La résilience numérique porte ses fruits

Une étude indique que toutes les organisations subissent des perturbations, mais certaines parviennent à les surmonter en investissant dans 5 domaines stratégiques.

splunk>

Résumé

Toutes les organisations ou presque ont déjà subi des interruptions de service, des défaillances et des failles de sécurité, surtout ces deux dernières années. Alors pourquoi certaines ont-elles mieux géré la situation que les autres ?

Pour le découvrir, Splunk a interrogé 2 100 leaders de la sécurité, de l'IT et du DevOps dans de grandes organisations au sein de onze pays et plus de six secteurs d'activité. Nous avons identifié quatre stades de maturité en termes de résilience : Lancement, Développement, Intermédiaire et Avancé. Nous avons aussi appris qu'un bon investissement finit par porter ses fruits.

L'étude indique que les organisations résilientes sont non seulement capables de survivre, mais aussi de prospérer. Malgré les défis liés à la pandémie mondiale et à une montée de l'instabilité économique et politique, les organisations les plus avancées dans ce domaine économisent en moyenne 48 millions de dollars par an selon l'étude.

Plutôt que de se concentrer sur des aspects précis de la résilience, comme la reprise après une catastrophe ou leur plan de continuité des activités, ces organisations ont développé cinq domaines stratégiques : visibilité, détection, investigation, réponse et collaboration.

Cette étude démontre la rentabilité de la résilience. Les organisations avancées parviennent mieux que les autres à minimiser les coûts liés aux interruptions de service. Elles sont mieux préparées au changement, mènent plus efficacement leur transformation numérique, et atteignent et dépassent plus souvent leurs objectifs financiers. Le rapport met en évidence des points de départ pour le parcours de résilience et les facteurs clés qui apportent le plus d'avantages : gestion de crise inter-fonctionnelle, réponse automatique aux incidents et collaboration pour prendre en charge l'accélération des cycles de publication.

L'étude révèle que près de la moitié des organisations ne sont pas complètement prêtes à s'adapter aux perturbations, qu'elles proviennent d'une récession (48 %) ou de la concurrence (50 %). En attendant, les événements macroéconomiques, les failles de sécurité, les interruptions liées à l'infrastructure et les autres défis capables de paralyser les organisations ne montrent aucun signe d'affaiblissement. Par conséquent, les RSSI, les DSI et les directeurs techniques doivent d'ores et déjà se préparer à préserver l'activité de leurs organisations.

Résilience numérique

Capacité à prévenir et à détecter les événements susceptibles de perturber les processus et services de l'entreprise, à y répondre et à s'en rétablir.

Le défi : des perturbations sont inévitables

La pandémie et d'autres événements majeurs ont changé la signification des termes « efficacité des opérations » pour les organisations actuelles. Malgré ces changements incessants, les clients continuent d'attendre des expériences sécurisées, transparentes et toujours disponibles. Le rythme de la transformation et les enjeux pour les organisations sont plus élevés que jamais.

C'est la nouvelle norme. Comme personne n'est insensible aux perturbations, les organisations qui investissent dans la résilience disposent d'un immense avantage.

D'après notre étude, les organisations qui maîtrisent la résilience économisent en moyenne 48 millions de dollars par an sur les coûts liés aux interruptions. Ces entreprises peuvent gérer plus facilement les opérations quotidiennes, résister aux événements soudains majeurs et assurer leur transformation.

Méthodologie

En octobre 2022, des chercheurs ont interrogé plus de 2 100 leaders de la sécurité, de l'IT et du DevOps dans onze pays. Les participants étaient des cadres et des dirigeants issus d'entreprises d'au moins 1 000 employés.

11 pays : Allemagne, Australie, Brésil, Canada, États-Unis, France, Inde, Japon, Nouvelle-Zélande, Royaume-Uni, Singapour

7 secteurs d'activité : industrie manufacturière, santé, secteur public, services financiers, télécommunications, vente au détail, technologie.

5 domaines essentiels de la résilience

Nous avons demandé aux participants de répondre à 26 questions à propos de 5 domaines clés de la résilience pour évaluer le stade de maturité de leur résilience. Ces questions portent sur des aspects spécifiques de chaque fonction, comme la couverture des données au sein d'environnements hybrides et multicloud, le tri des alertes, le partage de données au travers de la sécurité, de l'IT et du DevOps, etc.

Visibilité

Quelle visibilité les équipes ont-elles sur leur environnement technologique, la qualité et la fidélité des données, et l'exhaustivité de la couverture ?

