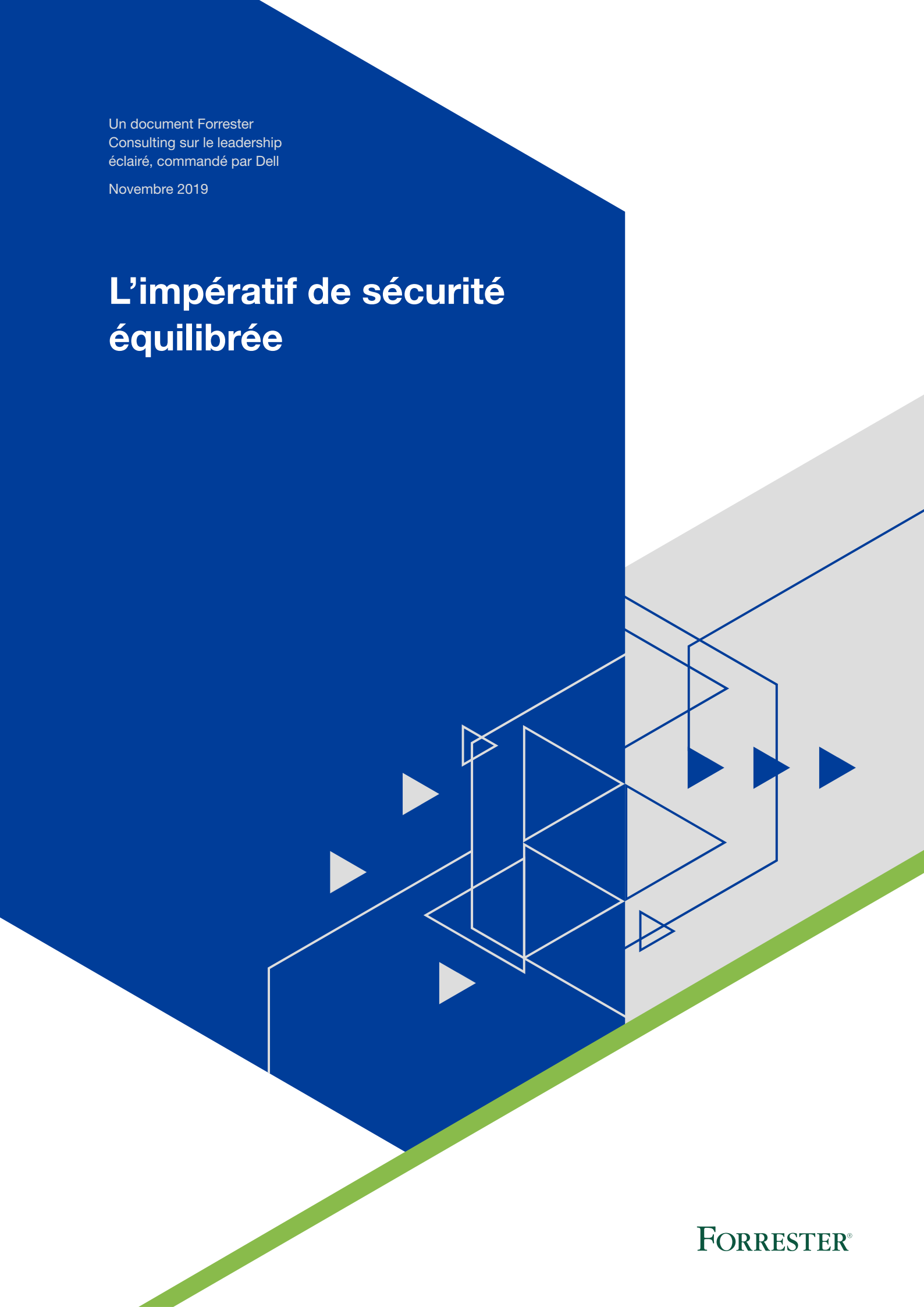
Un document Forrester Consulting sur le leadership éclairé, commandé par Dell

Novembre 2019

L'impératif de sécurité équilibrée



FORRESTER®

Table des matières

1 Synthèse

2 Les organisations ont besoin d'une sécurité équilibrée pour optimiser l'efficacité opérationnelle et l'expérience collaborateur

3 Les menaces en constante évolution et la complexité informatique sont des défis récurrents

6 Votre infrastructure de sécurité doit évoluer avec le temps

9 Une sécurité équilibrée profite aux collaborateurs et à l'activité

11 Principales recommandations

12 Annexe

Directeur du projet :
Tarun Avasthy,
Market Impact Consultant

Recherche connexe :
Groupe de recherche Forrester's Infrastructure & Operations

FORRESTER®

Synthèse

Pour trouver l'équilibre en matière de sécurité, les entreprises doivent envisager la confidentialité et la sécurité des données sous un nouvel angle, c'est-à-dire plus comme des exigences de conformité, mais comme des notions à défendre et servant à différencier la marque. Tout faux pas ou toute modification apportée à l'infrastructure informatique peut exacerber, et exacerbera, la complexité. C'est pourquoi il est primordial d'élaborer une stratégie de sécurité équilibrée. Une stratégie de sécurité équilibrée neutralise la complexité en s'adaptant au rythme des changements technologiques, ainsi qu'aux perturbations du secteur et à l'évolution de la conformité aux normes.

En mars 2019, Dell a demandé à Forrester Consulting de sonder l'évolution des tendances de sécurité et des technologies nécessaires pour protéger les collaborateurs et leur permettre de travailler. Notre étude a révélé que le fait de donner les moyens d'agir aux collaborateurs, tout en respectant les protocoles de sécurité, améliore leur productivité. Forrester a mené une enquête en ligne auprès de 887 décideurs informatiques et métier pour étudier ce sujet.

PRINCIPALES CONCLUSIONS

- **Les menaces en constante évolution obligent les entreprises de taille intermédiaire à se montrer plus proactives que réactives.** Alors que de nombreuses failles de sécurité et/ou cyberattaques font régulièrement l'objet des gros titres, il est important que les entreprises de taille intermédiaire adoptent une approche plus novatrice de la sécurité.
- **De plus, dépenser uniquement dans le domaine de la sécurité n'est pas la solution miracle.** Les entreprises de taille intermédiaire doivent se forger une culture qui donne les moyens de travailler aux collaborateurs, qui développe leurs compétences en continu, et plus important encore peut-être, une infrastructure de sécurité solide et saine.
- **Si les règles informatiques sont restrictives, les collaborateurs se soustrairont aux pratiques d'excellence en matière de sécurité informatique, pour pouvoir travailler.** Il n'est pas rare de déroger aux règles sur le lieu de travail, mais il est risqué de contourner purement et simplement celles qui touchent à l'informatique dans le but de travailler.

