Note de l´Analyste IDC

Parrainé par : **LastPass by LogMeIn**

Auteur :

Mark Child

Janvier 2020

Les contrôles des identités intégrés au sein de l'entreprise offrent sécurité et avantages commerciaux

Questions posées par : LastPass by LogMeIn

Réponses de : Mark Child, Responsable de la recherche, Sécurité européenne, IDC

Q. À l'ère numérique, l'identité est devenue un défi et une opportunité pour de nombreuses entreprises. Le périmètre sécurisé traditionnel est en train de disparaître et l'identité fournit un moyen de créer un nouveau périmètre flexible sécurisé. D'après IDC, quelles solutions fondamentales constituent une solution globale dans le domaine de l'IDT (Identity and Digital Trust) ? Quels outils les entreprises doivent-elles déployer pour assurer une sécurité IDT efficace ?

R.

L'IDT (notion précédemment appelée « gestion des identités et des accès » selon la taxonomie IDC) regroupe un ensemble de solutions permettant d'identifier les utilisateurs (employés, clients, intérimaires, etc.) et de contrôler leur accès aux ressources informatiques en associant des droits et des restrictions à un identifiant et à des comptes utilisateurs. Au premier semestre 2019, les entreprises européennes ont investi 932 millions de dollars dans les solutions IDT. Les principales sous-catégories du marché de l'IDT sont les suites de gestion des identités et l'identification unique (SSO, Single Sign-On), l'authentification avancée, la gestion des identités B2C et la gestion des comptes à privilèges (PAM, privileged account management).

La suite de gestion des identités devrait idéalement régir l'ensemble du cycle de vie de l'identité d'un utilisateur, de la création à la gestion continue en passant par la mise hors service. Ce dernier point est très important, car il arrive très souvent que des cybercriminels compromettent des systèmes en utilisant des identifiants censés être obsolètes.

L'identification unique, la gestion des mots de passe d'entreprise (EPM, enterprise password management) et l'authentification avancée, en particulier l'authentification multifactorielle (MFA, multifactor authentication), sont actuellement très demandées dans tous les secteurs, car les entreprises consolident leur infrastructure et leurs systèmes tout en s'efforçant de fournir aux utilisateurs un accès fluide et efficace, ainsi qu'une sécurité renforcée.

Ensemble, les suites de gestion des identités et l'identification unique représentent un peu plus de la moitié des investissements européens dans l'IDT. Les solutions

d'authentification représentent un tiers supplémentaire. Les investissements restants concernent la gestion des identités B2C et la gestion des comptes à privilèges. La demande de solutions de gestion des comptes à privilèges est motivée par des inquiétudes concernant les menaces internes et la fuite d'informations confidentielles. Les entreprises cherchent à renforcer la sécurité et le contrôle des « superutilisateurs », ainsi que de toute personne ayant accès à des données sensibles ou à forte valeur ajoutée.

Enfin, il convient d'examiner sérieusement quelle solution d'identité est déployée et comment. Comme nous l'avons indiqué précédemment, la gestion des identités nécessite un ensemble complexe de solutions afin de pouvoir répondre à toutes les exigences. Ces solutions doivent être intégrées, interopérables, correctement configurées et à jour. Le déploiement de produits hétérogènes provenant de différents fournisseurs risque d'entraîner des problèmes d'intégration, voire même des angles morts dans la couverture. Une suite d'identité intégrée provenant d'un même fournisseur, ou une plate-forme d'identité qui ajoute des composants intégrés provenant de partenaires d'alliance bien établis, permet de considérablement réduire ce risque. En outre, les entreprises devraient envisager d'utiliser une solution IDaaS (Identity as a Service) basée sur le Cloud, car celles-ci permettent de relever de nombreux défis opérationnels liés à la gestion de la plate-forme d'identité et peuvent même améliorer le niveau global de protection de l'entreprise. Une solution IDaaS nécessite moins de ressources internes (en termes d'effectifs et de compétences requises) et libère ainsi l'équipe de sécurité qui peut alors se concentrer sur d'autres tâches. Cette approche s'appuie sur l'expérience et l'expertise d'un fournisseur d'identité dédié, et peut permettre de réaliser des économies considérables, ce qui représente un avantage supplémentaire pour l'entreprise. D'après les données d'IDC, au cours du premier semestre 2019, le marché européen des solutions d'identité basées sur le Cloud a augmenté de 18 %, tandis que le chiffre d'affaires des solutions sur site est resté stable par rapport à l'année précédente.

