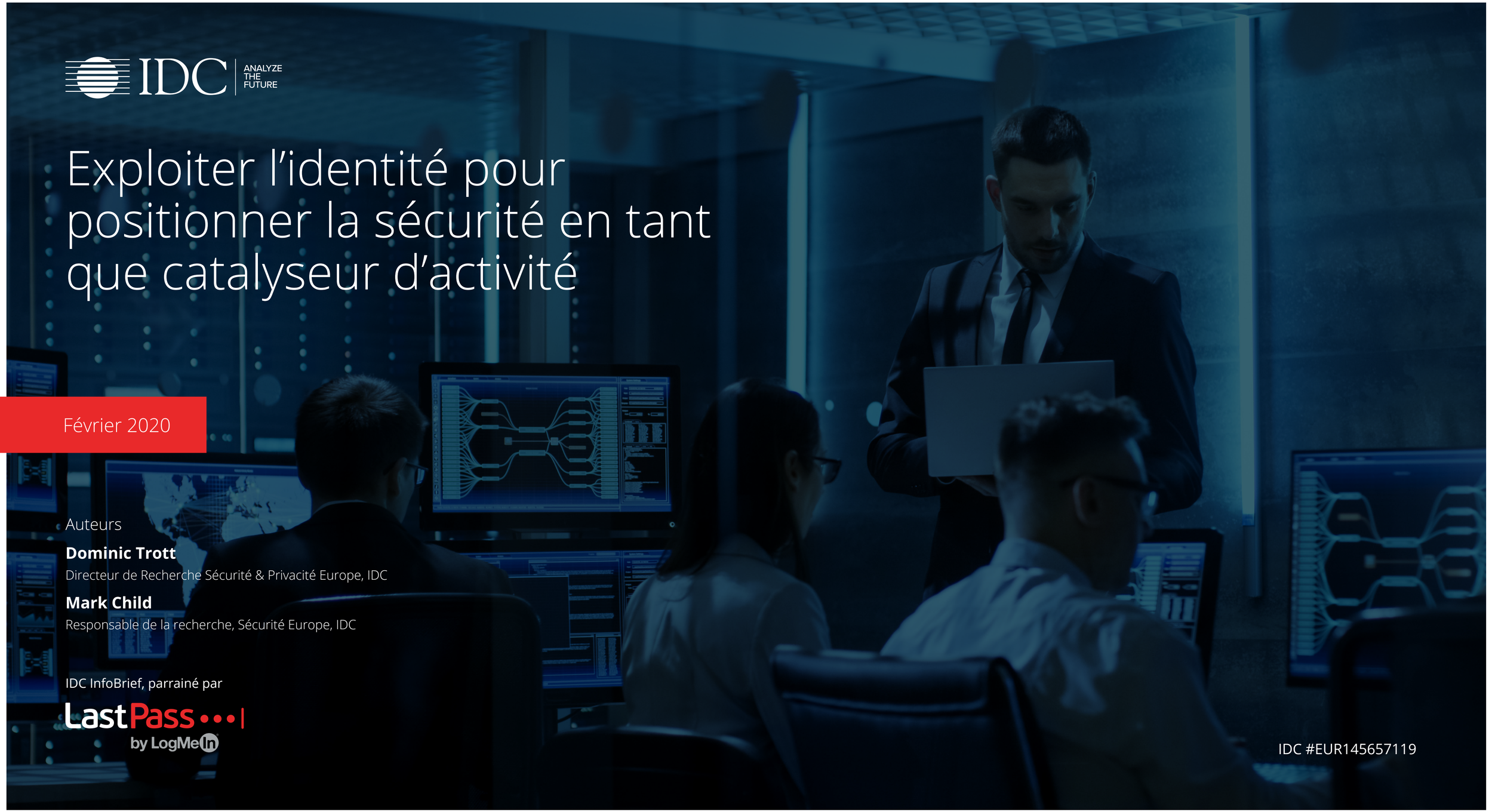


Exploiter l'identité pour positionner la sécurité en tant que catalyseur d'activité

Février 2020

Auteurs

Dominic Trott

Directeur de Recherche Sécurité & Privacité Europe, IDC

Mark Child

Responsable de la recherche, Sécurité Europe, IDC

IDC InfoBrief, parrainé par

LastPass by LogMeIn

IDC #EUR145657119

Qu'allez-vous apprendre dans cette édition d'Infobrief ?

PARTIE 1

CONTEXTE

Il est important que la sécurité génère un impact au-delà du déploiement de la technologie et du blocage des menaces. Plus précisément, la sécurité doit devenir un vecteur de valeur ajoutée. Comment la gestion des identités peut-elle aider les équipes de sécurité à atteindre cet objectif ?

PARTIE 2

LE DÉFI

La sécurité a longtemps été perçue comme un obstacle commercial et, dans certaines entreprises, elle le reste. Quelles sont les implications opérationnelles de ce problème de réputation de marque pour les équipes de sécurité ? Que réserve l'avenir à la réputation de marque, aux équipes de sécurité européennes et à leurs responsables ?

PARTIE 3

L'OPPORTUNITÉ

La gestion des identités et des accès des utilisateurs est l'un des problèmes de sécurité les plus épineux pour les entreprises européennes. Ce rapport identifie 5 thèmes clés pour aider les responsables de la sécurité à exploiter la puissance des identités, non seulement pour résoudre ces problèmes, mais aussi pour créer de la valeur.

PARTIE 4

ENGAGER LE CONSEIL D'ADMINISTRATION

La gestion des identités permet de transformer la sécurité en vecteur de création de valeur. Mais les équipes de sécurité sont-elles prêtes à s'investir dans l'activité de l'entreprise, notamment au niveau du conseil d'administration ? Cette section présente les bonnes pratiques permettant aux équipes de sécurité de parler le langage de l'entreprise pour renforcer leur influence.

PARTIE 1

CONTEXTE

Contexte

Le rôle de l'équipe de sécurité est en pleine mutation. Le raisonnement traditionnel consiste à identifier et bloquer les menaces visant l'entreprise. Cependant, la montée en puissance de la transformation numérique (DX) **qui, selon les recherches d'IDC, est une priorité de la stratégie commerciale pour**

89% **des entreprises européennes,**

implique un changement d'approche, car il faut comprendre l'appétence aux risques de l'entreprise.

