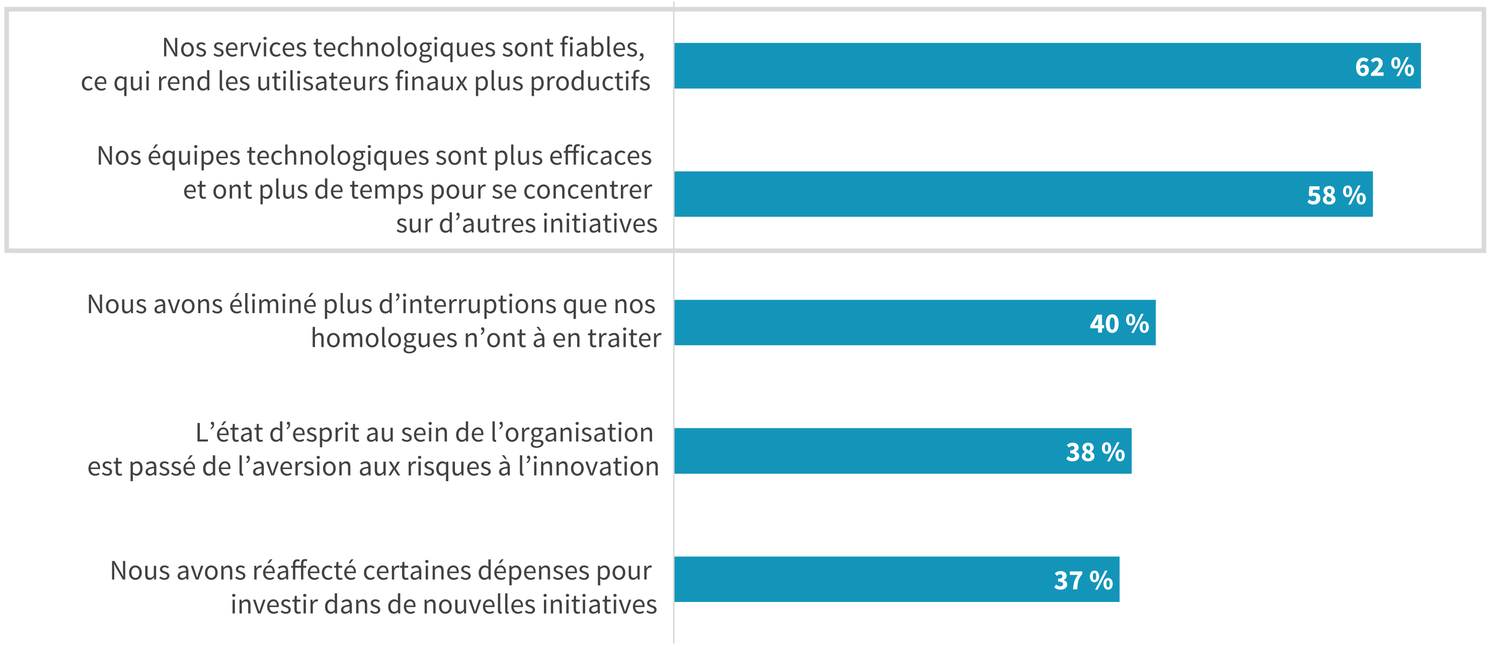
L'étude répond à la question intéressante de savoir comment la résilience améliore les capacités de l'entreprise.

Deux impacts clés et complémentaires se démarquent. Tout d'abord, la résilience assure la disponibilité des parties prenantes et des centres de profit de votre entreprise : 62 % des participants déclarent que leurs investissements contribuent à garantir que les services technologiques sur lesquels les utilisateurs finaux s'appuient pour être efficaces sont disponibles et performants.

Deuxièmement, 58 % des participants déclarent que l'investissement dans des bases solides de résilience réduit les incidents que les équipes technologiques doivent résoudre, ce qui leur permet de consacrer leurs efforts au soutien et à l'accélération de projets et d'initiatives innovants qui donneront à leur organisation un avantage concurrentiel.