Les solutions IDaaS permettent de relever de nombreux défis opérationnels liés à la gestion d'une plate-forme d'identité, nécessitent moins de ressources internes et peuvent améliorer le niveau général de protection de l'entreprise.

Q. Bien que l'entreprise doive faire face aux besoins d'identité à l'échelle numérique, les mots de passe restent un composant essentiel des approches IDT. Néanmoins, les mots de passe sont également une source de frustration pour les utilisateurs et de vulnérabilité pour les entreprises. Certains prétendent que l'explosion numérique a rendu le système des mots de passe intenable. Considérez-vous que c'est le cas ? Si oui, les mots de passe sont-ils voués à disparaître ?

R.

Les mots de passe sont un composant essentiel de nombreuses solutions d'authentification multifactorielle qui combinent « quelque chose que vous possédez » (par exemple, un jeton ou un smartphone) et « quelque chose que vous êtes » (généralement une caractéristique biométrique telle qu'une empreinte digitale) avec « quelque chose que vous connaissez » : le mot de passe. Cependant, même dans un contexte d'authentification multifactorielle, les mots de passe

restent un problème majeur : l'utilisateur type doit aujourd'hui se souvenir d'environ 90 à 200 identifiants et mots de passe (voir LastPass — L'exposé sur les mots de passe), chaque site Web ou application ayant ses propres exigences en termes de robustesse, de longueur, de complexité et de caractères du mot de passe. Les recommandations concernant les mots de passe varient également, certains experts recommandent d'utiliser des phrases de passe et d'autres des mots de passe longs, complexes, alphanumériques et truffés de caractères spéciaux. Il en résulte une attitude ambivalente vis-à-vis de la sécurité des mots de passe, ainsi que des mauvaises pratiques généralisées : mots de passe faibles, mots de passe réutilisés, partage de mots de passe, mots de passe communs pour des utilisations personnelles et professionnelles, et bien sûr des mots de passe griffonnés sur des post-its et collés sur l'écran d'ordinateur. Ces pratiques sont particulièrement préoccupantes compte tenu de la large gamme d'outils dont les pirates informatiques disposent et qui peuvent leur permettre de trouver des mots de passe faibles en quelques minutes ; sans parler des dangers supplémentaires de l'ingénierie sociale et du vol de mot de passe.

La technologie permet de relever ces défis : l'identification unique permet aux entreprises de réduire le nombre de mots de passe utilisés par les employés en couvrant un ensemble approuvé d'applications via une connexion unique. Néanmoins, l'identification unique n'est pas une solution complète. Les employés sont toujours susceptibles d'utiliser un ensemble d'applications plus large que celui couvert par l'identification unique et la réutilisation des informations d'identification unique pour un autre site ou service constitue un risque majeur. En cas de piratage de ce site, le mot de passe d'identification unique se retrouve alors entre les mains des pirates informatiques. Les coffres-forts à mots de passe, également appelés gestionnaires de mots de passe d'entreprise (EPMs, enterprise password managers), constituent un excellent outil complémentaire. Ils permettent aux utilisateurs de stocker en toute sécurité un nombre illimité de mots de passe forts et générés de manière aléatoire, et de les saisir instantanément et en toute sécurité lorsqu'ils y sont invités. Les gestionnaires de mots de passe d'entreprise peuvent également offrir des fonctionnalités supplémentaires qui profitent considérablement à l'entreprise, telles que la vérification des informations d'identification du site visité, l'application de politiques de réinitialisation des mots de passe, la fourniture d'un accès fédéré, la journalisation et les sessions d'audit, ainsi que la fourniture de rapports de conformité.