Cela amène en retour deux exigences supplémentaires :

DÉPLOYER
les bons outils pour mieux identifier et gérer les risques de sécurité propre aux utilisateurs

INTÉGRER LA SÉCURITÉ
dans de nouveaux projets métier dès la phase de conception, afin de trouver un équilibre entre la protection et la simplicité d'utilisation

Cependant, les équipes de sécurité doivent composer avec la « réputation de la marque », car elles sont souvent perçues par le reste de l'entreprise comme un obstacle, plutôt que comme un accélérateur. L'approche traditionnelle de la sécurité consistant à « faire barrage à tous les risques » n'est plus compatible avec l'impératif d'optimisation de la gestion des risques propre à la transformation numérique. Cela empêche les équipes de sécurité de s'impliquer dans les projets métier qu'elles sont censées protéger et limite encore davantage leur impact.

Par conséquent, pour accompagner ces changements, il leur incombe de démontrer leur impact sur l'activité. Cela leur donnera la crédibilité nécessaire pour s'impliquer dans les initiatives numériques et sectorielles dont elles ont été tenues à l'écart jusqu'à présent.

IDC estime que l'exploitation de la gestion des identités et des accès (IAM) constitue une opportunité clé qui permettra aux équipes de sécurité de démontrer leur importance pour le développement de l'activité de l'entreprise. Exemple :

- l'intégration d'outils disparates dans une plate-forme d'identité de bout en bout peut dégager des économies et améliorer l'utilisation des effectifs
- La mise en place de processus d'accès plus intuitifs incite davantage des comportements conformes pour une meilleure hygiène de sécurité
- Comprendre et suivre qui a accès à quelles applications et données peut contribuer au respect de la réglementation

Cet InfoBrief IDC explique comment l'identité peut aider à positionner les équipes de sécurité en tant qu'accélérateur d'activité et comment elles peuvent communiquer avec le conseil d'administration pour y parvenir.

PARTIE 2

LE DÉFI

Le défi de perception

Que l'on s'en rende compte ou non, et malgré les efforts déployés dans le sens contraire, la sécurité a un problème : elle souffre d'une image négative au sein de l'entreprise.

- Les recherches d'IDC menées en 2019 révèlent que la majorité des entreprises européennes (58 %) perçoivent les équipes de sécurité comme un accélérateur d'activité.
- Il s'agit d'une amélioration par rapport à 2017, où à peine plus de la moitié des personnes interrogées, soit 53 %, considéraient la sécurité comme un accélérateur.
- Mais cela signifie qu'en 2019, 42 % des personnes interrogées considéraient toujours la sécurité au mieux comme un « coût nécessaire », voire un obstacle direct à l'amélioration de la satisfaction des clients et de la fidélisation des employés.

Ce problème, grave en lui-même, a un impact considérable sur l'entreprise :

- lorsqu'on leur demande à quel stade la sécurité est intégrée aux nouvelles initiatives commerciales, la majorité des entreprises européennes (40 %) affirment que la sécurité est intégrée à l'étape de planification de toutes les nouvelles initiatives.
- Cet aspect positif masque un côté obscur, car cela signifie que 60 % des entreprises n'intègrent pas la sécurité dès le début.
- Les répercussions sont triples :

1. Les niveaux d'hygiène de sécurité et de conformité aux stratégies sont réduits, ce qui expose l'entreprise aux risques de sécurité et de non-conformité aux réglementations.
2. Lorsque la sécurité est mise en place, il est peut-être trop tard pour maximiser son impact. En effet, la simplicité d'utilisation et la sécurité deviennent alors non conciliables.
3. La sécurité est alors vue (à tort) comme un obstacle, ce qui entraîne un cercle vicieux.

Ces problèmes sont révélateurs du défi imposé par les « menaces internes involontaires » :

- en d'autres termes, il s'agit des risques résultant du manque d'hygiène de sécurité et mettant en danger de façon accidentelle les identifiants, sans intentions malveillantes.
- Compte tenu des défis présentés précédemment, il n'est pas surprenant que, derrière les logicielles rançons et les programmes malveillants, les menaces internes soient le troisième problème de sécurité le plus important pour les entreprises européennes, selon l'enquête d'IDC.

Q. Quelle est la vision de la direction en matière de sécurité ?

Q. Dans quelle mesure la sécurité est-elle intégrée aux nouveaux projets métier ?

40%
Depuis l'étape de planification de tous les nouveaux projets

37%
Pendant l'exécution, mais avant lancement

14%
Uniquement après la mise en production/la vente

9%
La sécurité n'est pas encouragée de façon explicite

LES PERCEPTIONS NÉGATIVES DE LA SÉCURITÉ LA TIENNENT À L'ÉCART DES NOUVEAUX PROJETS ET ATTÉNUENT LA SENSIBILISATION.

La capacité limitée du personnel de sécurité

La faible sensibilisation à la sécurité et le comportement des employés entraînent une charge de travail supplémentaire pour le personnel de sécurité.

- Par exemple, le manque d'implication et d'hygiène de base en matière de sécurité fait que les équipes de sécurité sont généralement réfractaires au développement de la transformation numérique.
- Par conséquent, les RSSI ont tendance à penser que « l'entreprise a décidé d'appliquer des modèles de transformation numérique sans nous demander notre avis (ce qui est le plus souvent vrai). Pourtant, on attend de nous une protection efficace, par le biais de nos contrôles sur site existant. »
- Ce mouvement provient généralement d'experts métiers. L'abandon de la sécurité au niveau du processus décisionnel est un exemple classique de l'impact de la réputation du « service du non » sur la perception de la sécurité.
- La tendance à l'alignement des dépenses métier sur les objectifs de transformation numérique est considérée par les services de sécurité comme négative, car cela est synonyme d'informatique « fantôme » (à savoir des dépenses et des déploiements informatiques qui ne sont approuvés ni par le RSSI, ni par le DSI), et, par définition au-delà de leur visibilité et de leur contrôle.

Cependant, les mauvaises pratiques ne se limitent pas à la communauté d'utilisateurs :

- les équipes de sécurité ont tendance à souffrir d'environnements technologiques mal intégrés dominés par des solutions ponctuelles qui ne fonctionnent pas bien ensemble.

Les recherches d'IDC ont permis de révéler que le principal obstacle à l'élargissement de la capacité des équipes de sécurité européennes est que le personnel est accaparé par la gestion des outils et est indisponible pour les tâches de sécurité à plus forte valeur ajoutée.