« Deux impacts clés et complémentaires se démarquent. »

Comment les investissements dans la résilience contribuent-ils à la réussite de votre entreprise ? (Pourcentage de personnes interrogées)



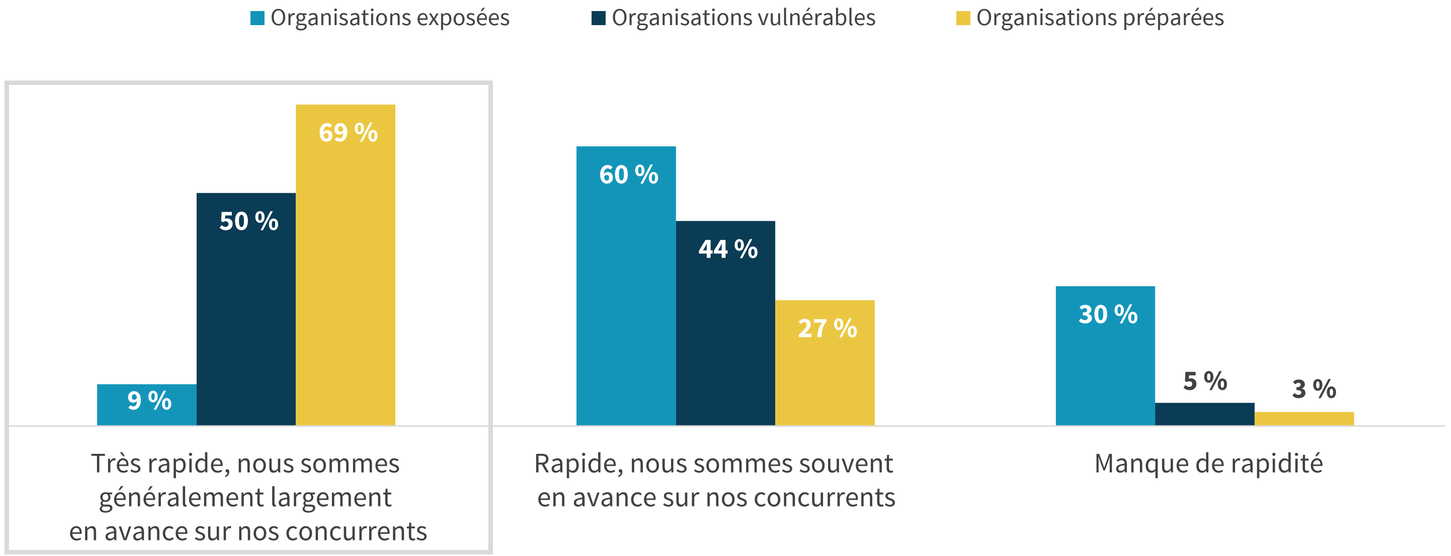
Retour à la table des matières

Les organisations résilientes sont mieux à même de soutenir l'innovation

Les données indiquant la capacité de la résilience à soutenir l'innovation organisationnelle sont probantes. Les organisations « préparées » sont 7,7 fois plus susceptibles que les organisations « exposées » de commercialiser de nouvelles offres avant la concurrence.

Lorsqu'il leur a été demandé de partager plus de détails sur cet avantage, dans l'ensemble, les participants des organisations « préparées » ont déclaré en moyenne que leur organisation avait plus de 8 mois d'avance sur ses concurrents en matière de délai de commercialisation, soit un avantage considérable pour ces précurseurs.

Dans quelle mesure votre organisation réussit-elle à développer et à lancer de nouveaux produits et services par rapport à ses concurrents ? (Pourcentage de personnes interrogées)



Les organisations « préparées » sont

7,7 fois plus susceptibles

de commercialiser de nouvelles offres avant la concurrence.

Retour à la table des matières

Les organisations résilientes sont plus optimistes quant à la croissance du chiffre d'affaires dans le futur

Au-delà de l'innovation, la résilience est un facteur indiscutable de croissance.

Nous avons demandé aux participants quel était le taux de croissance du chiffre d'affaires de leur organisation auquel ils s'attendaient au cours des prochaines années.

En moyenne (médiane), les participants des organisations « préparées » s'attendaient à ce que le chiffre d'affaires de leur société augmente deux fois plus que celui des organisations « exposées ». La capacité de ces organisations à éliminer les interruptions, à maintenir la productivité du personnel et à innover est un facteur décisif de l'optimisme des participants.