Détection

Dans quelle mesure les organisations exploitent-elles les données pour identifier les problèmes potentiels, accroître la couverture de la détection et produire des alertes ?

Investigation

Les organisations utilisent-elles pleinement les données pour rechercher des problèmes potentiels et accélérer les analyses, pour apporter du contexte, traquer les menaces et analyser les logs, les métriques et les traces ?

Réponse

À quelle vitesse les équipes de sécurité, IT ou DevOps répondent-elles aux problèmes et aux incidents quotidiens ?

Collaboration

Dans quelle mesure les équipes et les outils à leur disposition facilitent-ils la collaboration de la sécurité, de l'IT et du DevOps ?

Les organisations avancées qui maîtrisent la résilience **économisent en moyenne 48 millions de dollars par an** sur les coûts liés aux interruptions.

Les organisations repensent la résilience

Par le passé, les leaders pensaient que la résilience se limitait aux fonctions d'audit, de risques et de conformité. Les plans de continuité des activités et de récupération en cas de sinistre sont souvent vus comme une simple formalité par la direction.

À l'heure actuelle, la résilience est devenue stratégique et doit être intégrée aux plans, aux décisions et aux technologies de l'organisation.

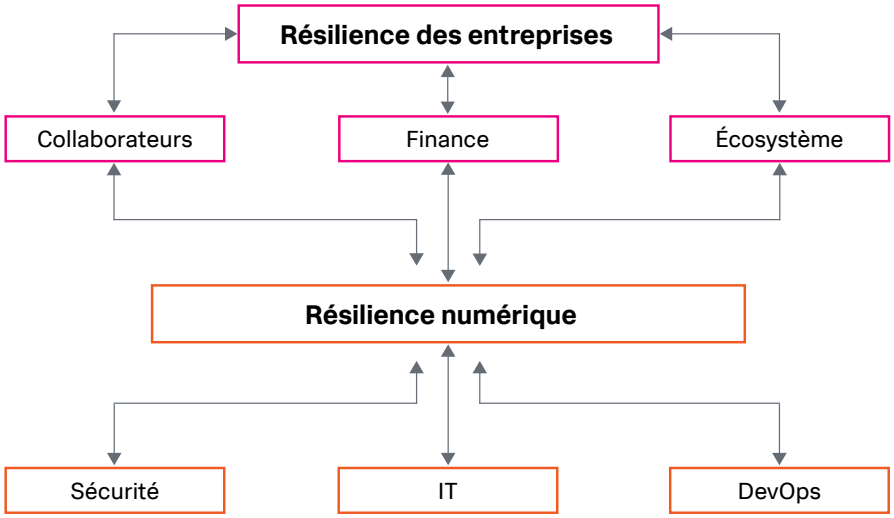
Les organisations résilientes sont capables de prévenir les incidents, de se rétablir, de survivre et de continuer à prospérer malgré les perturbations. Elles savent aussi s'adapter rapidement aux nouveaux modèles d'exploitation. Elles peuvent non seulement rebondir, mais aussi avancer au rythme des évolutions.

Les systèmes numériques sont la clé de la résilience des entreprises

En quelques années, le numérique est passé du rôle de soutien aux opérations à celui de moteur de croissance essentiel. Pour cette raison, les perturbations subies par les entreprises imposent aux systèmes numériques un stress qui a un impact bien supérieur sur l'ensemble de l'organisation.

Les décideurs doivent considérer de nombreux aspects pour bâtir la résilience de leur entreprise : ils doivent assurer sa santé financière, trouver et fidéliser les talents, et avoir des partenaires et fournisseurs fiables. Mais ce sont les ressources numériques qui sont à la base de tout. Les entreprises se tournent massivement vers le numérique, et leur résilience dépend de celle de leurs systèmes informatiques.

Un cadre pour la résilience des entreprises



La résilience des entreprises a plusieurs facettes. La **résilience numérique** unifie la sécurité, l'IT et le DevOps pour former la base de la résilience des entreprises.

L'implication de toutes les équipes technologiques – sécurité, IT et DevOps – est primordiale. Ces dernières années, les perturbations comme les interruptions de service et les failles de sécurité ont révélé qu'une approche traditionnelle en silos peut engendrer des risques au sein de différentes fonctions. Richard M Marshall, Fondateur de Concept Gap, explique : « Par le passé, les développeurs produisaient du code et l'envoyaient aux opérations pour qu'elles le fassent fonctionner, pendant que l'équipe de sécurité était assise de l'autre côté sans parler à personne ».