Certains fournisseurs estiment que la biométrie est la réponse aux problèmes de mot de passe et d'authentification. Toute entreprise qui envisage d'adopter l'authentification biométrique doit évaluer avec soin chaque cas d'utilisation, les données biométriques requises, si ces données seront stockées et la manière dont elles seront protégées. La commodité et la sophistication des méthodes d'authentification biométrique modernes et avancées peuvent fournir une réponse efficace à certaines exigences de l'entreprise. Elles offrent ainsi aux employés un moyen d'authentification simple, qui facilite l'utilisation tout en respectant les exigences de sécurité et améliore l'expérience utilisateur globale.

Certaines entreprises œuvrent pour un avenir sans mot de passe à l'aide d'organismes tels que FIDO Alliance, qui souhaite développer des normes d'authentification ouvertes pour renforcer l'authentification tout en limitant la

La gestion des utilisateurs, des identités et des accès est une priorité absolue en matière de sécurité pour la plupart des entreprises européennes, quel que soit le pays, le secteur ou la taille de l'entreprise.

complexité d'utilisation. C'est le compromis idéal que les entreprises cherchent à atteindre. Tant que l'activité en entreprise se déroule sans heurts, les considérations concernant l'expérience utilisateur sont susceptibles de prévaloir car elles sont alignées sur la productivité et sont donc intéressantes aux yeux du conseil d'administration. Quant aux mots de passe eux-mêmes, même si les fournisseurs de solutions progressent vers un avenir moins dépendant des mots de passe, il est peu probable qu'ils disparaissent de sitôt.

Q. Retrouve-t-on le besoin d'une suite d'identité intégrée partout et dans toutes les entreprises ? Les PME sont-elles moins « dans la ligne de mire » que les grandes entreprises ? Qu'en est-il des différents secteurs ? S'agit-il principalement des secteurs bancaires et financiers, ou sommes nous tous concernés ? Enfin, qu'en est-il des différentes régions du monde ? L'Europe, par exemple, utilise désormais le RGPD. Est-ce que cela la distingue ?

R.

Selon l'*enquête paneuropéenne de sécurité 2019* d'IDC (couvrant 700 responsables, cadres, décideurs et influenceurs en matière de sécurité dans 16 pays), « la gestion des utilisateurs, des identités et des accès » est la deuxième préoccupation en matière de sécurité informatique, juste derrière la « culture de la sécurité et la sensibilisation » (un domaine étroitement lié à l'IDT en matière d'hygiène de sécurité et de bonnes pratiques). Elle arrive également en deuxième position dans la sous-région qui rassemble les pays d'Europe centrale et orientale (PECO) et en quatrième position en Europe de l'Ouest (juste derrière la conformité, un autre domaine étroitement lié si l'on considère l'accès aux données confidentielles). Par pays, elle arrive en deuxième position au Royaume-Uni, en République tchèque, en Pologne et en Russie, et fait partie des cinq principales préoccupations en Belgique, en Allemagne et en Italie. Certains marchés tels que le Benelux et les pays nordiques classent l'identité en dehors des cinq principales préoccupations, mais il est probable que ces pays aient une longueur d'avance, ayant investi massivement au cours des dix dernières années dans des infrastructures et des solutions pour l'administration en ligne et d'autres initiatives. Par exemple, la présence de longue date de fortes initiatives d'identité électronique et d'identité gouvernementale dans ces pays, comme le concept danois NemID pour les services bancaires et gouvernementaux en ligne, aide à intégrer l'idée que l'identité est un principe central pour la sécurité comme pour la convivialité.

En termes de secteurs, l'identité n'est que la cinquième préoccupation dans la banque et la finance (où une grande partie du travail est déjà achevé). Elle est néanmoins la première préoccupation dans les télécommunications et dans l'éducation, et fait partie des cinq principales préoccupations dans presque tous les autres secteurs. Il s'agit de la première préoccupation pour les petites entreprises (entre 100 et 499 employés), de la deuxième pour les entreprises moyennes (entre 500 et 999) et de l'une des cinq principales préoccupations pour la plupart des grandes entreprises (2 500 employés ou plus). Pour conclure, l'identité et l'accès sont une priorité pour toutes les entreprises européennes, quel que soit leur pays, leur secteur et leur taille.