D'après vous, à quel taux annuel votre organisation va-t-elle développer (ou contracter) son chiffre d'affaires au cours des années à venir ? (Taux de croissance annuel moyen)

Les participants des organisations « préparées » prévoient que leur chiffre d'affaires

augmentera 2 fois plus rapidement

que celui des organisations « exposées ».

Retour à la table des matières

Comment devenir une entreprise cyber-résiliente

Les organisations « préparées » allouent plus de dépenses technologiques à la cybersécurité que leurs homologues

Nous savons, selon nos critères de segmentation, que les organisations « préparées » financent les technologies de cybersécurité et de résilience à un niveau qu'elles considèrent comme « optimal », tandis que les organisations « vulnérables » et « exposées » considèrent que des améliorations peuvent être apportées.

Toutefois, ces données sans contexte ne sont pas exploitables par les responsables IT et de sécurité. Pour aller plus loin, nous avons demandé aux participants quel pourcentage de leurs dépenses technologiques était alloué à la cybersécurité. Nous avons constaté que les organisations « préparées » consacrent près de 14 % de leur budget technologique à la cybersécurité, soit 49 % de plus que leurs homologues « exposés ».

Les organisations dont les dépenses sont inférieures à ce seuil doivent modifier leurs investissements pour s'aligner sur les leaders du marché.

Quel pourcentage du budget IT votre organisation alloue-t-elle à la cybersécurité ? (Moyenne estimée)

En moyenne, les organisations « préparées » prélèvent

49 % de plus

sur leurs budgets technologiques pour investir dans les domaines de la cybersécurité/résilience.

Retour à la table des matières

Les organisations « préparées » allouent davantage de capital humain à la sécurité et à la résilience

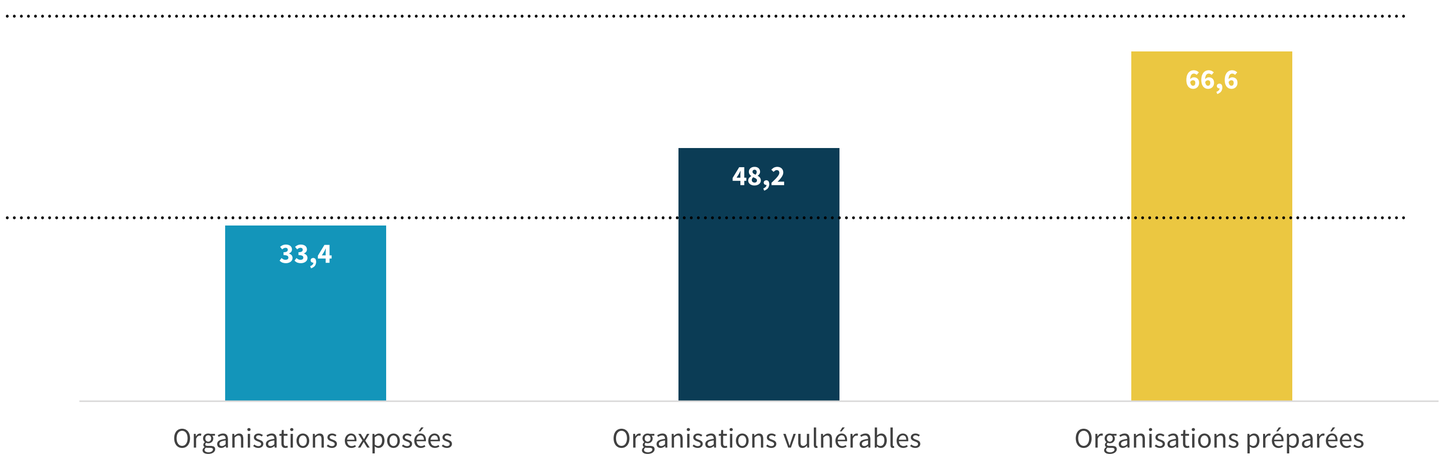
À l'instar du financement, nous savons que les organisations « préparées » estiment que leurs équipes de sécurité (y compris les professionnels IT axés sur la sécurité) disposent d'un personnel suffisant. Cependant, si nous nous penchons sur le nombre moyen d'ETP alloués par niveau de résilience, nous pouvons voir à quel point la disparité est grande.

En moyenne, les organisations « préparées » emploient deux fois plus d'ETP dans leurs équipes de sécurité que les organisations « exposées » (66,6 ETP contre 33,4).