Les organisations visionnaires ont conscience que cette approche ne fonctionne pas. De nos jours, les entreprises efficaces élaborent une stratégie de résilience unifiée qui englobe des fonctions multiples afin de gérer et de surmonter les perturbations.

Les différents stades de maturité de la résilience

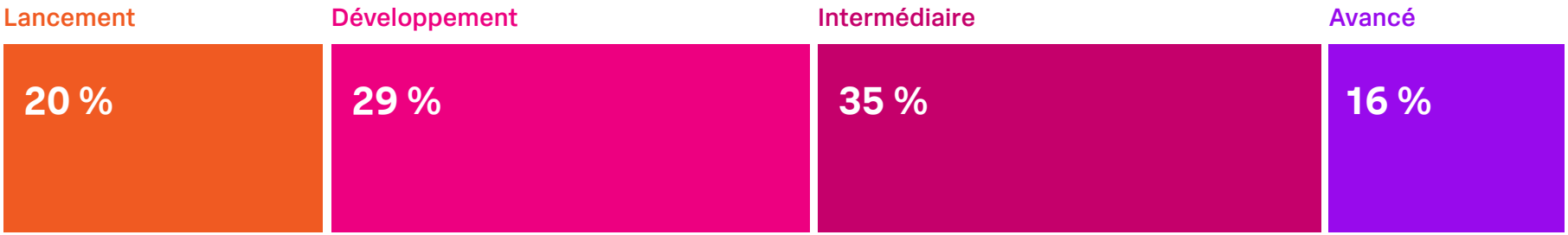
L'adoption d'une nouvelle approche impose aux responsables des technologies et de la sécurité de revoir les méthodes d'évaluation de leur posture de résilience. Ils doivent désormais pouvoir démontrer la valeur de leurs investissements dans la résilience et leurs progrès sur une courbe de maturité à leur comité de direction.

Sean Crabtree, Directeur exécutif d'Accenture, l'affirme : « Dans le futur, toutes les entreprises qui ne le sont pas encore deviendront des entreprises technologiques. [...] Il est absolument essentiel d'intégrer la résilience aux capacités de production de l'entreprise et aux équipes qui les mettent en œuvre ».

L'étude révèle des stades de maturité variés chez les organisations. Une organisation sur cinq n'en est qu'au début de son parcours et une sur six en est au stade Avancé. Cependant, la majorité se situe en milieu de peloton, avec des forces dans certains domaines et des faiblesses dans d'autres.

L'étude montre que les organisations au stade Avancé possèdent les capacités nécessaires pour réussir, en particulier en période de troubles [voir Méthodologie]. Par exemple, ces dernières ont une meilleure visibilité, qui couvre différentes sources de données IT, de sécurité et DevOps, ainsi qu'une capacité de réponse plus développée, permettant d'anticiper et d'éviter les incidents à l'aide du machine learning et de la correction automatique. En fin de compte, ces capacités produisent de meilleurs résultats commerciaux, y compris en termes de revenus et de chiffre d'affaires.

Les différents stades de maturité de la résilience



Conclusions clés

Investir dans la résilience porte ses fruits de quatre façons. Par rapport à leurs homologues, nous avons constaté que les organisations au stade Avancé parviennent mieux à :

- minimiser les coûts liés aux interruptions,
- se préparer au changement,
- gérer efficacement la transformation numérique,
- atteindre les objectifs de performance financière.

Minimiser les coûts liés aux interruptions

Toutes les entreprises subissent une quantité considérable d'interruptions de service

Les interruptions sont inévitables. Qu'elles proviennent d'une défaillance, d'une faille ou d'autres événements, les interruptions imprévues qui impactent négativement l'expérience client, le chiffre d'affaires ou la productivité, sont inéluctables pour la plupart des organisations. Les participants ont signalé en moyenne 240 heures d'interruptions de service chaque année, l'équivalent de dix jours. Ces conclusions étaient similaires pour chaque stade de maturité : Lancement, Développement, Intermédiaire et Avancé.

Les organisations devront faire face à des interruptions imprévues, quelle que soit leur maturité. Nous les avons interrogées sur les types d'événements ou de menaces les plus susceptibles de perturber leur organisation : un quart des participants a mentionné les interruptions d'infrastructure et un cinquième les ransomwares.

Les enjeux sont élevés. Chaque heure d'interruption coûte en moyenne 365 000 dollars, ce qui signifie qu'une organisation peut s'attendre à des coûts moyens de 87 millions de dollars par an de pertes de productivité et de chiffre d'affaires suite aux interruptions.