FORRESTER®

Les organisations ont besoin d'une sécurité équilibrée pour optimiser l'efficacité opérationnelle et l'expérience collaborateur

Un paysage technologique diversifié et l'évolution des modes de travail ont ouvert la voie à une multitude de risques qui menacent la sécurité globale des organisations et leur réputation. Une infrastructure de sécurité robuste et équilibrée garantit l'optimisation et la protection des performances de l'entreprise. Parallèlement, l'expérience collaborateur prend de plus en plus d'importance en tant qu'initiative professionnelle, car de plus en plus de sociétés souhaitent développer une stratégie d'expérience du personnel réduisant les frictions et permettant aux collaborateurs de réaliser leurs tâches les plus importantes de manière efficace.

Les dépenses consacrées aux technologies ne suffiront pas, à elles seules, à améliorer l'expérience collaborateur. Les organisations, en particulier les entreprises de taille intermédiaire, doivent également investir pour se forger une culture qui donne les moyens de travailler aux collaborateurs, qui développe leurs compétences en continu et qui renforce la sécurité afin de gérer les risques, tout en soutenant les performances de leur activité. Pour proposer une excellente expérience collaborateur, les entreprises doivent adopter une approche équilibrée de la sécurité dans trois domaines clés (voir figure 1) :

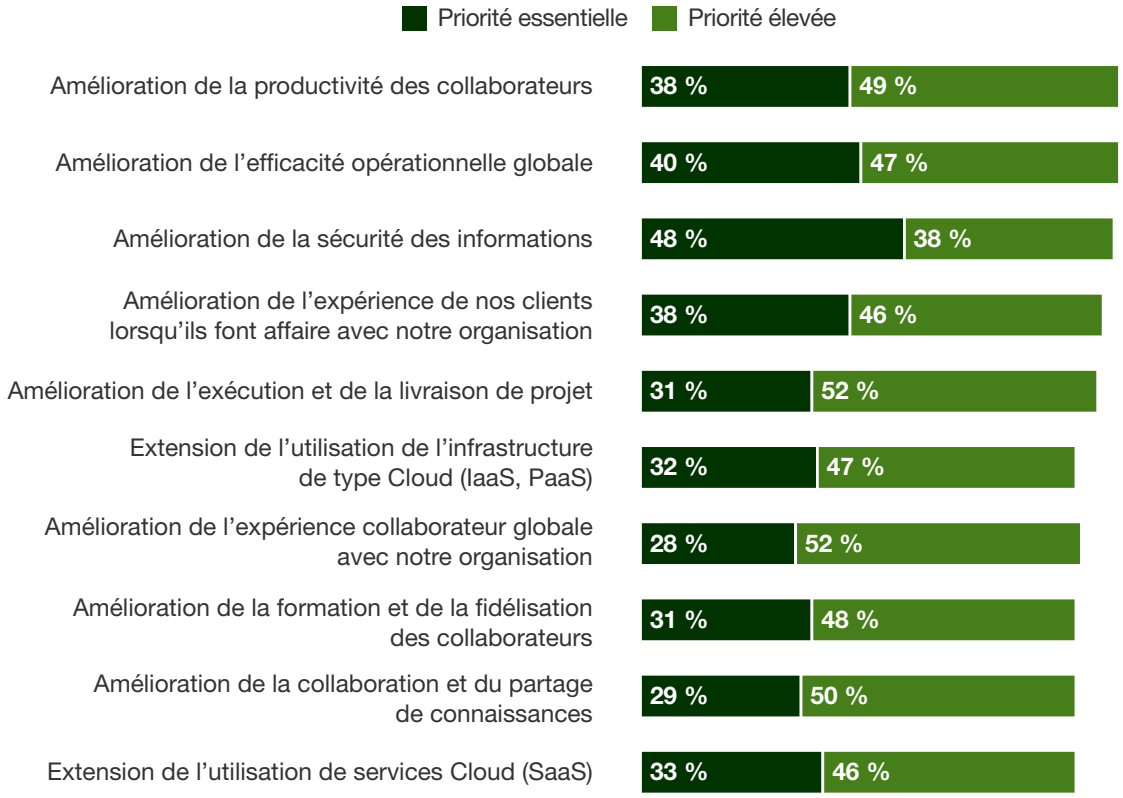
- **Augmentation de la productivité des collaborateurs.** Aujourd'hui, l'intensité de l'activité professionnelle soumet les collaborateurs à de fortes charges cognitives. Une bonne expérience collaborateur doit donc les aider à maîtriser leurs tâches. Cependant, de nombreuses mesures de sécurité font l'inverse et affectent leur productivité. Dans cette optique, les entreprises de taille intermédiaire cherchent à améliorer la productivité de leurs collaborateurs au cours des 12 prochains mois (88 %). À mesure que les technologies continueront d'évoluer, les personnes interrogées ont également indiqué qu'elles amélioreraient la fidélisation et la formation des collaborateurs (79 %), en veillant à ce que le manque de talents reste aussi minime que possible.
- **Optimisation de la sécurité des informations.** Pour réussir, les collaborateurs ont également besoin d'un accès illimité aux informations nécessaires pour accomplir leurs tâches, quel que soit le lieu d'où ils travaillent et les appareils qu'ils utilisent. Cependant, les entreprises sont confrontées à différents types de cyberattaques et d'événements qui peuvent perturber les opérations métier et compromettre les données sensibles, qu'il s'agisse d'informations personnelles de clients/collaborateurs ou d'informations professionnelles sensibles. En outre, les préoccupations liées aux risques tiers et à la sécurité de la chaîne d'approvisionnement signifient que les organisations doivent élargir leur vision des risques pour l'entreprise au-delà de leur propre environnement. Il n'est pas surprenant que 86 % des entreprises aient indiqué qu'elles privilégieraient la sécurité des informations à l'avenir.
- **Amélioration de l'efficacité opérationnelle.** Les équipes de sécurité qui soutiennent les opérations métier doivent mettre en place un processus bien plus cohérent dans leur façon de fonctionner et s'efforcer d'adopter une approche proactive de la sécurité, plutôt que réactive. Les entreprises de taille intermédiaire doivent voir au-delà de leurs efforts de sécurité standard visant principalement à respecter les exigences de conformité. Elles doivent adopter une approche plus stratégique de la sécurité, et davantage basée sur les risques. Il leur faudra donc des processus pour prendre en charge l'intelligence des risques, l'identification des menaces et la réaction face à ces dernières, l'évaluation des risques et la résilience de l'activité afin de tenir leurs promesses d'exécution et de livraison de projet (83 %).