L'analyse de ces données par taille d'entreprise permet de rendre ces informations encore plus concrètes.

- Les entreprises « préparées » de taille intermédiaire et de taille moyenne (250 à 4 999 collaborateurs) emploient 62 ETP, contre 27,7 ETP pour leurs homologues « exposés ».
- Les grandes entreprises « préparées » (plus de 5 000 collaborateurs) emploient 76,8 ETP, contre 47,8 ETP pour leurs homologues « exposés ».

Environ combien d'ETP dédiés l'équipe de cybersécurité interne de votre organisation compte-t-elle (en incluant les rôles IT axés sur la cybersécurité) ? (Moyenne estimée)



En moyenne, les organisations « préparées » emploient

deux fois plus d'ETP

dans leur équipe de sécurité.

Retour à la table des matières

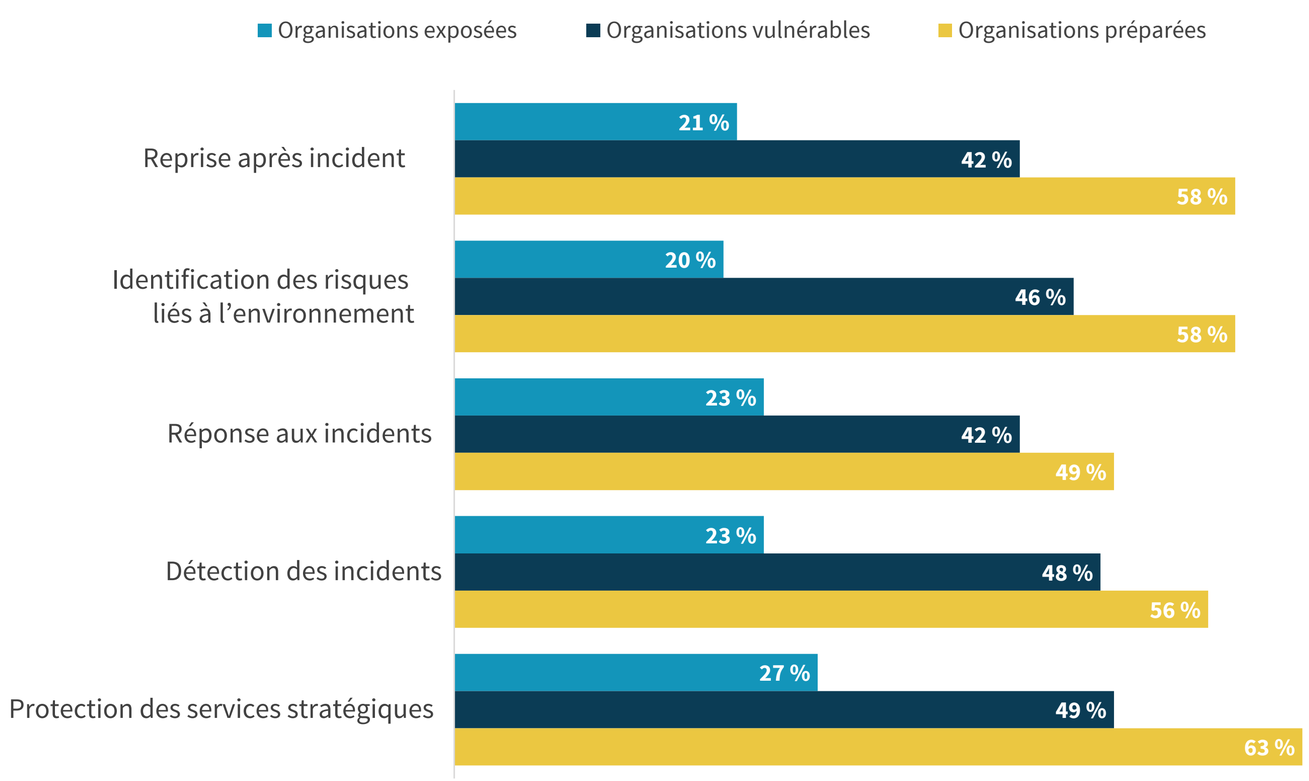
Les organisations « préparées » accroissent leurs investissements tout au long du cycle de vie des risques

Les participants ont été invités à réfléchir à leurs investissements tout au long du cycle de vie des risques (tel que défini par le CSF du NIST), de l'identification des risques à la reprise après incident.