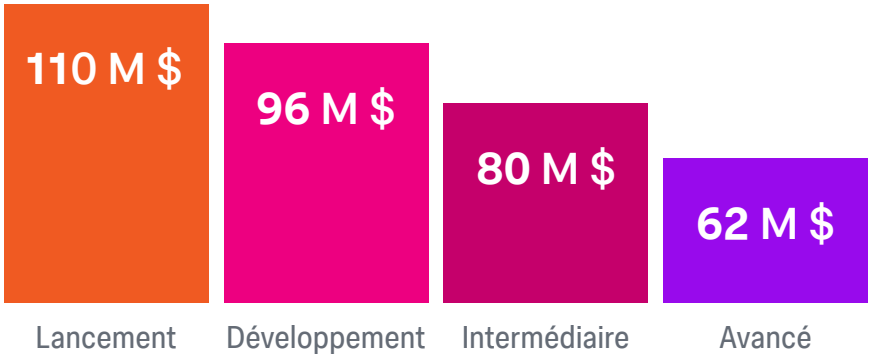
Une organisation s'expose à des coûts moyens de **87 millions de dollars** par an, dus aux pertes de productivité et de revenus suite aux interruptions.

Les organisations avancées minimisent l'impact des interruptions et économisent environ 48 millions de dollars par an

En réalité, la question n'est pas tant de savoir « si » des interruptions vont survenir, mais « quand ». Toutefois, les organisations qui investissent dans la résilience sont en mesure de réduire l'impact des perturbations et d'économiser des sommes importantes par rapport à leurs pairs. Notre étude démontre qu'en cas d'interruption, le groupe Avancé dépense considérablement moins annuellement (62 millions de dollars) que le groupe Lancement (110 millions de dollars).

Que peut-il bien se passer en coulisses ? Grâce à une meilleure visibilité et à de puissantes capacités d'investigation, les organisations au stade Avancé sont capables de hiérarchiser la réponse en fonction de l'impact de l'interruption sur l'organisation. Par exemple, elles se concentreront d'abord sur le rétablissement et le bon fonctionnement de leur application génératrice de revenus, et feront passer au second plan la remise en ligne d'un outil de collaboration utilisé par quelques équipes internes seulement.

Coûts liés aux interruptions imprévues, par an



Cette conclusion est en accord avec l'avis de Richard Marshall, selon qui les organisations apprennent à prévoir l'inattendu et à concentrer leurs efforts sur l'atténuation des conséquences :

« Vous apprenez à tomber sans vous blesser. La résilience consiste à savoir ce qui va, ou pourrait, mal se passer, puis à identifier ce que vous ne connaissez pas encore. »

Fait marquant : l'industrie des services financiers enregistre les coûts les plus élevés en cas d'interruption

Les interruptions ont de lourdes conséquences sur tous les secteurs d'activité. Par rapport au secteur public, aux télécommunications, à la technologie, à la santé, la vente au détail ou l'industrie manufacturière, les coûts liés aux interruptions pour une société de services financiers sont très supérieurs et atteignent en moyenne 141 millions de dollars par an. Cette conclusion est à rapprocher des taux élevés d'adoption de la banque numérique et du trading en ligne, qui expliquent l'ampleur des pertes en cas d'interruption de service.

Les pertes des organisations de services financiers liées aux interruptions s'élèvent à **141 millions de dollars** par an, soit **54 millions de dollars** de plus que la moyenne tous secteurs confondus.

Facteur clé :

la gestion des crises inter-fonctionnelle joue un rôle essentiel

Les interruptions font davantage de dégâts en temps de crise, comme l'ont démontré la faille Log4shell et la cyberattaque de Colonial Pipeline. Ces événements nécessitent que la gestion de crise soit coordonnée de manière inter-fonctionnelle par les équipes de sécurité, IT et DevOps. Nous avons constaté que c'est le cas dans la plupart des organisations (96 %) sur au moins certains de leurs produits et services.

Cependant, les organisations qui ne respectent pas ce principe (4 %) subissent plus de dégâts : les coûts liés aux interruptions imprévues s'élèvent à 211 millions de dollars par an. Les recherches indiquent que la gestion de crise est un point de départ stratégique pour implémenter les processus et les outils visant à améliorer la résilience.