Les entreprises de taille intermédiaire doivent investir pour se forger une culture qui donne les moyens de travailler aux collaborateurs, qui développe leurs compétences en continu et qui défend une infrastructure de sécurité robuste.

FORRESTER®

Figure 1

« Parmi les initiatives technologiques suivantes, lesquelles seront la priorité de votre département ou division au cours des 12 prochains mois? »



Base : 887 décideurs informatiques et métier impliqués dans la prise de décisions concernant les ordinateurs portables, les ordinateurs de bureau et d'autres appareils
Source : étude réalisée par Forrester Consulting au nom de Dell, septembre 2019

Les menaces en constante évolution et la complexité informatique sont des défis récurrents

Confrontés à des priorités contradictoires, à des technologies émergentes et à de nouvelles exigences réglementaires, les responsables de la sécurité sont chargés d'assurer la protection en continu et de déjouer les attaques. Cependant, lorsque nous avons demandé aux personnes interrogées quels étaient les principaux défis en matière de sécurité, voici ce qu'elles nous ont répondu (voir figure 2) :

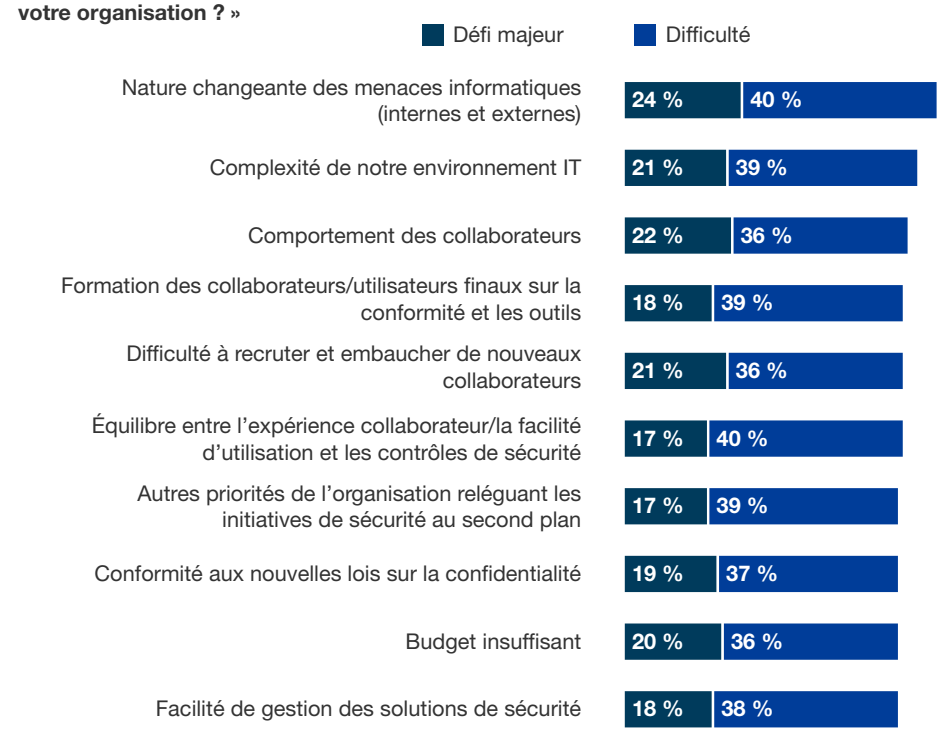
› **La nature évolutive des menaces oblige les entreprises de taille intermédiaire à rester vigilantes en permanence et à sans cesse rattraper leur retard.** Le département IT doit disposer d'une stratégie robuste et adaptable afin de poser des difficultés aux cybercriminels. Aujourd'hui, 65 % des organisations sont confrontées à des problèmes liés à la nature changeante des attaques de sécurité. Alors que vos dirigeants voient les dernières mentions de cyberattaques et d'incidents de sécurité dans les actualités, puis demandent si votre organisation pourrait être touchée, il peut s'avérer utile d'évaluer comment et pourquoi un tel événement pourrait se produire (ou pourquoi pas, selon votre environnement et vos contrôles), puis de les en informer. Cependant, ne laissez pas cette approche réactive guider votre stratégie de sécurité globale.

FORRESTER®

› **La complexité informatique se traduit par une augmentation des risques et des défis liés à la gestion informatique.** Tout faux pas ou toute modification apportée à l'infrastructure informatique peut exacerber, et exacerbera, la complexité. C'est pourquoi il est primordial d'élaborer une stratégie de sécurité robuste. Une stratégie de sécurité capable de s'adapter au rythme des changements technologiques, aux perturbations du secteur et à l'évolution de la conformité aux normes servira de catalyseur pour des changements positifs. Une stratégie de sécurité qui vous permet de prévenir plutôt que de guérir est préférable, tout comme une stratégie visant à consolider le nombre de produits de sécurité de votre environnement afin de faciliter la gestion informatique. Actuellement, 60 % des personnes interrogées considèrent la complexité de leur environnement informatique comme une menace pour leur organisation.