Conclusion : les organisations « préparées » sont beaucoup plus susceptibles que leurs homologues d'avoir augmenté leurs investissements de plus de 15 % en glissement annuel dans tous les domaines.

Ce comportement souligne l'importance d'une stratégie de défense en profondeur face aux risques qui donne aux organisations les ressources nécessaires pour limiter les risques à chaque étape.

Parmi les domaines suivants d'atténuation des risques, dans lesquels votre organisation a-t-elle augmenté ses investissements de plus de 15 % en glissement annuel au cours des 12 à 24 derniers mois ? (Pourcentage de personnes interrogées)



Retour à la table des matières

Les organisations « préparées » renforcent leur environnement avec des technologies intrinsèquement sécurisées

Cet eBook met l'accent sur le concept de résilience organisationnelle et les résultats associés de manière globale. L'étude explore de façon plus approfondie plusieurs aspects des environnements des organisations, du stockage aux serveurs, en passant par les appareils clients.

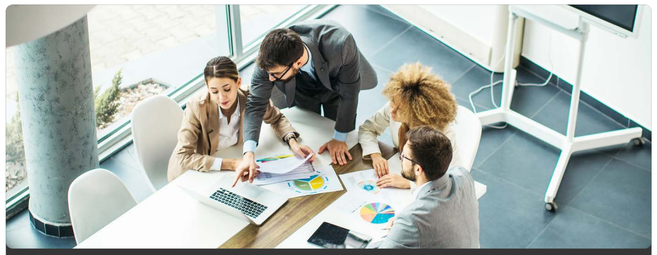
Dans chaque domaine, les organisations « préparées » sont leaders sur le marché en matière d'adoption de technologies dotées de fonctionnalités de sécurité intrinsèques. En outre, elles améliorent les performances en réduisant les interruptions de service, le nombre d'interruptions de service et la fréquence de corruption des appareils.

Les organisations « préparées » réduisent les pannes et la perte de données dans leur environnement de stockage grâce à des solutions dotées de fonctionnalités intrinsèques de protection des données.

CONSULTER LE RAPPORT

Les organisations « préparées » favorisent l'innovation grâce à l'automatisation intelligente de la sécurité dans leur environnement de calcul.

CONSULTER LE RAPPORT



Les organisations « préparées » réduisent la corruption des appareils et limitent la perte de données grâce aux technologies clientes dotées de fonctionnalités de sécurité intrinsèques, ce qui leur permet d'offrir aux collaborateurs une expérience optimale.

CONSULTER LE RAPPORT

Les organisations « préparées » privilégient l'adoption de solutions technologiques dotées de fonctionnalités de sécurité intrinsèques. Découvrez-en davantage sur ce concept et sur les motivations des organisations.