Se préparer au changement

La plupart des organisations ne sont pas prêtes à s'adapter

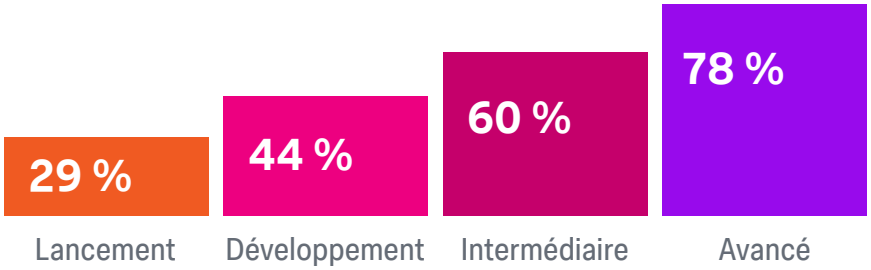
Outre les incidents qui mènent aux interruptions de service, des événements macro-économiques de plus grande ampleur continuent de menacer les organisations, qu'il s'agisse d'une récession économique ou d'une perturbation sectorielle. Celles qui ne sont pas capables de s'adapter vont mettre la clé sous la porte.

Seule la moitié des organisations se sentent préparées à changer leur façon d'opérer et à interagir avec leurs clients pendant les périodes de perturbation, que ce soit pour faire face aux exigences d'une récession (52 %) ou pour répondre à la concurrence (50 %).

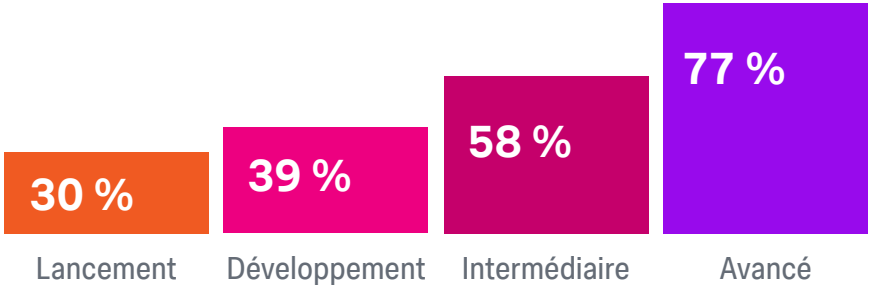
Les organisations avancées sont 2,5 fois plus susceptibles d'être préparées

Quand ces résultats sont répartis par niveau de maturité en matière de résilience, les conclusions sont édifiantes. Plus de trois quarts des organisations au stade Avancé déclarent être préparées à la fois à s'adapter aux exigences d'une récession (78 %) et aux bouleversements du marché (77 %), contre un tiers des organisations au stade Lancement (30 %) environ.

Organisations préparées à faire face aux exigences d'une récession



Organisations préparées à faire face aux bouleversements du marché



Mettre en place des capacités de résilience permet de bâtir des fondations de fiabilité et de sécurité et de consacrer plus de temps à l'innovation. En d'autres termes, les organisations au stade Avancé peuvent se concentrer sur le développement de nouvelles fonctionnalités, sur la recherche de nouveaux moyens de distribuer leurs produits et services ou sur l'expansion vers de nouveaux marchés pour tirer parti des opportunités.

Dans les périodes de changement, les gagnants sont ceux qui parviennent à s'adapter rapidement et à tirer profit de l'évolution des forces du marché. Prenons l'exemple de ManpowerGroup, une entreprise de solutions de recrutement avec un chiffre d'affaires de 19 milliards de dollars, 400 000 clients et 3,4 millions d'associés chaque année. Elle a su relever le défi de la pénurie des talents pendant la pandémie. Randy Herold, RSSI de l'entreprise, souligne l'impact des investissements dans la résilience qui ont, selon lui, permis à l'entreprise de garder une longueur d'avance. Il déclare : « La visibilité est absolument essentielle pour nos opérations quotidiennes. C'est important pour nos stratégies à long terme. C'est important pour notre innovation. »

Facteur clé :

l'automatisation permet aux organisations de rester efficaces

Les périodes de changement accentuent les vulnérabilités des organisations. Quand les ressources sont limitées, elles doivent être plus intelligentes et efficaces. L'automatisation entre alors en jeu.