- Ces précieuses ressources seraient bien mieux utilisées pour se concentrer sur des activités à plus forte valeur ajoutée (par exemple, détection des menaces et mise en place de contre-mesures, threat hunting).
- Au lieu de cela, le temps de travail est monopolisé par des tâches répétitives de moindre valeur, telles que la surveillance des journaux et la corrélation.

Ce point est mis en avant par la nature des limitations en quatrième et cinquième place : (4) « la prolifération des tâches de routine réduit encore à la disponibilité du personnel de sécurité » et (5) « la complexité liée à l'utilisation de plusieurs tableaux de bord ».

Il s'agit bien de défis clés à part entière, mais cela a aussi des implications importantes :

- cette surutilisation impose de se concentrer sur les besoins actuels et à court terme, aux dépens de la planification et de la préparation de l'avenir.
- Les équipes de sécurité sont obligées de se concentrer sur la « lutte contre l'incendie » et ne sont donc pas en capacité de planifier de meilleures contre-mesures pour l'avenir, ce qui crée un cercle vicieux qui peut être difficile à rompre.

Q. Qu'est-ce qui limite la capacité de votre entreprise à améliorer ses capacités de sécurité ?

LA MAUVAISE INTÉGRATION - DES TECHNOLOGIES DE SÉCURITÉ, MAIS AUSSI AVEC DES SECTEURS D'ACTIVITÉ - MET SOUS PRESSION UN PERSONNEL DE SÉCURITÉ EN SOUS EFFECTIF.

Source : European Security Strategies Survey d'IDC, 2019 (n = 700)

PARTIE 3

L'OPPORTUNITÉ

L'opportunité : 5 facteurs d'identité pour répondre aux besoins de l'entreprise

- Les recherches d'IDC révèlent que la plupart des équipes de sécurité européennes sont surchargées en raison du manque de sensibilisation des utilisateurs et de technologies mal déployées.
- La nécessité de relever ces défis à court terme les empêche de se concentrer sur des solutions à plus long terme pour résoudre ces problèmes. Ces solutions à plus long terme sont nécessaires pour répondre aux cinq thèmes suivants qu'IDC a identifiés comme essentiels pour répondre aux besoins de l'entreprise, comme illustré dans le schéma ci-contre.
- Ces thèmes aident les équipes de sécurité à transformer leur image de « bloqueurs d'activité » et à devenir des accélérateurs d'activité.
- De cette manière, elles peuvent bénéficier de l'assistance et de la participation active des utilisateurs, ce qui contribue à une bonne hygiène de sécurité et, par conséquent, à soutenir leur implication dans de nouvelles initiatives métier.
- C'est l'une des raisons principales pour lesquelles, si l'on compare la perception actuelle de la sécurité par rapport à celle d'il y a deux ans, les recherches d'IDC montrent que le contexte est devenu bien plus positif :
  - en 2019, 58 % des entreprises européennes considéraient la sécurité comme un accélérateur d'activité.
  - Ce niveau a progressé de 5 % par rapport à 2017.
  - IDC prévoit la poursuite de cette tendance, en raison des efforts de plus en plus nombreux visant à positionner la sécurité comme un accélérateur d'activité.

LA PERCEPTION DE LA SÉCURITÉ S'AMÉLIORE EN EUROPE, ET UNE APPROCHE CONCERTÉE DE LA GESTION DES IDENTITÉS PEUT CONTRIBUER À STIMULER ET À ACCÉLÉRER CE CHANGEMENT.

Source : European Security Strategies Survey d'IDC, 2019 (n = 700)

FACTEUR D'IDENTITÉ 1

Expérience utilisateur/client optimisée

- La sécurité a acquis une mauvaise réputation en partie parce qu'elle est perçue comme étant en contradiction avec les objectifs métier. Toutefois, cette perception change :
  - les équipes de sécurité se rendent compte qu'elles ont besoin de gagner « les cœurs et les esprits » des utilisateurs. La réévaluation de l'approche de la sécurité pour les utilisateurs doit fonctionner sur deux niveaux :
    1. Le parrainage au niveau du conseil d'administration contribuera à sensibiliser et à faire connaître le projet et en stimuler l'adoption du haut vers le bas. Cela peut contribuer, par exemple, à s'assurer que la sécurité est intégrée dans la vision de l'entreprise au niveau du PDG et dans la plate-forme numérique de l'entreprise au niveau du directeur informatique.
    2. Pourtant, il est essentiel que la sécurité devienne partie intégrante de la culture d'entreprise - pour dire les choses simplement, un élément fondamental du « business as usual » Cela est essentiel pour garantir des niveaux d'hygiène de sécurité élevés et constants.
  - Les approches relatives au positionnement et à la perception de la sécurité par l'entreprise doivent changer, afin de ne plus surcharger les équipes de sécurité et de modifier le comportement des utilisateurs.
  - Par conséquent, lorsque IDC a demandé aux entreprises européennes comment elles allaient hiérarchiser une série de préoccupations en matière de sécurité informatique, la culture de la sécurité et la sensibilisation au sein de l'entreprise se sont classées en tête.
- Mais comment la sécurité peut-elle chercher à interagir avec les utilisateurs, en particulier lorsque la mise en oeuvre de la transformation numérique réduit, voire supprime l'interaction humaine ?
  - La transformation numérique signifie que les utilisateurs et les clients sont de plus en plus physiquement séparés de leurs fournisseurs de produits et services.
  - Cependant, le point de contact unique et constant est la gestion des identités pour déterminer si les utilisateurs doivent ou non avoir accès aux applications et aux données.
  - Cela signifie que l'authentification est une opportunité clé pour prendre en charge l'expérience utilisateur.
  - Pourtant, la sécurité étant perçue par les autres services comme une source de frictions, il s'agit actuellement d'une occasion manquée.
- C'est une des principales raisons pour lesquelles, après la culture et la sensibilisation, la gestion de l'identité et de l'accès des utilisateurs est la deuxième plus grande priorité en matière de sécurité en Europe.
  - Dans un marché soumis à la transformation numérique, les contrôles de sécurité basés sur le périmètre (par exemple, le réseau, le terminal) ne sont plus fiables étant donnée la dissolution du concept de périmètre d'une entreprise.
  - Dans ce scénario, l'identité devient la première ligne naturelle de la gestion de la sécurité et, par conséquent, la priorité logique des équipes de sécurité pour répondre aux besoins des utilisateurs dans un environnement d'entreprise axé sur la transformation numérique.
  - Cela fournit un point de départ pour que les équipes de sécurité collaborent avec les experts métiers lors du lancement de nouveaux projets de transformation numérique, afin non seulement de traiter la sécurité, mais aussi de l'intégrer dans de nouveaux projets dès la phase de conception.
- Les approches traditionnelles en matière d'identité constituent un point de friction pour les utilisateurs :
  - elles sont généralement basées sur des approches par nom d'utilisateur/mot de passe, qui contribuent à une mauvaise hygiène de sécurité.
  - La diversité des applications d'entreprise signifie que les utilisateurs ont potentiellement besoin de mémoriser des dizaines de combinaisons différentes de noms d'utilisateur et de mots de passe, ce qui est une exigence irréaliste et débouche invariablement sur des mots de passe répétés, partagés ou stockés de manière non sécurisée.
  - Les solutions sur site uniquement sont une source de friction, compte tenu de la prolifération des solutions SaaS. Cela signifie que les solutions d'identité basées sur le cloud deviennent un facteur clé de simplification de l'accès pour les utilisateurs.
- Cela constitue un argument de poids pour que les équipes de sécurité intègrent dès le départ des approches plus conviviales de la gestion des identités dans les nouveaux projets métier :
  - intégration de la sécurité « dès la phase de conception » pour se mettre en retrait par rapport aux utilisateurs et limiter les frictions
  - Améliorer la visibilité et le contrôle de la sécurité grâce à une meilleure hygiène de sécurité de la part des utilisateurs