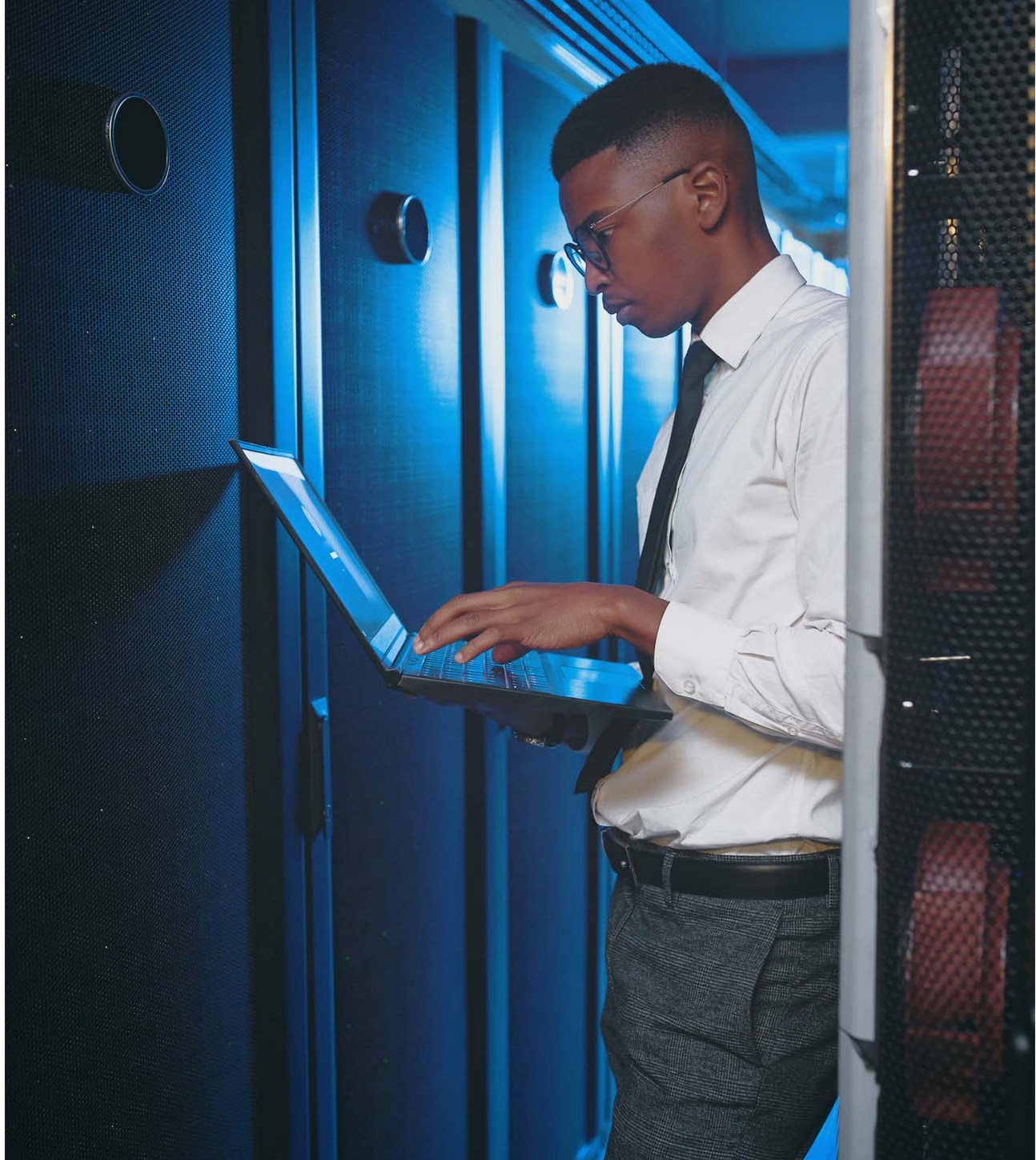
CONSULTER LE RAPPORT

Retour à la table des matières

Conclusion

Que ce soit grâce à leur capacité à maintenir la productivité des utilisateurs finaux, à répondre rapidement aux incidents de sécurité ou à libérer du temps pour les équipes techniques afin qu'elles fassent progresser les initiatives stratégiques de transformation de l'IT, les organisations « préparées » sont un exemple convaincant, étayé par les données, pour toutes les organisations qui s'efforcent d'atteindre un haut niveau de résilience. Selon la situation actuelle de votre organisation, ce parcours peut sembler complexe, mais cette étude vous aidera à construire votre dossier commercial.

Comment Dell Technologies peut vous aider



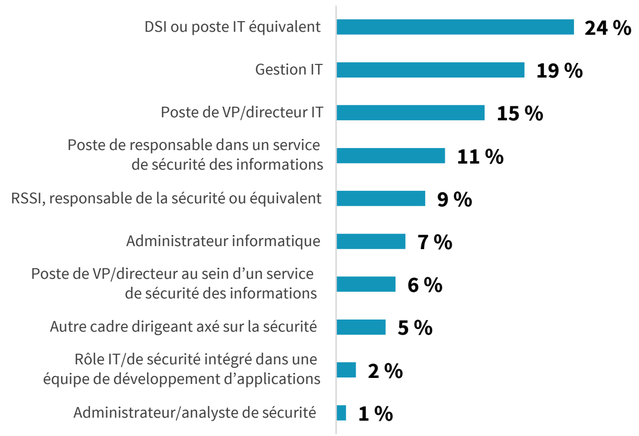
Données démographiques

Les données présentées dans ce rapport proviennent d'une enquête réalisée entre le 11 janvier et le 7 février 2022. Ces chiffres décrivent en détail les profils des participants de l'enquête situés en Amérique du Nord (187 participants), en Europe de l'Ouest (185 participants), dans la région APAC (179 participants) et en Amérique latine (199 participants).