Les organisations « lean » utilisent l'automatisation pour réduire les coûts et gagner du temps, mais aussi pour produire davantage avec moins de ressources. Le taux d'adoption de l'automatisation est plus élevé chez les organisations avancées que chez leurs pairs : 75 % rapportent qu'au moins la moitié de leurs workflows est automatisée, contre 39 % pour les organisations au stade Lancement. Plus précisément, le machine learning et la correction automatique aident ces organisations à prédire et éviter ces incidents. Les systèmes de réparation automatique exécutent automatiquement des tâches telles que le redémarrage d'application en cas de mémoire insuffisante, tandis que les procédures automatisées s'occupent d'isoler les hôtes infectés par un malware ou de suspendre les comptes suspectés d'activité malveillante. Les entreprises qui appliquent le machine learning et la correction automatique à tous leurs produits et services sont deux fois plus susceptibles (66 %) d'être prêtes à faire face à une récession que celles qui ne l'ont pas adopté (34 %).

Gérer efficacement la transformation numérique

Les organisations peinent à extraire de la valeur

La transformation numérique est au cœur de la stratégie des leaders de la technologie. Pour autant, faire les choses correctement n'a rien de facile. La plupart des participants (61 %) ont déclaré que moins de la moitié de leurs projets de transformation numérique avaient eu un impact positif et durable au cours des deux dernières années.

De la refactorisation du code à la révision de l'infrastructure, les projets à grande échelle engendrent des défis complexes. Par exemple, au sein des environnements cloud, la surface d'attaque à protéger est considérablement plus large et le nombre de services à superviser est bien plus conséquent.

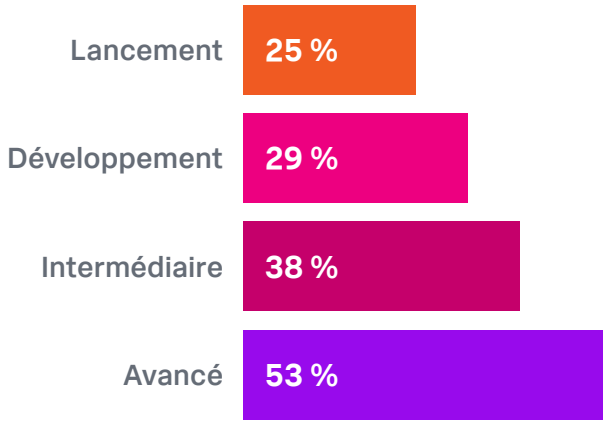
Les organisations avancées sont deux fois plus susceptibles de réussir

Les organisations au stade Avancé se démarquent de la concurrence en matière de transformation numérique. Ces dernières (53 %) ont été bien plus susceptibles de mettre en place des projets qui aboutissent dans la majorité des cas que les organisations au stade Lancement (25 %) au cours de ces deux dernières années.

Les organisations avancées possèdent des capacités qui leur offrent flexibilité et évolutivité. Par exemple, elles ont indiqué en moyenne que 64 % de leurs workloads s'exécutent dans le cloud.

Réussite des projets de transformation numérique

Entreprises ayant déclaré que la majorité de leurs projets de transformation numérique avaient eu un impact positif et durable au cours des deux dernières années.



Fait marquant : le secteur public et l'industrie des télécommunications sont à la traîne

Les organisations du secteur public (19 %) et de l'industrie des télécommunications (16 %) sont moins nombreuses à réussir leurs projets de transformation numérique. À cause du manque d'investissement, et parce qu'elles sont tributaires d'environnements technologiques tentaculaires et anciens, ces organisations éprouvent plus de difficultés à moderniser leurs services. Par conséquent, ces organisations aux ressources limitées sont souvent plus vulnérables aux menaces. D'après notre rapport sur les Prévisions 2023 pour le secteur public (en anglais), chaque incident lié aux ransomwares coûte en moyenne 2,7 millions de dollars aux écoles primaires et secondaires, contre 1,8 million de dollars dans le secteur privé.

Réussite des projets de transformation numérique par secteur

19 %
Secteur public

16 %
Télécommunications

35 %
Tous les autres secteurs

Facteur clé :

accélération du rythme de publication des versions, avec l'appui de la sécurité et de l'IT

Au moment de la publication d'une version, les équipes de sécurité et des opérations IT peuvent être perçues comme des obstacles. Et pourtant, la collaboration est essentielle pour faire aboutir les efforts de transformation numérique des organisations. Quand leurs équipes de sécurité et IT soutiennent les initiatives d'accélération du cycle de vie de tous les produits et services, les entreprises sont deux fois plus nombreuses (39 %) à réussir leur transformation numérique qu'à l'époque où ces initiatives n'existaient pas (21 %).

L'amélioration du rythme et de la qualité des versions alimente la transformation numérique. Cette observation souligne un point essentiel pour réussir : toutes les équipes technologiques d'une organisation doivent, sans attendre, se mettre à poursuivre ensemble les mêmes objectifs.