Figure 2

« Parmi les propositions suivantes, lesquelles représentent des défis de sécurité informatique pour votre organisation ? »



Base : 887 décideurs informatiques et métier impliqués dans la prise de décisions concernant les ordinateurs portables, les ordinateurs de bureau et d'autres appareils
Source : étude réalisée par Forrester Consulting au nom de Dell, septembre 2019

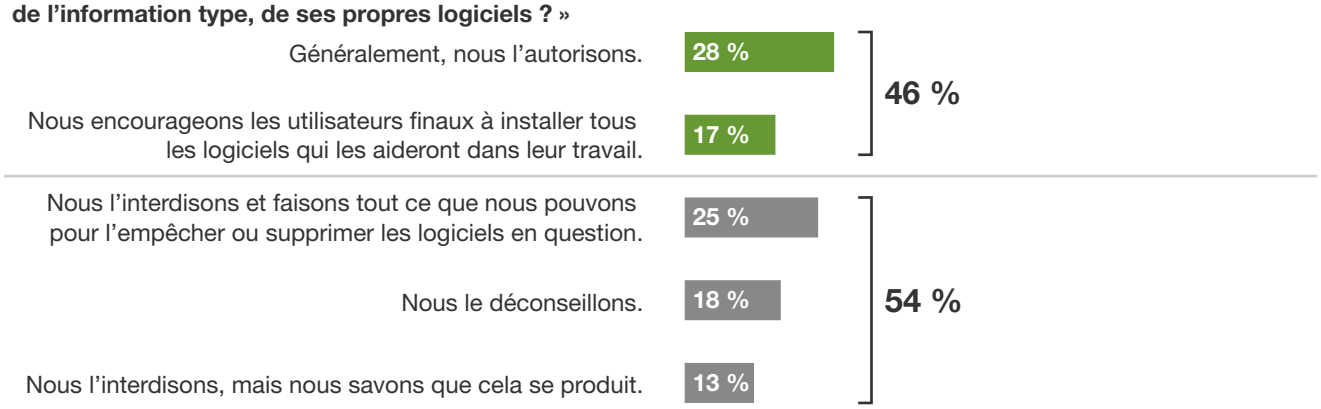
LES COLLABORATEURS ONT BESOIN DE POUVOIR TRAVAILLER SANS ENTRAVE, SINON ILS CONTOURNERONT LES RÈGLES INFORMATIQUES

Les collaborateurs choisiront l'option la plus simple pour réaliser leur travail. Si des collaborateurs souhaitent installer leurs propres logiciels/applications pour travailler plus facilement, 54 % des personnes interrogées dans les entreprises de taille intermédiaire ont déclaré qu'elles les en empêchaient, les décourageaient et leur interdisaient, mais qu'ils le faisaient quand même. Les collaborateurs ont besoin de se sentir soutenus par leur entreprise (voir figure 3).

Les collaborateurs doivent pouvoir travailler d'une manière qui n'entrave pas leur productivité, et le personnel de sécurité doit s'assurer que l'entreprise est protégée. 58 % des personnes interrogées ont signalé qu'il arrivera aux collaborateurs de contourner les règles informatiques pour réaliser leurs tâches, ce qui risque de nuire à l'entreprise. C'est pourquoi il est important de trouver l'équilibre entre l'expérience collaborateur/la facilité d'utilisation et les contrôles de sécurité, mais 57 % des personnes interrogées ont indiqué que cela restait difficile. En outre, si les organisations ne peuvent pas mesurer l'efficacité de leur programme de sécurité (52 %), elles auront l'impression de s'être lancées dans une course sans fin où la belle arche dorée de la ligne d'arrivée, représentant la stratégie de sécurité équilibrée, leur semblera hors d'atteinte.

Figure 3

« Quelle est la politique de votre département IT concernant l'utilisation/l'installation, par un travailleur de l'information type, de ses propres logiciels ? »



Base : 887 décideurs informatiques et métier impliqués dans la prise de décisions concernant les ordinateurs portables, les ordinateurs de bureau et d'autres appareils
Source : étude réalisée par Forrester Consulting au nom de Dell, septembre 2019

Votre infrastructure de sécurité doit évoluer avec le temps

L'idée d'un périmètre d'entreprise est dépassée aujourd'hui. Les collaborateurs travaillent depuis différents sites et ont besoin d'accéder aux informations où qu'ils se trouvent. Le marché du grand public influence la façon dont les collaborateurs travaillent dans un environnement d'entreprise et avec quels appareils. Une entreprise numérique n'a pas de périmètre. Aujourd'hui, votre organisation peut s'étendre dans le Cloud, prendre en charge des collaborateurs mobiles ou encore numériser des environnements physiques avec une connectivité via des capteurs et d'autres appareils connectés à Internet. Les possibilités que des collaborateurs exposent des données sensibles et que des pirates compromettent votre environnement et vos données augmentent de plus en plus. Dans l'environnement de travail et de menaces actuel, l'architecture et la stratégie de sécurité doivent évoluer pour se focaliser sur les données et s'enraciner dans une approche de sécurité Zero Trust (confiance zéro).