En ce qui concerne les dépenses dans l'IDT par pays, sans surprise, le Royaume-Uni (22,6 %), l'Allemagne (21,5 %) et la France (14,7 %) sont les trois plus grands marchés européens. L'Allemagne et la France sont également deux des marchés à la croissance la plus rapide pour les investissements dans l'IDT, avec des taux de croissance annuels moyens (TCAM) sur cinq ans de respectivement 7,6 % et 8,7 %. De nombreux autres marchés européens affichent cependant des prévisions de croissance comparables pour les dépenses dans l'IDT, notamment la Belgique, la République tchèque, les Pays-Bas, la Russie et l'Espagne. En termes de technologies, la gestion des identités B2C, l'authentification avancée, les suites de gestion des identités et l'identification unique stimuleront la croissance en Europe de l'Ouest. Les tendances sont similaires dans les PECO, mais cette région connaîtra également une forte augmentation des investissements dans la gestion des comptes à privilèges au cours des cinq prochaines années.

La conformité réglementaire est un important moteur commercial dans l'adoption de solutions IDT, en particulier dans les secteurs réglementés. Dans le cadre de la norme de sécurité de l'industrie des cartes de paiement (PCI DSS, Payment Card Industry Data Security Standard), qui régit les services financiers et le secteur de la vente au détail, les entreprises peuvent être pénalisées si elles échouent à mettre en œuvre des contrôles d'accès qui limitent l'accès des employés aux données sensibles. La seconde directive sur les services de paiement (PSD2, Second Payments Services Directive) de l'UE ajoute une couche de sécurité aux règles déjà complexes concernant l'utilisation des données clients par les banques européennes. Lorsque des fournisseurs tiers ont accès à des API financières, d'importants contrôles d'authentification sont essentiels pour protéger les clients contre la fraude. Le RGPD de l'UE, qui prévoit de lourdes sanctions financières en cas de non-conformité, a stimulé la croissance du marché européen de l'IDT en 2017 et 2018, car les entreprises, grandes comme petites, doivent désormais veiller à ce que la sécurité soit au cœur de leur stratégie de données. Ces entreprises doivent également prouver qu'elles peuvent contrôler et protéger l'accès aux systèmes qui contiennent des données personnelles. Avec d'importantes sanctions financières similaires à celles du RGPD, la directive européenne sur la sécurité des réseaux et des systèmes d'informations (NIS, EU Security of Networks & Information Systems Directive) renforce également l'importance de prendre les mesures appropriées pour sécuriser l'infrastructure des entreprises, y compris les contrôles d'accès et d'identité aux systèmes et fonctions fournissant des services essentiels, tels que l'énergie et les services publics.

Q. Les exigences sont là, les solutions également, et les tendances du marché sont généralement positives. Cependant, toutes les entreprises ne prennent pas d'initiatives en matière d'identité. Comme nous le savons tous, convaincre le RSSI ou le directeur de la sécurité est une chose, mais persuader le conseil d'administration d'approuver un investissement en est une autre. Quels sont les avantages commerciaux potentiels d'un déploiement ou d'une mise à niveau IDT, ou à quels cas d'utilisation pourraient-ils s'appliquer ? Quels indicateurs de performance peuvent être utilisés pour évaluer la réussite d'une initiative IDT ?

R.

Investir dans une solution IDT peut répondre à de nombreux besoins et cas d'utilisation. L'adoption d'applications SaaS est l'une des principales tendances de la transformation numérique. Elle est essentielle pour offrir une réduction des coûts, ainsi qu'un grand nombre d'autres avantages recherchés par les entreprises, mais elle nécessite également une réduction des risques supplémentaires lors de la migration des charges de travail vers le Cloud. Selon une étude d'IDC, la migration vers O365 est le premier cas d'utilisation pour les déploiements et les mises à niveau IDT. Viennent ensuite l'amélioration de l'efficacité des utilisateurs par la mise en place de l'identification unique pour les applications Cloud et le rapprochement de l'identité sur site et dans le Cloud. Une suite IDT d'entreprise peut également améliorer l'efficacité, par exemple en automatisant la fourniture des accès des utilisateurs grâce à l'intégration de l'IDT aux systèmes RH. En outre, elle peut contribuer à réduire les coûts des applications Cloud en identifiant les licences inutilisées. La réduction des coûts, l'amélioration de l'efficacité et la réduction des charges de travail grâce à l'automatisation sont des avantages commerciaux évidents que le conseil d'administration peut comprendre et est susceptible de soutenir.