Q. Comment hiérarchisez-vous les problèmes de sécurité informatique pour votre entreprise ?

N° 1 La culture et la sensibilisation à la sécurité sont les principales priorités de sécurité pour les entreprises européennes

N° 2 La gestion des utilisateurs, des identités et des accès est leur deuxième priorité de sécurité

L'IDENTITÉ EST LA NOUVELLE « LIGNE DE FRONT » POUR LA SÉCURITÉ POST-PÉRIMÈTRE, ET UN MOYEN DE SOUTENIR L'EXPÉRIENCE DES UTILISATEURS DANS UN MARCHÉ AXÉ SUR LA TRANSFORMATION NUMÉRIQUE.

Source : European Security Strategies Survey d'IDC, 2019 (n = 700)

FACTEUR D'IDENTITÉ **2**

Gestion des identités à l'échelle numérique pour faciliter la transformation numérique

- Il est essentiel que les équipes de sécurité soient perçues comme faisant partie de la solution pour la transformation numérique, ce qui entraînera un changement dans la perception actuelle :
  - il s'agit d'un élément essentiel pour garantir que la sécurité n'est pas seulement liée à n'importe quel projet de transformation numérique, mais qu'elle est bien au cœur de celui-ci, afin de gérer tout risque connexe.
  - Démontrer comment l'approche de la gestion des identités « dès la phase de conception » peut fournir une expérience utilisateur plus fluide lors de la transformation numérique peut permettre aux équipes de sécurité d'avoir leur « mot à dire » sur les nouveaux projets métier.
  - En fait, les responsables de la sécurité doivent viser à être considérés comme faisant partie de « l'équipe numérique de rêve », qui est au cœur des stratégies d'entreprise basées sur des plates-formes numériques.
  - Cela constitue un avantage pour les responsables informatiques et les responsables des domaines d'activité dans leur déploiement, l'implication des équipes de sécurité ajoutant de la crédibilité à leur travail.
- Cela est d'autant plus vrai que moins de la moitié (46 %) des responsables de la sécurité ont des relations directes et régulières avec le conseil d'administration :
  - cela illustre les difficultés que rencontrent les équipes de sécurité lorsqu'elles doivent démontrer l'intérêt de la sécurité pour des objectifs métier tels que la transformation numérique. Mais IDC estime que l'accès régulier au conseil d'administration est une caractéristique clé des équipes de sécurité et un accélérateur d'activité.

- IDC a identifié quatre approches par lesquelles les équipes de sécurité peuvent exploiter la gestion des identités pour démontrer leur pertinence par rapport à la transformation numérique :

1. Approche cohérente des divers environnements applicatifs :

- utilisation de la technologie de connexion unique (SSO) pour simplifier l'accès des utilisateurs aux applications sur site, cloud privé et SaaS

2. Prise en charge des stratégies mobiles :

- reconnaître l'identité propre à chaque utilisateur, quel que soit le périphérique ou la fonction de formulaire qu'il utilise

3. Comptabilisation de la fragmentation des définitions d'identité/de nature d'un utilisateur :

- fournir une approche cohérente de l'identité à TOUS les utilisateurs, qu'ils se trouvent à l'intérieur ou à l'extérieur de l'entreprise - il s'agit là d'une préoccupation essentielle compte tenu de l'incohérence des approches de la sécurité tout au long de la chaîne d'approvisionnement

4. Lutte contre le risque de menaces internes :

- réduire le risque d'exposition des identifiants à cause d'une mauvaise hygiène de sécurité

46%

des entreprises européennes auditent TOUS les partenaires dans le cadre d'une gestion des risques par un tiers

21%

des RSSI européens communiquent régulièrement avec le conseil d'administration

N° 3

Après 1) les logicielles rançons et 2) les programmes malveillants, les menaces internes constituent la principale préoccupation en matière de sécurité en Europe

EXPLOITER LA GESTION DES IDENTITÉS POUR POSITIONNER LA SÉCURITÉ EN TANT QU'ACCÉLÉRATEUR DE LA TRANSFORMATION NUMÉRIQUE, LUI DONNANT UNE VOIX AU NIVEAU DU CONSEIL D'ADMINISTRATION.

FACTEUR D'IDENTITÉ 3

Propagation de la conformité sans sacrifier la convivialité

- La conformité réglementaire exerce une forte influence sur le marché de la gestion des identités, notamment en matière de confidentialité et de protection des données :
  - le Règlement général sur la protection des données (RGPD) est entré en vigueur en 2018.
  - Les recherches d'IDC montrent que la conformité est la quatrième priorité européenne en matière de sécurité.
  - Le RGPD exige également l'utilisation de « technologies de pointe », notamment la gestion d'identité, comme moyen de contrôle (et d'audit) de qui a accès à quelles données et de ce qui est utilisé.*

- La conformité réglementaire est une exigence, et non une option, mais il reste la possibilité de démontrer une valeur ajoutée par le biais de bonnes pratiques :
  - le non-respect des réglementations peut nuire gravement à la réputation de la marque.
  - Outre les amendes réglementaires pouvant être infligées en cas de non-conformité, les atteintes à la réputation représentent potentiellement un coût encore plus élevé sur une période prolongée.