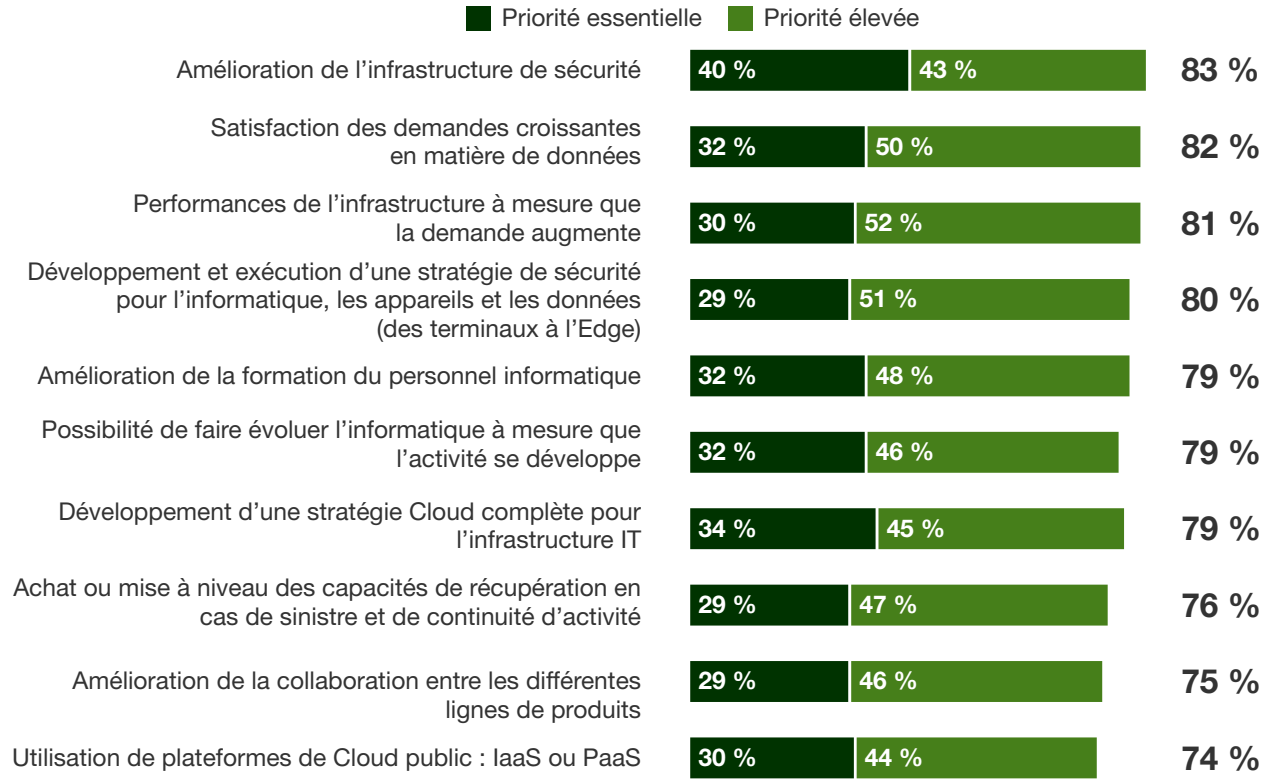
Zero Trust est un modèle conceptuel et architectural qui permet aux équipes de sécurité de repenser les réseaux en micro-périmètres sécurisés, d'utiliser l'obscurcissement pour renforcer la sécurité des données, de limiter les risques associés à des privilèges d'utilisateur excessifs et d'utiliser l'analytique et l'automatisation pour améliorer considérablement la détection et la réaction face aux menaces. Cette approche permet de renforcer sensiblement la sécurité des données. Aujourd'hui, de nombreuses organisations adoptent déjà une approche Zero Trust. Les personnes interrogées ont identifié les priorités d'infrastructure suivantes, indiquant qu'elles sont prêtes pour le modèle Zero Trust (voir figure 4) :

- **Formation des utilisateurs finaux afin d'améliorer les pratiques de gestion sécurisée des données.** Pour accéder à la propriété intellectuelle, les cybercriminels ciblent les collaborateurs et les sous-traitants. Au travail, les collaborateurs utilisent des appareils connectés qui interagissent avec des services Cloud sur des systèmes/réseaux appartenant à l'entreprise, mais lorsqu'ils sont ailleurs, que ce soit en déplacement, chez eux ou dans des espaces publics tels que des aéroports et des cafés, les collaborateurs ont toujours besoin d'accéder à des informations et données confidentielles, et le font à partir d'appareils personnels qui ne sont pas aussi bien protégés. Le fait que les collaborateurs doivent gérer les données de manière responsable, en suivant des pratiques sécurisées, etc., n'est pas forcément bien compris ni clairement communiqué.
- **Formation du personnel informatique pour limiter les risques.** Le développement continu des compétences du personnel informatique est essentiel pour s'assurer que les personnes responsables des infrastructures technologiques et de sécurité aient connaissance des pratiques d'excellence actuelles. Pour réussir, il faut que l'équipe informatique comprenne les changements liés aux options technologiques et l'évolution des risques et des menaces. Par conséquent, 79 % des personnes interrogées ont indiqué qu'elles amélioreraient la formation de leur personnel informatique. Cette bonne nouvelle présente deux avantages. Elle permettra : 1) de s'assurer que les compétences et les approches du personnel informatique restent pertinentes, et 2) d'aider à soutenir les efforts de fidélisation dans une période où la demande de talents est élevée.

› **Refonte de la stratégie de sécurité.** Les organisations prennent de plus en plus conscience que le respect des exigences de conformité n'est pas synonyme de sécurité robuste. Les partenaires commerciaux tiers demanderont des preuves d'une pratique de sécurité et de gestion des risques solide comme condition de collaboration. Une stratégie tournée vers l'avenir aide les organisations à mettre en œuvre un programme de sécurité robuste et à anticiper les domaines dans lesquels elles doivent procéder à des améliorations ou apporter de nouvelles compétences pour répondre aux préoccupations, en fonction des priorités métier. 80 % des personnes interrogées ont indiqué que leur priorité était de développer de d'exécuter une stratégie de sécurité pour l'informatique, les appareils et les données.

Figure 4

« Parmi les initiatives suivantes, lesquelles devraient figurer parmi les grandes priorités de votre organisation concernant l'infrastructure IT au cours des 12 prochains mois ? »



Base : 887 décideurs informatiques et métier impliqués dans la prise de décisions concernant les ordinateurs portables, les ordinateurs de bureau et d'autres appareils
Source : étude réalisée par Forrester Consulting au nom de Dell, septembre 2019