D'autres analyses de rentabilité font ressortir une amélioration de la sécurité, une réduction des risques et un soutien de la gouvernance et de la conformité :

- Le renforcement de la sécurité de l'entreprise grâce à une authentification forte
- L'amélioration des contrôles d'accès aux informations personnelles
- La réduction des risques grâce à l'authentification adaptative ou contextuelle
- L'utilisation de la plate-forme IDT pour faciliter la création de rapports de conformité

Tous ces éléments contribuent à réduire les risques et à répondre aux exigences de l'entreprise en matière de réglementation et de conformité. Selon une étude d'IDC, parmi tous les types de risques pouvant être tolérés afin de soutenir des initiatives commerciales, les conseils d'administration sont moins susceptibles d'accepter les risques réglementaires et juridiques. Ainsi, les solutions IDT telles que

l'authentification multifactorielle constituent l'un des arguments les plus convaincants pour garantir le soutien du conseil d'administration. Enfin, il existe des cas d'utilisation spécifiques au secteur, par exemple la connexion de la plate-forme IDT à un moteur de fraude afin d'améliorer la détection et de réduire les coûts ou les pertes liés à la fraude.

Bien que la compréhension et la communication des cas d'utilisation soient des éléments clés pour mettre en œuvre des déploiements technologiques tels que l'IDT, un autre point important consiste à savoir comment éveiller l'intérêt des différents domaines d'activité et le conseil d'administration. Les équipes de sécurité ont tendance à prendre des exemples d'utilisation basés sur les architectures technologiques et les fonctionnalités des produits. Toutefois, pour entraîner une adhésion plus large et donc améliorer les chances de réussite, il est essentiel de se concentrer sur la manière dont les investissements prévus dans l'IDT généreront de la valeur commerciale.

La principale valeur commerciale que les entreprises européennes recherchent auprès de leur équipe de sécurité est la gestion des risques. Les équipes de sécurité doivent donc repenser la façon dont elles communiquent sur les impacts des solutions.

L'étude d'IDC montre que la principale valeur commerciale que les entreprises européennes recherchent auprès de leur équipe de sécurité est la gestion des risques. Les équipes de sécurité doivent donc repenser la façon dont elles communiquent l'impact des solutions. Par exemple, au lieu de se concentrer sur le renforcement des connexions conformes aux politiques, la discussion concernant l'IDT pourrait insister sur la réduction de l'exposition aux risques offerte par une expérience d'authentification transparente et une meilleure prise en charge des utilisateurs**.**

En outre, la gestion financière constitue la base des décisions commerciales. Il est essentiel que les responsables de la sécurité comprennent et communiquent les implications financières de leurs plans. Il s'agit par conséquent de présenter une analyse coûts-avantages du déploiement de l'IDT. Les principaux éléments démontrant la valeur ajoutée peuvent être les suivants : la simplification de la gestion des fournisseurs grâce à une suite d'identités de bout en bout, l'augmentation de la productivité des utilisateurs de l'entreprise grâce à une meilleure expérience utilisateur offerte par une solution d'identification unique, ou encore la réduction de la charge de travail liée aux ressources de sécurité insuffisantes et surexploitées grâce aux solutions IDaaS.

Q. Qu'en est-il des employés et des partenaires commerciaux ? Ce sont eux qui utilisent la technologie au quotidien et sont susceptibles de devoir changer leurs processus, ainsi que d'être frustrés par les complications liées à une solution IDT. Ils peuvent également créer un point faible ou une vulnérabilité par le biais de mauvaises pratiques de sécurité. Comment conjuguer la sécurité et l'expérience utilisateur, et comment garantir l'adhésion des employés ? Comme nous le savons, le rejet des utilisateurs peut entraîner l'échec de tout projet informatique, en dépit des meilleures intentions de l'équipe initiatrice du projet.

R.