- La distribution du niveau de maturité des entreprises européennes pour la conformité au RGPD suit une « courbe en cloche » classique :
  - quelques entreprises se trouvent aux extrémités, soit « totalement ignorantes », soit bien au-delà de la simple conformité.
  - La grande majorité se trouve quelque part au milieu, capable de répondre aux exigences d'un audit prospectif, mais avec des possibilités d'amélioration.

- Dans le cadre de cette distribution, des éléments anecdotiques suggèrent que la plupart des entreprises se décrivent comme « conformes manuellement » :
  - Dépend dans une certaine mesure des processus manuels
  - N'implémentant pas entièrement la « confidentialité dès la phase de conception » dans les activités habituelles

- Une approche plus concertée de l'identité peut aider les entreprises à rechercher la mise en œuvre de la confidentialité :
  - Automatisation des processus d'authentification et de contrôle d'accès grâce, par exemple, à la gestion des mots de passe d'entreprise (EPM), à l'authentification unique (SSO) et à l'authentification multi-facteurs (MFA)
  - Adopter une approche de plate-forme d'identité intégrée pour intégrer les bonnes pratiques en matière d'identité dans les activités habituelles

Q. Comment hiérarchisez-vous les problèmes de sécurité informatique pour votre entreprise ?

N° 4 La conformité est la quatrième priorité de sécurité pour les entreprises européennes (après culture/sensibilisation, identité et IoT)

Q. Quel est le principal domaine dans lequel votre entreprise attend de la sécurité informatique qu'elle crée de la valeur ?

N° 4 La réputation de la marque quatrième domaine le plus important dans lequel les entreprises européennes attendent de la sécurité qu'elle crée de la valeur

LA GESTION DES IDENTITÉS EST UN PILIER ESSENTIEL DU RESPECT DE LA RÉGLEMENTATION RELATIVE À LA VIE PRIVÉE ; LA SÉCURITÉ PEUT APPORTER UNE VALEUR AJOUTÉE EN DÉFENDANT LA RÉPUTATION DE LA MARQUE.

*Pour le texte officiel complet du RGPD de l'UE, **rendez-vous sur** https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

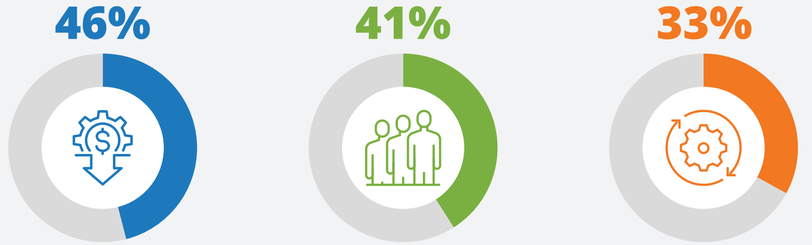
Source : European Security Strategies Survey d'IDC, 2019 (n = 700)

FACTEUR D'IDENTITÉ 4

Intégration de l'identité pour soutenir l'excellence opérationnelle

- Plusieurs éléments sont nécessaires pour garantir la réussite de l'environnement de gestion des identités :
  - les composants clés incluent des outils tels que SSO, MFA, EPM, PAM et des tableaux de bord de gestion.
- Cependant, le déploiement de plusieurs outils disparates, par exemple, complique encore davantage les tâches de l'équipe de sécurité/de l'environnement :
  - comme nous l'avons souligné précédemment, les équipes de sécurité ont déjà du mal à gérer des environnements technologiques disparates qui ne fonctionnent pas bien ensemble.
- Il est possible de déployer des plates-formes d'identité intégrées de bout en bout afin d'améliorer la simplicité et l'expérience de l'opérateur pour les équipes de sécurité :
  - Les recherches d'IDC montrent que la sécurité unifiée est le principal facteur de sélection des fournisseurs de sécurité parmi les entreprises européennes.
  - Cela indique la demande des acheteurs de solutions qui s'intègrent bien dans le portefeuille d'un fournisseur unique, s'intègrent bien aux produits tiers et, surtout, s'intègrent aux environnements de produits de sécurité existante des entreprises.
- La sécurité unifiée permet aux entreprises d'atteindre l'objectif commercial de l'excellence opérationnelle. Selon une étude récente d'IDC sur le sujet, les entreprises européennes considèrent que les principaux avantages de la sécurité unifiée sont les suivants :
  - Réduction des coûts d'exploitation
  - Meilleure rétention du personnel
  - Automatisation des tâches répétitives à faible valeur ajoutée
- Ces trois principales attentes en matière d'excellence opérationnelle représentent des mesures commerciales essentielles qui plairont jusqu'au niveau du conseil d'administration :
  - cela est important pour les équipes de sécurité qui cherchent à renforcer leur influence au niveau du conseil d'administration en se concentrant sur les résultats de l'entreprise, en particulier compte tenu du fait que moins de la moitié des responsables de la sécurité sont sous la responsabilité directe du conseil d'administration.
  - La mise en place de cette connexion au niveau du conseil d'administration peut donner un nouvel élan au repositionnement de la perception de la sécurité, passant de « bloqueur d'activité » à « accélérateur d'activité ».
  - Le renforcement de l'influence au niveau du conseil d'administration peut aider à démontrer le poids stratégique de la sécurité, qui peut à son tour garantir que la sécurité est intégrée de haut en bas dans les nouveaux projets métier, dès le début.

Q. Quels avantages tireriez-vous de l'amélioration de l'intégration et de la centralisation de votre environnement de sécurité ?



Source : Security Policy Survey d'IDC, 2019 (n = 702)

N° 1 La sécurité unifiée est le principal moteur de la sélection des fournisseurs de sécurité (avant le coût et l'efficacité technique)

46% des RSSI/ responsables de la sécurité européens communiquent régulièrement avec le conseil d'administration

UNE APPROCHE DE BOUT EN BOUT DE L'IDENTITÉ PEUT DÉMONTRER DES AVANTAGES MÉTIER QUI SUSCITERONT L'ADHÉSION AU NIVEAU DU CONSEIL D'ADMINISTRATION

Source : European Security Strategies Survey d'IDC, 2019 (n = 700)

FACTEUR D'IDENTITÉ 4

Intégration de l'identité pour soutenir l'excellence opérationnelle

L'identité et la confiance numérique exigent un ensemble de solutions

Pour concrétiser la vision de la sécurité unifiée dans un contexte d'identité et pour renforcer la confiance numérique,

AUTHENTIFICATION

La validation de la relation entre un utilisateur et une identité avec le niveau approprié d'atténuation des risques

GESTION DES IDENTITÉS/ SSO

La gestion active d'un répertoire d'utilisateurs comprenant les rôles et les autorisations tout au long du cycle de vie de l'identité. L'utilisation d'un outil de gestion des mots de passe d'entreprise (EPM) dans le cadre de la solution de gestion des identités aide les entreprises et les utilisateurs à atteindre de bons niveaux d'hygiène pour la sécurité des mots de passe.