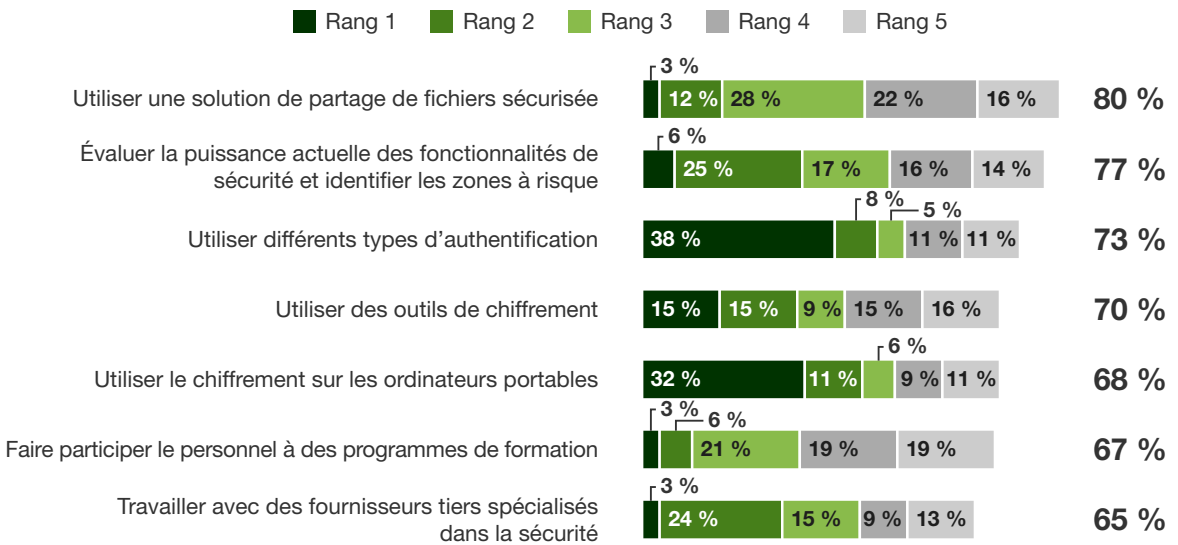
TACTIQUES D'AMÉLIORATION DE LA SÉCURITÉ

À l'ère du numérique, les cybermenaces sont partout et les failles de sécurité semblent faire les gros titres quotidiennement, ce qui coûte aux sociétés leur réputation, leur capital, et leur croissance et expansion à venir. En d'autres termes, la sécurité des résultats d'une organisation dépend des technologies qui protègent ses données, c'est-à-dire le bien le plus précieux de toute entreprise numérique. Les violations de données sont une réalité regrettable. 50 % des décideurs mondiaux en sécurité réseau ont déclaré que leur entreprise avait subi au moins une violation au cours de l'année écoulée, et ce pourcentage s'élevait à 55 % pour les personnes interrogées dans des entreprises de taille intermédiaire. Dans cette optique, les organisations ont révélé les éléments de sécurité qu'elles souhaiteraient améliorer (voir figure 5) :

- **Partage de fichiers, pour soutenir la collaboration entre les membres du personnel.** Les technologies et les membres du personnel jouent un rôle crucial pour permettre aux organisations de collaborer et de créer de la valeur économique à long terme. 80 % des personnes interrogées ont indiqué qu'elles utiliseraient une solution de partage de fichiers sécurisée pour renforcer la sécurité. Toutefois, celle-ci ne doit pas uniquement être utilisée entre les murs de l'entreprise, car les télétravailleurs et les professionnels qui se déplacent doivent également pouvoir accéder aux fichiers et les partager en cas de besoin.
- **Authentification, pour prendre en charge l'accès sécurisé aux données par les collaborateurs.** Dans leur forme la plus simple, les solutions d'authentification bloquent les méchants et acceptent les gentils. Alors que les violations de données sont si nombreuses dans le monde, l'application de contrôles revêt une grande importance. 73 % des personnes interrogées ont indiqué qu'elles utiliseraient différents types d'authentification, et 38 % ont classé l'authentification comme le 1er effort stratégique qu'elles feraient pour améliorer la sécurité. Cependant, ces processus ne doivent pas entraver la productivité des collaborateurs ni les empêcher de travailler. La fluidité de l'expérience d'authentification des utilisateurs fait une grande différence.
- **Chiffrement, pour contrôler les données et respecter les exigences de conformité.** 73 % des personnes interrogées ont indiqué qu'elles utiliseraient des outils de chiffrement, tandis que 68 % ont précisé qu'elles jugeaient le chiffrement des ordinateurs portables des collaborateurs (chiffrement complet du disque dur) important pour améliorer la sécurité. Dans un monde où il est facile pour un collaborateur de perdre un appareil ou de se le faire voler, c'est un choix prudent. Le chiffrement des données au repos peut également prendre plusieurs formes, et les organisations peuvent faire leur choix en fonction de leurs besoins, par exemple, disque complet, mode fichier, support, e-mail, niveau application/champ, chiffrement transparent/de base de données.
- **Évaluation de la sécurité, pour comprendre la maturité actuelle.** Bien que la plupart des équipes de sécurité aient mis en œuvre un large éventail de contrôles et de normes pour protéger leur entreprise, nombre d'entre elles ne parviennent pas à identifier objectivement leurs vulnérabilités. Par conséquent, elles ont du mal à déterminer si tous les problèmes clés sont traités ou si certains aspects des pratiques d'excellence restent sans réponse. 77 % des personnes interrogées en sont conscientes et cherchent à améliorer la sécurité en développant des plans de mesure corrective précis afin de s'assurer que tous les composants présentent l'état de fonctionnement souhaité.

Figure 5

« Qu'aimeriez-vous faire pour contribuer à améliorer la sécurité ? »



Base : 887 décideurs informatiques et métier impliqués dans la prise de décisions concernant les ordinateurs portables, les ordinateurs de bureau et d'autres appareils
Source : étude réalisée par Forrester Consulting au nom de Dell, septembre 2019

Une sécurité équilibrée profite aux collaborateurs et à l'activité

Une entreprise qui fournira des efforts en matière de sécurité sera mieux protégée, aura moins de problèmes en la matière et pourra donc plus facilement générer davantage de chiffre d'affaires. Pour libérer l'entreprise, les décideurs doivent adopter une approche de conception de l'expérience de sécurité centrée sur l'humain et basée sur les risques. Lorsque vous aurez trouvé l'équilibre entre une bonne expérience collaborateur et une sécurité renforcée, vous pourrez (voir figure 6) :