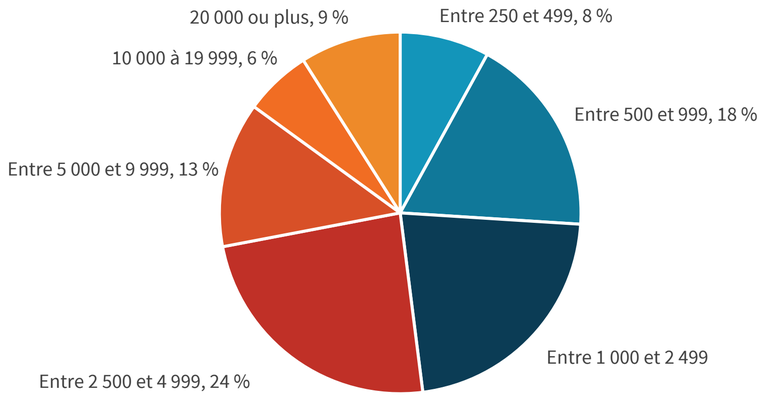
Il est possible que le résultat de l'addition des totaux des figures et des tableaux de ce rapport ne soit pas égal à 100 %, en raison de l'arrondi.

Pour un échantillon de 750 participants au niveau de confiance de 95 %, la marge d'erreur est de +/- 4 %.

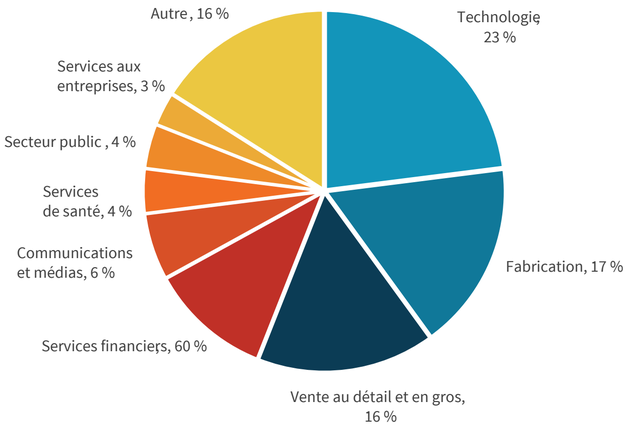
PARTICIPANTS PAR INTITULÉ DE POSTE



PARTICIPANTS PAR TAILLE D'ENTREPRISE



PARTICIPANTS PAR SECTEUR D'ACTIVITÉ



Retour à la table des matières

À propos de Dell Technologies, d'Intel et de VMware

La technologie n'a jamais été aussi importante qu'actuellement, à l'ère des données, et Dell estime qu'elles revêtent un pouvoir considérable pour améliorer le monde. Nous nous engageons à faire perdurer ce rôle qu'a la technologie dans le progrès humain, en vous aidant à planifier vos stratégies, et à vous préparer et vous protéger des attaques, afin que vous puissiez réaliser l'impossible, en toute confiance.

Sur site, dans le Cloud public comme à la périphérie, Dell Technologies et Intel collaborent pour garantir des performances optimales sur un large éventail de charges applicatives. La gamme centrée sur les données d'Intel repose sur des dizaines d'années d'optimisation des applications. Conçue pour stimuler votre activité, elle vous permet de stocker plus de données et de traiter toutes les opérations en périphérie comme sur le Cloud.

Ensemble, VMware et Dell offrent une valeur unique à leurs clients communs. Nos plateformes et solutions intégrées, ainsi que l'engagement sans faille des clients à l'échelle mondiale, accélèrent le processus de transformation numérique. La modernisation innovante des applications, le multi-cloud et le logiciel Anywhere Workspace proposés par VMware sont combinés à la vaste gamme de solutions IT de Dell Technologies, allant des points de terminaison au Cloud, afin d'aider les clients à réaliser des opérations sécurisées et cohérentes, tout en raccourcissant le délai de rentabilisation.

Retour à la table des matières

Enterprise Strategy Group est une entreprise intégrée d'analyse, de recherche et de stratégie technologiques qui fournit des données relatives aux marchés, des renseignements exploitables et des services de commercialisation à la communauté internationale des technologies.