Comme indiqué précédemment dans cette étude, de nombreuses initiatives IDT sont définies par l'équilibre entre la sécurité et la productivité, les utilisateurs étant l'élément déterminant. L'un des principaux défis est tout simplement de parvenir à lancer le projet : lors des premières étapes de l'adoption, l'expérience utilisateur n'est pas encore optimale et la productivité en souffre, ce qui peut entraîner le rejet de la solution. Deux éléments clés doivent être combinés pour surmonter ce problème et faire en sorte que le lancement atteigne sa vitesse de croisière.

- Tout d'abord, le projet doit être soutenu par le conseil d'administration, ainsi que par des experts du nouveau système aux postes de direction des services clés afin d'encourager l'acceptation et l'adoption par leurs équipes. Comme indiqué dans la réponse à la question précédente, cela se traduit par la présentation des cas d'utilisation et des avantages pour l'entreprise.
- Ensuite, lors des premières étapes d'un déploiement, les équipes informatiques et de sécurité doivent être très actives en matière de communication, de formation et d'éducation. Elles doivent également répondre aux difficultés et recueillir les commentaires des utilisateurs. Ce dernier élément est important : lorsque les utilisateurs sentent que leurs problèmes et leurs questions sont écoutés et traités, ils sont plus susceptibles de persévérer dans l'utilisation du système.

Lorsque les premières semaines se sont écoulées et que les utilisateurs commencent à se familiariser avec son utilisation, la productivité se rétablit (et dépasse souvent son niveau précédent) et le succès du projet est assuré.

Q. Les partenaires commerciaux peuvent être une préoccupation pour de nombreuses entreprises. On a beaucoup parlé des entreprises exposées au risque de la chaîne logistique : des systèmes sont menacés par une sécurité faible ou des informations d'identification sont compromises par un fournisseur ou un partenaire commercial. Comment l'identification unique doit-elle être contrôlée ou limitée en ce qui concerne les partenaires, et quels sont les avantages apportés par l'authentification multifactorielle et les gestionnaires de mots de passe d'entreprise en matière de sécurité ?

R.

Malgré les avantages évidents de l'identification unique, il faut comprendre que celle-ci sert généralement à contrôler l'accès à un ensemble spécifique d'applications par un ensemble spécifique d'utilisateurs, généralement les employés de l'entreprise. Si la solution d'identification unique de l'entreprise doit être étendue aux partenaires et aux fournisseurs, elle doit inclure la possibilité de configurer un accès basé sur les rôles pour des postes spécifiques, et limiter les droits et l'accès des utilisateurs ne faisant pas partie de l'entreprise. Le système ne doit autoriser aucun type de mouvement latéral ou d'escalade des privilèges non autorisée (deux comportements clés des cybercriminels lorsqu'ils parviennent à infiltrer un réseau).

L'authentification multifactorielle et les gestionnaires de mots de passe d'entreprise ont également un rôle à jouer ici. Il peut arriver que l'entreprise ait conclu un accord de diligence raisonnable avec ses partenaires et dans ses contrats de niveau de service concernant le service qu'elle fournit. Toutefois, ces politiques ne sont pas toujours appliquées de manière stricte ; il peut également arriver que les employés du prestataire de services partenaire ne respectent pas des normes de sécurité aussi strictes. Le partage et la réutilisation des informations d'identification sont ici les principales préoccupations. Dans ce type de situation, l'authentification multifactorielle peut fournir une couche de sécurité supplémentaire, garantissant que chaque connexion d'un partenaire aux systèmes de l'entreprise est authentifiée séparément et individuellement. Les gestionnaires de mots de passe d'entreprise peuvent également représenter un avantage considérable pour les partenaires : s'ils fournissent des services à des dizaines ou des centaines de clients, avec des identifiants de connexion uniques pour chacun d'eux, un gestionnaire fournit un outil précieux qui leur permet de gérer en toute sécurité toutes ces informations d'identification, sans recourir à la réutilisation des mots de passe ou à des mots de passe faibles.

Q. Comme vous l'avez expliqué, il existe de nombreuses raisons convaincantes de passer à une solution IDT moderne basée sur le Cloud. Pour conclure, quels conseils ou recommandations donneriez-vous aux RSSI ou DSI devant examiner ces facteurs, quel que soit l'avancement du déploiement de leur solution IDT ?