PROVISIONNEMENT FÉDÉRÉ

La fourniture de l'accès aux ressources en ligne, soit sur site ou dans le cloud

GOVERNANCE

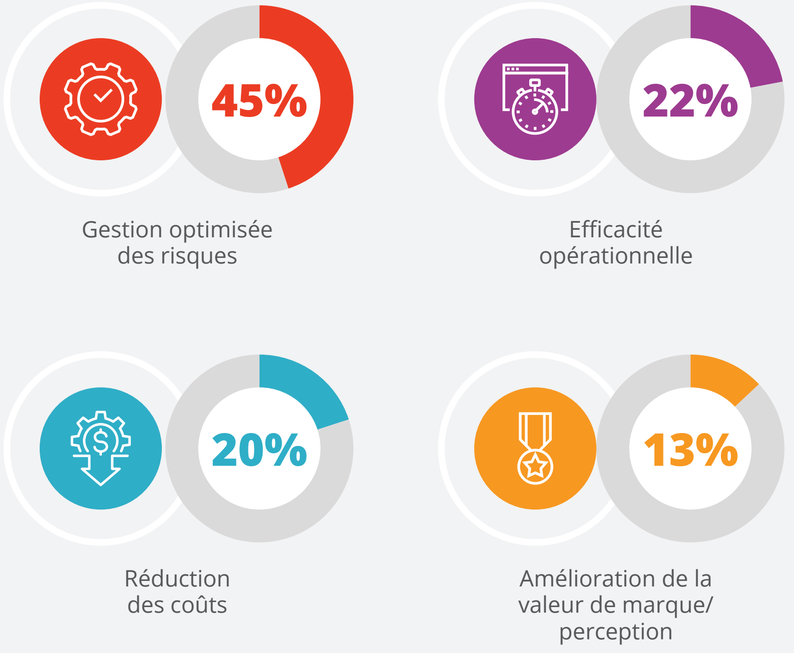
Le suivi des ressources informatiques pour le rendement, la conformité et la gestion des risques

FACTEUR D'IDENTITÉ **5**

Gestion des risques d'entreprise grâce à une identité de confiance

- L'impact financier et opérationnel des suites d'identité permet d'éveiller l'intérêt du conseil :
  - la réduction des coûts et l'efficacité opérationnelle sont des moyens importants par lesquels le service sécurité peut démontrer comment il contribue aux avantages métier et n'est pas un simple centre de coûts.
  - Toutefois, cela doit être considéré comme un point de départ pour démontrer que la sécurité est un accélérateur d'activité, plutôt que la somme totale de sa proposition de valeur.
- Si la réduction des coûts et l'efficacité opérationnelle sont importantes, les entreprises attendent plus de la sécurité :
  - l'étude d'IDC révèle que les entreprises européennes attendent principalement de la sécurité l'optimisation de la gestion des risques.
  - Cet aspect est si dominant que la part de la réponse au risque (45 %) est plus de deux fois supérieure à la réponse suivante (22 % pour l'efficacité opérationnelle).
- La gestion des identités ouvre d'excellentes opportunités pour agir en tant que point de contrôle par le biais duquel il est possible d'aborder le risque sous un angle positif :
  - des solutions d'authentification basées sur le contexte, capables d'appliquer des stratégies en fonction des conditions de l'utilisateur, permettent de s'assurer que l'accès peut être adapté en fonction de l'appétence des entreprises pour le risque.
  - En exploitant des caractéristiques conviviales telles que l'EPM, l'identité et l'accès deviennent une expérience transparente (ou aussi transparente que possible) pour les utilisateurs, ce qui favorise l'adhésion des utilisateurs et un bon comportement en matière d'hygiène, réduisant ainsi les risques à un niveau général en réduisant les menaces internes.
  - L'application d'approches cohérentes en matière d'identités et d'accès aux utilisateurs internes et externes est un moyen essentiel de réduire l'exposition aux risques, étant donné qu'environ un cinquième des entreprises européennes appliquent des approches cohérentes en matière de gestion des risques à tous les partenaires de la chaîne d'approvisionnement.
- Si la gestion des risques reste clairement une exigence clé, la gestion des identités a l'opportunité de démontrer sa valeur à un niveau plus élevé :
  - en collaboration avec le panel de RSSI européens d'IDC, il a développé un plan en trois étapes pour la transformation de la sécurité.
  - Alors que l'excellence opérationnelle et l'optimisation des risques sont les deux premières étapes, la confiance numérique est le sommet, comme détaillée à la page suivante.
  - La confiance numérique fournit à la sécurité l'occasion de s'intégrer à des projets métier, telle que la transformation numérique, afin de fournir la confiance numérique nécessaire pour sécuriser l'adhésion des employés, des partenaires et des clients.

Q. Quel est le principal domaine dans lequel votre entreprise attend de la valeur de la sécurité ?



LA SÉCURITÉ NE PEUT PAS ATTÉNUER TOUS LES RISQUES - CE QUI EST IMPOSSIBLE - MAIS DOIT ENGLOBER L'OPTIMISATION DES RISQUES POUR DÉMONTRER SA VALEUR MÉTIER.