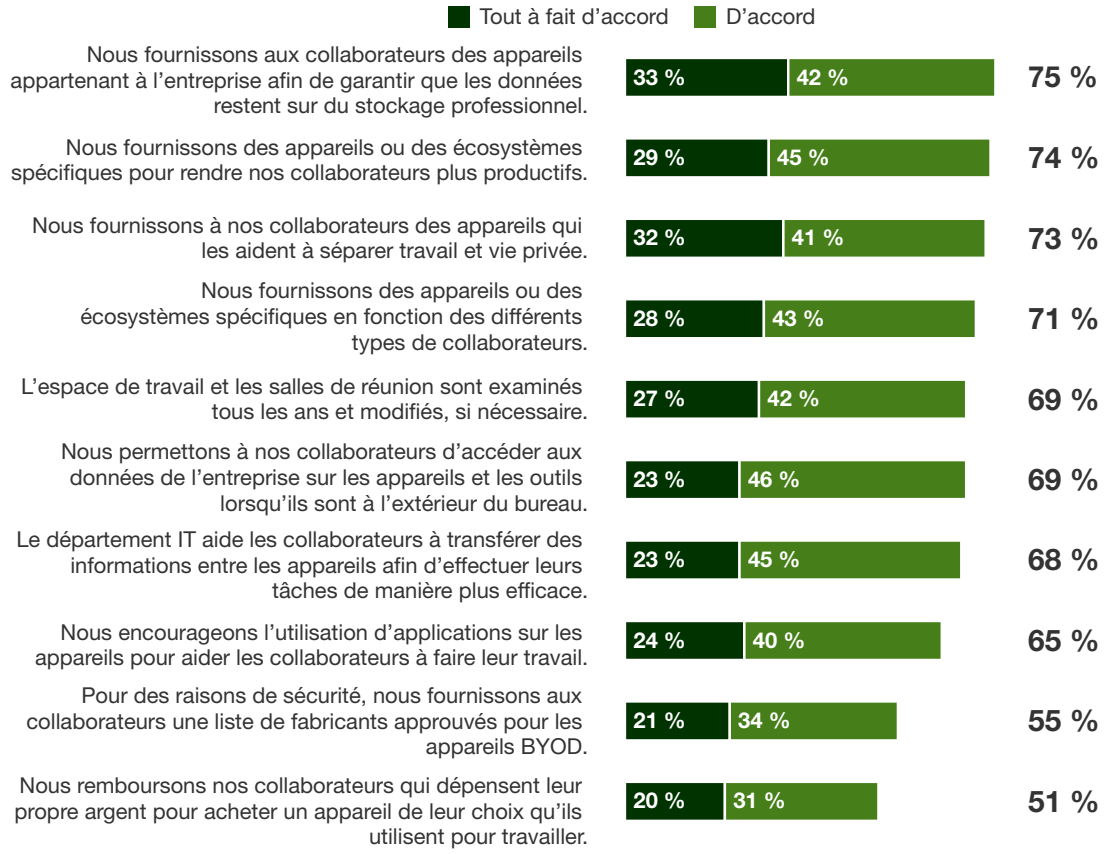
- **Autoriser le travail à distance pour soutenir la productivité et vous offrir un avantage concurrentiel.** Que les collaborateurs exigent une meilleure solution pour favoriser leur équilibre entre travail et vie privée ou que votre entreprise cherche la personne la plus qualifiée pour un poste, quelle que soit la distance qui la sépare du bureau, la prise en charge du télétravail est un avantage concurrentiel pour le recrutement et la fidélisation des talents. Les technologies aident à rendre le télétravail possible, et la sécurité est un élément essentiel à sa mise en œuvre. 69 % des personnes interrogées ont indiqué qu'elles permettaient l'accès aux données de l'entreprise sur des appareils lorsque les collaborateurs travaillaient en dehors du bureau.
- **Encourager la collaboration pour stimuler l'innovation.** Les collaborateurs souhaitent partager leurs expériences et, au final, ils souhaitent partager des fichiers et des idées avec leurs collègues. La connexion humaine et les outils permettant de la faciliter sont des conditions préalables à l'entretien d'un environnement ou d'une culture de l'innovation, notamment lorsque les collaborateurs sont dispersés, c'est-à-dire quand ils ne travaillent pas toujours face à face avec leurs pairs dans un bureau. Pour l'heure, 49 % des personnes interrogées déclarent qu'elles ont du mal à permettre aux collaborateurs de partager des données facilement et en toute sécurité. Des améliorations sont donc possibles pour en tirer des avantages.

FORRESTER®

› **Améliorer l'expérience client et réduire la rotation du personnel.** Lorsque vous proposez une meilleure expérience collaborateur, les membres du personnel sont plus heureux et vos clients aussi, car ils bénéficient d'un meilleur support et d'interactions plus satisfaisantes avec vos collaborateurs. Des collaborateurs heureux sont plus susceptibles de faire les bons choix, et des choix justes pour vos clients[1]. Une étude a montré que les organisations dont les collaborateurs sont épanouis ont constaté une satisfaction client supérieure de 81 % et une rotation du personnel moitié moindre[2].

Figure 6

« Qu'a fait votre entreprise pour permettre le télétravail ou le travail flexible ? »



Base : 887 décideurs informatiques et métier impliqués dans la prise de décisions concernant les ordinateurs portables, les ordinateurs de bureau et d'autres appareils
Source : étude réalisée par Forrester Consulting au nom de Dell, septembre 2019

Principales recommandations

Investir dans votre infrastructure de sécurité et dans des contrôles en la matière est un élément primordial de votre programme de sécurité. Cependant, les investissements technologiques à eux seuls sont insuffisants. Déterminez le niveau adéquat de sécurité équilibrée pour votre organisation, en fonction de vos besoins spécifiques et de votre tolérance aux risques.

Suivez quatre étapes, dès aujourd'hui, pour permettre à votre organisation de trouver le bon équilibre entre la sécurité et l'expérience collaborateur :

Évaluez votre maturité en matière de sécurité. Le processus d'évaluation lui-même peut également offrir une visibilité sur des procédures ou processus qui constituent des connaissances institutionnelles. Étant donné que certaines de ces procédures/certains de ces processus ne sont pas documentés, il sera important d'en découvrir les détails au cas où des membres clés de l'équipe ne partent à la retraite ou ne quittent l'organisation. Une évaluation fournira un aperçu des contrôles, des processus et des problèmes de sécurité existants, ce qui aidera à déterminer les domaines qui présentent des failles potentielles et doivent être traités. Cette évaluation vous servira de guide pour l'avenir et vous indiquera où concentrer votre attention et pourquoi.

Identifiez les données sensibles, les raisons de leur caractère sensible et leur emplacement. Cette étape consiste notamment à déterminer quelles données sont réglementées par des exigences de conformité et à définir la valeur des données pour l'organisation dans son ensemble. Parallèlement aux contrôles de sécurité et aux éléments appropriés à prendre en compte en matière de gestion des données, la compréhension de vos données constitue également une base pour prendre en charge la confidentialité et l'utilisation éthique des données personnelles. Une vision plus claire et une meilleure compréhension de vos données, vous permettent de mieux déterminer ce qui est nécessaire pour les protéger et les utiliser correctement.