R.

Ceux qui envisagent d'adopter une plate-forme IDT ou de mettre à jour leur solution existante doivent garder une chose essentielle à l'esprit : de nombreuses solutions utilisées aujourd'hui ont été conçues et développées pour l'ancienne architecture et l'ancienne infrastructure, souvent intégrées à des solutions disparates ou ajoutées après coup. Elles ne sont conçues et optimisées ni pour les architectures modernes, ni pour l'infrastructure basée sur le Cloud, ni pour l'adoption d'applications SaaS prolifiques, ni pour les pratiques de travail mobiles des utilisateurs actuels. Les plates-formes IDT modernes comprennent des solutions intégrées prêtes pour le Cloud, conçues pour répondre à tous les besoins et problématiques des utilisateurs et de l'entreprise. Ainsi, lorsque des inquiétudes

surgissent concernant l'adoption ou le rejet par les utilisateurs d'une nouvelle solution IDT, soyez clair sur le fait qu'elle représente une avancée et non une chose à craindre.

Néanmoins, l'étude d'IDC montre également que la plupart des entreprises européennes utilisent ce qu'on appelle un environnement multi-Cloud : une combinaison de plusieurs applications et infrastructures sur site, dans le Cloud privé et dans le Cloud public. Il est essentiel que les plates-formes IDT prennent en compte la nécessité pour les utilisateurs et les charges de travail de passer d'un composant multi-Cloud à un autre, sans sacrifier la convivialité ou la sécurité, ce qui n'est pas une mince affaire. Les entreprises ne doivent cependant pas hésiter à mettre leurs potentiels fournisseurs de solution IDT au défi de répondre à ces exigences.

À propos de l'analyste

Mark Child, Responsable de la recherche, Sécurité européenne

Mark Child est responsable de la recherche pour le groupe européen de sécurité d'IDC. Son travail se concentre sur la sécurité Endpoint et l'IDT (Identity and Digital Trust). Il étudie également l'innovation dans les technologies de sécurité, l'émergence de nouvelles approches de sécurité, et comment celles-ci peuvent aider les entreprises à relever les défis de la sécurité des informations à mesure que l'infrastructure et les menaces évoluent.

IDC UK

5e étage, Ealing Cross,
85 Uxbridge Road
Londres
W5 5TH, Royaume-Uni
+ 44.208.987 7100
Twitter : @IDC
idc-community.com
www.idc.com

Siège mondial : 5 Speen Street, Framingham, MA 01701, États-Unis Tél. : +1 508 872 8200
Fax : +1 508 935 4015

À propos du portefeuille de gestion des identités et des accès de LogMeIn

LastPass est un gestionnaire de mots de passe primé qui aide plus de 17,8 millions d'utilisateurs à organiser et à protéger leur vie en ligne. LastPass fournit des solutions de gestion des identités et des accès faciles à utiliser à plus de 61 000 entreprises de toutes tailles. De l'authentification unique à la gestion des mots de passe d'entreprise en passant par l'authentification multifactorielle adaptative, LastPass for Business offre un contrôle supérieur aux services informatiques et un accès simple aux utilisateurs. Pour plus d'informations, rendez-vous sur https://www.lastpass.com/fr. LastPass est une marque commerciale de LogMeIn aux États-Unis et dans le monde.

À propos d'IDC

International Data Corporation (IDC) est le principal prestataire international dans le secteur de la recherche, du conseil et de l'événementiel sur les marchés des technologies de l'information, des télécommunications et de la technologie grand public. IDC aide les professionnels de l'informatique, les cadres et les investisseurs à prendre des décisions étayées par des informations tangibles, dans le cadre d'achats technologiques et de stratégie d'entreprise. Plus de 1 100 analystes IDC mettent en application leurs connaissances au niveau mondial, régional et local en matière de technologie et de secteur d'activité, dans plus de 110 pays à travers le monde. Depuis 50 ans, IDC fournit un éclairage stratégique afin d'aider ses clients à atteindre leurs objectifs clés. IDC est une filiale d'IDG, leader mondial dans les secteurs des supports technologiques, de la recherche et de l'événementiel.