Source : European Security Strategies Survey d'IDC, 2019 (n = 700)

Plan directeur d'IDC pour la transformation de la sécurité

L'EXCELLENCE OPÉRATIONNELLE DE LA SÉCURITÉ

- Enjeux du marché actuels de la sécurité
- Intégration de l'efficacité
- Automatiser pour l'efficacité
- Envisager une « sécurité par conception » dans les activités plus larges de l'entreprise (pas seulement la sécurité)
- Externaliser en fonction de l'échelle et de la capacité d'accès

PARTIR DES RISQUES POUR DÉMONTRER L'IMPACT BUSINESS

- Focus du jour : le risque
- Le « pont » qui comble le fossé entre la sécurité et l'entreprise par la quantification et le contenu
- Expression des concepts de sécurité en termes que l'entreprise peut comprendre
- Un point de comparaison par rapport à ses pairs
- Démontrer l'impact positif/la progression du programme de sécurité
- Justifier l'investissement dans la sécurité

CONFIANCE NUMÉRIQUE DÉBOUCHANT SUR LA TRANSFORMATION NUMÉRIQUE

- Un voyage, pas une destination
- La réalisation d'un alignement complet entre la sécurité et l'entreprise
- La « mise en œuvre » de la sécurité et de la confidentialité dès la phase de conception
- Un « fil de sécurité » qui s'exécute dans toute l'entreprise, qui guide le comportement des employés, pour permettre la réalisation des objectifs de l'entreprise
- Des implications plus larges : au-delà de l'entreprise pour favoriser la sélection des partenaires et soutenir la réputation de la marque
- Tout est contextualisé par le risque

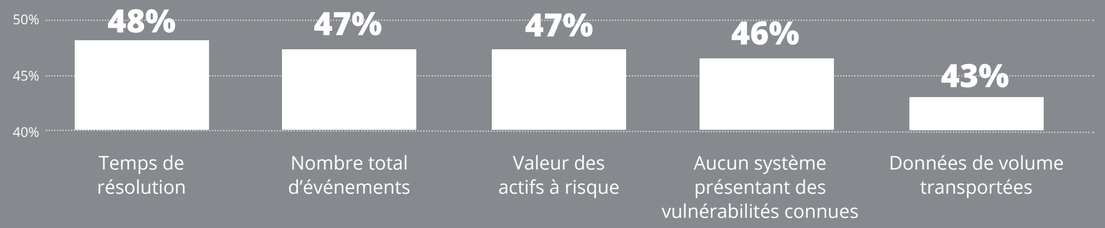
Source : European Security Strategies Survey d'IDC, 2019 (n = 700)

PART 4

ENGAGER LE CONSEIL D'ADMINISTRATION

Soyez prêt à travailler avec l'entreprise et le conseil d'administration (1/2)

- L'adoption d'une approche optimale de l'identité offre des avantages tangibles aux équipes de sécurité et à l'entreprise dans son ensemble. Mais pour tirer parti de ces avantages, les équipes de sécurité et plus particulièrement les responsables de la sécurité doivent être prêts à travailler avec les experts métier et le conseil d'administration :
  - la perception de la sécurité a des implications positives significatives lorsqu'il y a des liens plus forts avec le conseil d'administration.
  - Par exemple, les recherches d'IDC révèlent que dans les entreprises où la sécurité est perçue comme un accélérateur, non seulement les RSSI rendent généralement compte à un membre du conseil d'administration, mais il est aussi fréquent que cette relation soit directe.
- Pour établir ces lignes de communication, le service de sécurité doit adopter un langage susceptible de capter l'attention de l'entreprise et du conseil d'administration :
  - cela suggère que les équipes de sécurité adoptent des KPI relatifs aux résultats de l'entreprise pour mesurer leur impact et leurs performances.
  - Mais l'European Security Survey d'IDC (enquête européenne sur la sécurité) de 2019 montre que les 5 principaux indicateurs clés de performance (mesurés par la fréquence d'utilisation parmi les échantillons) utilisés pour mesurer les performances de la sécurité sont de nature hautement technique.
  - Bien que les KPI techniques restent importants pour mesurer les opérations de sécurité, et que les risques figurent dans cette liste, les équipes de sécurité ont clairement la possibilité de se concentrer davantage sur les résultats de l'entreprise afin d'améliorer leur profil et leur impact.



- Il existe des variations claires dans les priorités axées sur les équipes de sécurité considérées comme des accélérateurs par rapport à celles perçues comme des obstacles :
  - même dans le cas de la mesure de la valeur des ressources à risque, il s'agit d'une approche « réactive », qui explique pourquoi la sécurité est importante pour protéger ces actifs.
  - Cela n'explique pas le travail réalisé par les équipes de sécurité pour protéger ces ressources, ni la réduction des risques d'atteinte à ces ressources.
- Mais, pour aller au-delà du service de sécurité, il est essentiel de se concentrer sur des mesures métier, telles que la gestion des risques, la gestion des coûts et l'utilisation des ressources :
  - la gestion optimisée des risques est la valeur clé que l'entreprise attend de la sécurité.
  - De même, pour commencer à penser et à agir comme un leader de l'entreprise, et pour ouvrir des canaux de communication avec les experts métier et le conseil d'administration, la gestion des coûts et des ressources sont des valeurs clés.
- Il est intéressant de noter que les valeurs varient selon que les équipes de sécurité sont perçues comme des accélérateurs ou des obstacles :
  - **pour les accélérateurs**, l'efficacité opérationnelle est mise en avant, mais également la confiance numérique pour permettre la transformation numérique, ainsi que la sensibilisation et la culture de la sécurité dans l'entreprise.
  - **Pour les obstacles**, si des valeurs centrées sur l'entreprise telles que la réduction des coûts et la confiance numérique sont bien présentes, la priorité absolue est clairement de réduire l'impact de la sécurité sur l'expérience de l'utilisateur. Cela signifie qu'il est admis que la sécurité est négative pour l'expérience utilisateur et nécessite une « limitation des dommages ».