Atteindre les objectifs de performance financière

Les attentes sont de plus en plus élevées

Les organisations doivent investir dans la résilience pour réduire les interruptions de service, s'adapter aux changements macroéconomiques et réussir leur transformation numérique. Cependant, la performance financière présentée aux investisseurs doit aussi intégrer le retour sur investissement.

La volatilité récemment observée sur les marchés, combinée aux coupures budgétaires et à l'inflation, engendre une pression financière considérable. Satisfaire les attentes des investisseurs dans cet environnement n'est pas une mince affaire.

Les résultats financiers des organisations avancées surpassent celles de leurs homologues

Les organisations avancées ont été bien plus nombreuses que les autres à atteindre leurs objectifs de croissance au cours du dernier exercice fiscal : 17 points les séparent en effet des entreprises au stade Lancement.

Nous avons observé des résultats similaires concernant la croissance du cours des actions pour les entreprises cotées incluses dans l'étude. Les organisations au stade Avancé étaient plus nombreuses (82 %) à avoir enregistré une augmentation du cours de leurs actions depuis janvier 2020, que les organisations au stade Lancement (70 %).

Croissance du cours de l'action

Évolution du cours de l'action rapportée par des entreprises cotées en bourse sur la période du 1er janvier 2020 au 1er janvier 2022

82 %
des organisations avancées
indiquent une croissance

70 %
des organisations débutantes
indiquent une croissance

Ces conclusions suggèrent deux choses : non seulement les organisations avancées font le bon choix en investissant dans la résilience, mais elles en tirent également une valeur considérable. Comme les pressions économiques continuent à s'intensifier, nous conseillons aux leaders de la technologie et de la sécurité d'arrêter de voir la résilience comme un coût mais plutôt comme un investissement qui entraîne des retours positifs.

Bâtir les fondations de la résilience pour l'avenir

Cette étude met en évidence la rentabilité nette d'un investissement dans la résilience. Les 5 domaines stratégiques que sont la visibilité, la détection, l'investigation, la réponse et la collaboration produisent des résultats tangibles quand il s'agit de :

- minimiser les coûts liés aux interruptions,
- se préparer au changement,
- gérer efficacement la transformation numérique,
- atteindre les objectifs de performance financière.

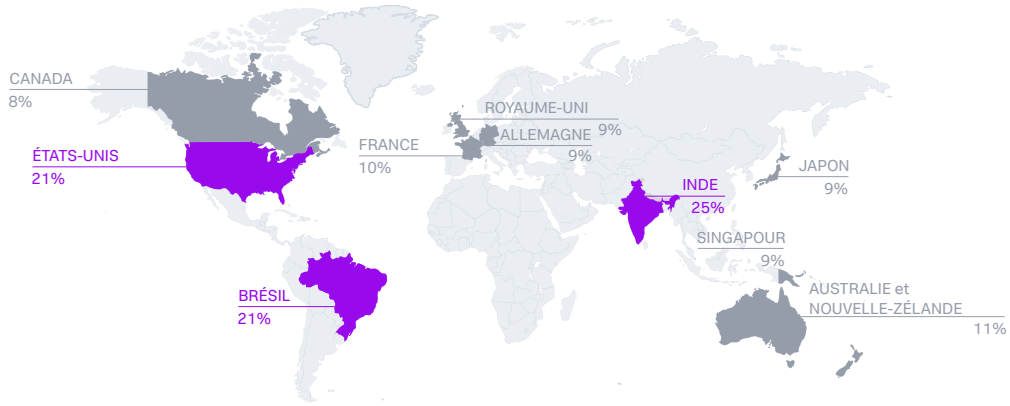
Étant donné le potentiel infini des perturbations, les responsables des technologies et de la sécurité doivent investir dans le renforcement de chacun de ces domaines pour améliorer la maturité de leur organisation. Les entreprises peuvent commencer par améliorer la gestion des crises de manière inter-fonctionnelle, adopter le machine learning et la correction automatique, et renforcer la sécurité et l'IT pour accélérer le rythme des publications. En mettant en place des bases solides de résilience, les dirigeants peuvent donner à leur entreprise les moyens de s'adapter à toutes les situations.

Annexe

Quels sont les pays les plus avancés ?