Définissez le niveau de tolérance aux risques de votre organisation. Bien que les réglementations puissent dicter certaines actions et activités, les types et le niveau de contrôle que votre organisation choisit de mettre en œuvre dépendent de votre niveau de tolérance aux risques. Étudiez les risques auxquels vos données et votre organisation sont exposées, et prenez des décisions basées sur ces risques concernant les contrôles de sécurité afin de trouver l'équilibre entre les besoins des collaborateurs et la productivité.

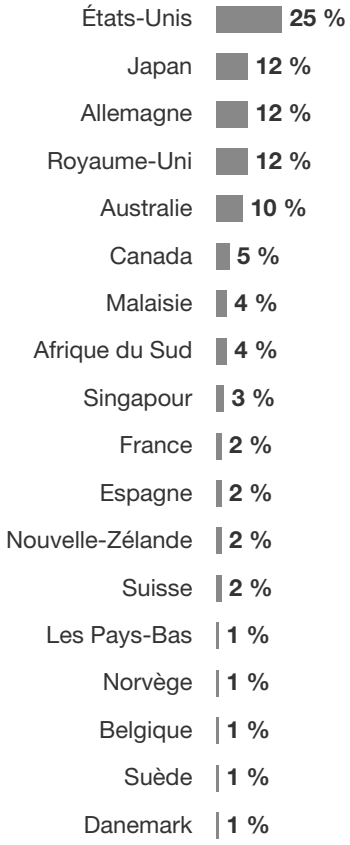
Évaluez les modes de travail de vos collaborateurs. Identifiez les contrôles de sécurité qui affectent l'expérience de travail des collaborateurs et le niveau d'incidence qu'ils peuvent avoir sur leur journée et leur productivité. Selon les différents profils de collaborateurs, qu'il s'agisse de leur rôle ou des données auxquelles ils ont accès pour accomplir leur travail, les besoins technologiques, les risques auxquels ils sont susceptibles d'être confrontés et les types de contrôles de sécurité que vous devrez mettre en œuvre pour limiter ces risques varieront. Implémentez les contrôles de sécurité nécessaires pour ne pas créer de frictions inutiles.

Annexe A : Méthodologie

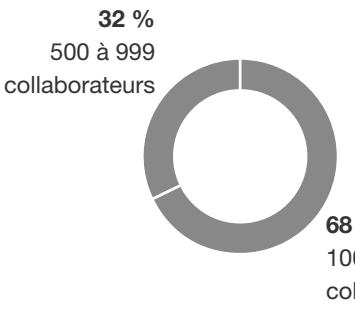
Pour cette étude, Forrester a mené une enquête en ligne auprès de 887 responsables informatiques et métier de différents secteurs d'activité du marché. Les questions fournies aux participants portaient sur l'évolution de leurs dépenses en matière de sécurité, les éléments qui influencent leur stratégie de sécurité, leurs défis en matière de conformité et de réglementation, ainsi que sur la manière dont ils envisagent l'avenir de la sécurité de leur organisation. L'étude a débuté en mars 2019 et la rédaction du présent document a été achevée en août 2019.

Annexe B : Données démographiques

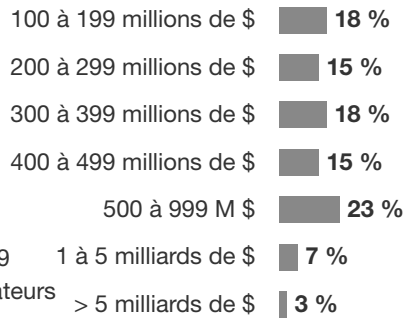
« Dans quel pays se trouve votre entreprise ? »



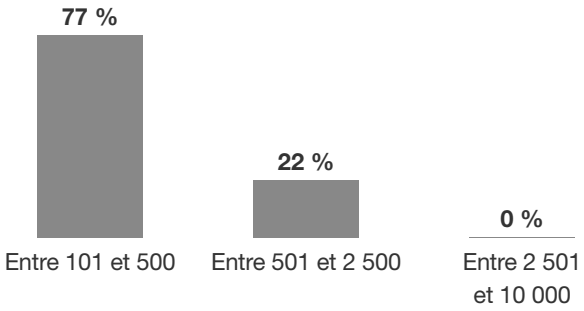
« D'après votre estimation, combien d'employés travaillent pour votre entreprise/organisation dans le monde ? »



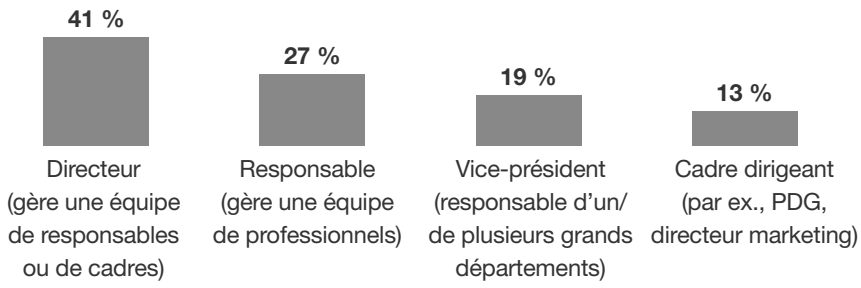
« Quel est le chiffre d'affaires annuel approximatif de votre organisation (USD) ? » (N = 861)



« Pour les décisions d'achat de technologies et de services que vous influencez le plus, combien de collaborateurs de votre organisation sont directement concernés ? »



« Quel titre décrit le mieux votre position au sein de votre organisation ? »



Base : 887 décideurs informatiques et métier impliqués dans la prise de décisions concernant les ordinateurs portables, les ordinateurs de bureau et d'autres appareils
Source : étude réalisée par Forrester Consulting au nom de Dell, mars 2019

FORRESTER®

Annexe C

NOTES DE FIN

[1] Source : « Transform The Employee Experience To Drive Business Performance », Forrester Research, Inc., 12 février 2018.

[2] Source : James K. Harter, Frank L. Schmidt et Theodore L. Hayes, « Business-Unit-Level Relationship Between Employee Satisfaction, Employee Engagement, and Business Outcomes: A Meta-Analysis », Journal of Applied Psychology, avril 2002 (http://www.factorhappiness.at/downloads/quellen/s17_harter.pdf).