Parmi les onze pays inclus dans l'étude, l'Inde, le Brésil et les États-Unis affichent les pourcentages les plus élevés d'organisations avancées

- Organisations plus avancées
- Organisations moins avancées
- Non interrogé

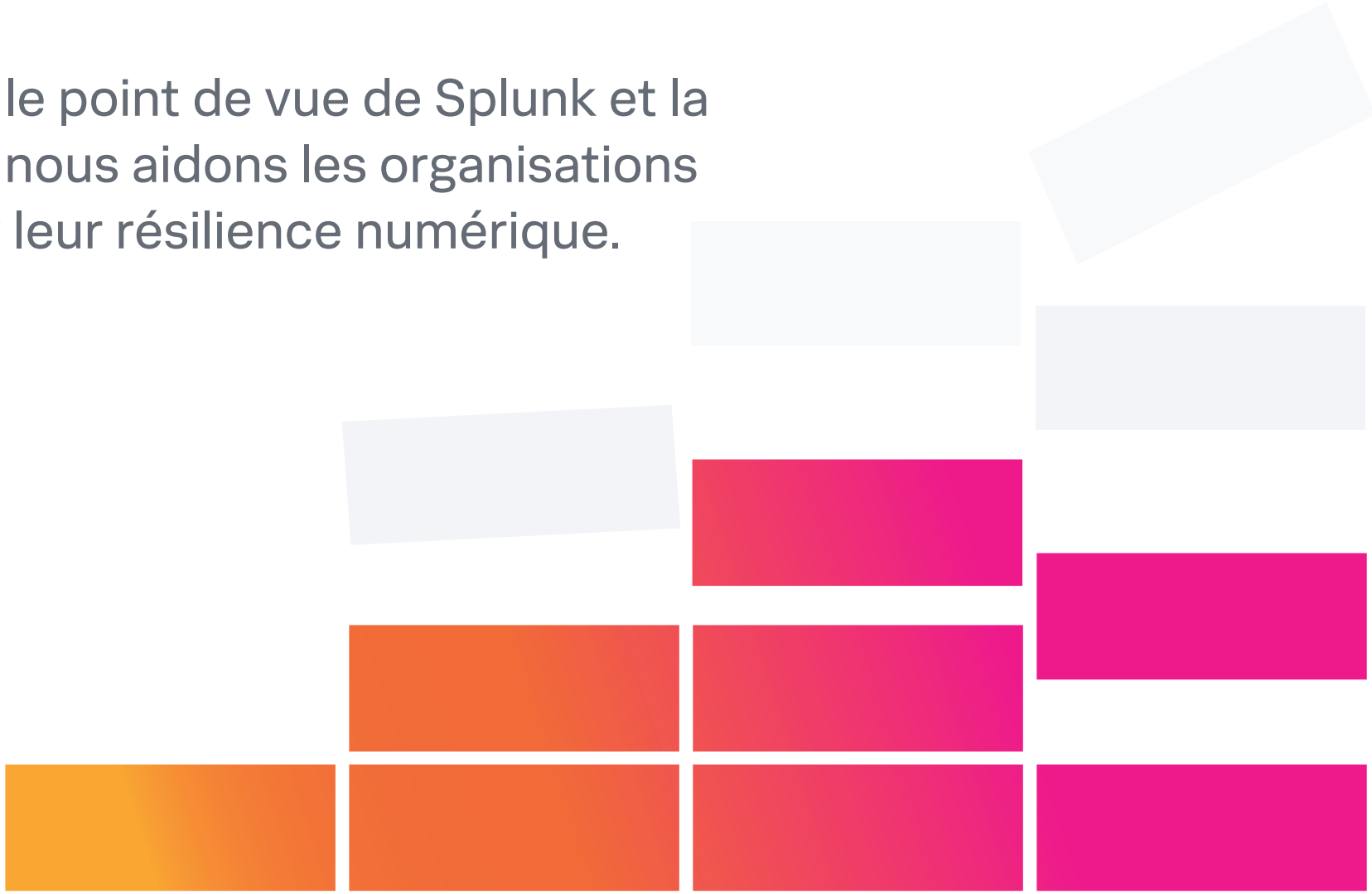


Quelles sont les industries les plus avancées ?

Parmi les industries incluses dans l'étude, les services financiers, la technologie et l'industrie manufacturière sont les plus représentées parmi les organisations avancées

22 %	20 %	18 %	15 %	9 %	7 %
Services financiers	Technologie	Fabrication	Commerce de détail	Santé	Télécommunications

Découvrez le point de vue de Splunk et la façon dont nous aidons les organisations à améliorer leur résilience numérique.



AW_23-26751-Splunk-Digital Resilience Pays Off-EB-SS-108

splunk>