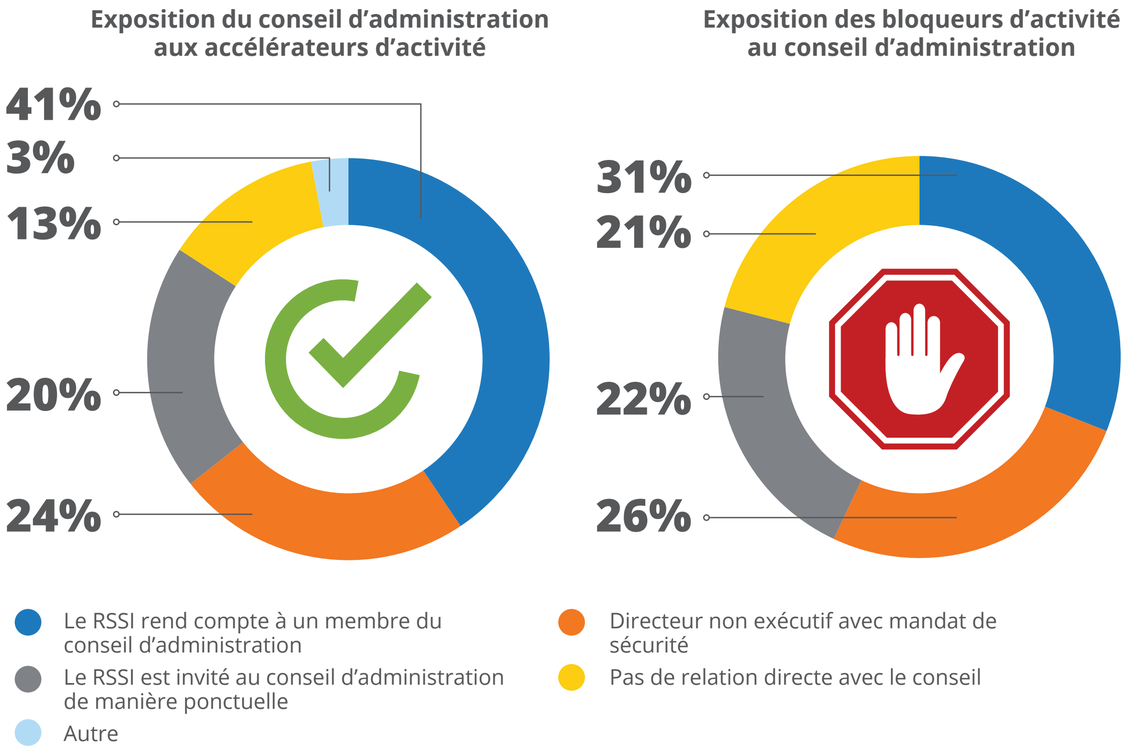
LE SERVICE DE SÉCURITÉ DOIT ÉVEILLER L'ATTENTION DU CONSEIL D'ADMINISTRATION EN COMMUNIQUANT DANS LE LANGAGE DES AFFAIRES QUE LA GESTION DES IDENTITÉS EST UN MOYEN DE CRÉER DE LA VALEUR.

- Concentrez-vous sur la sécurité en tant que sujet de gestion des risques de l'entreprise pour prendre en charge les préoccupations au niveau du conseil d'administration
- Faites des assertions fondées sur des preuves grâce à la quantification des avantages financiers et des ressources humaines
- Évitez l'utilisation d'un langage technique qui pourrait rebuter les non-spécialistes de la sécurité

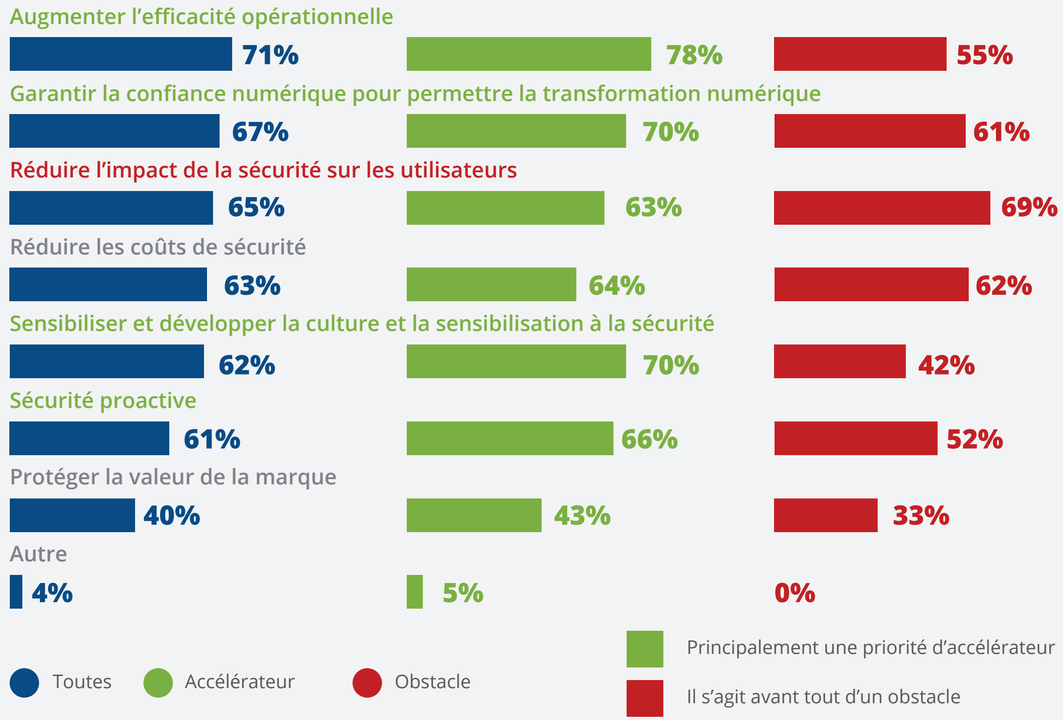
Source : European Security Strategies Survey d'IDC, 2019 (n = 700)

Soyez prêt à travailler avec l'entreprise et le conseil d'administration (2/2)

Q. Comment le service de sécurité est-il représenté au niveau du conseil d'administration dans les organisations où elle est perçue comme un accélérateur d'activité ou de bloqueur d'activité ?



Q. En plus de l'optimisation de la gestion des risques, comment pouvez-vous démontrer la valeur de la sécurité ?



LES ÉQUIPES DE SÉCURITÉ IMPLIQUÉES DANS LES ACTIVITÉS MÉTIER SONT PLUS SUSCEPTIBLES DE RENDRE DES COMPTES À UN MEMBRE DU CONSEIL D'ADMINISTRATION ET DE SUIVRE LES KPI CENTRÉS BUSINESS

Source : Security Survey d'IDC, 2019, n = 283

Résultats d'une collaboration plus étroite avec l'entreprise et le conseil d'administration

- IDC estime qu'une fois que le service de sécurité adoptera le langage des affaires, de meilleures relations avec le conseil d'administration suivront naturellement :
  - à partir de là, le service de sécurité doit se positionner pour se concentrer sur les besoins de l'entreprise et démontrer en quoi les initiatives de sécurité sont des exigences clés. Ceci est essentiel pour garantir un soutien du haut vers le bas depuis le conseil d'administration.
  - L'influence du service de sécurité au niveau du conseil d'administration peut être grandement facilitée par la désignation d'un porte-parole au sein du conseil qui « comprenne » l'importance de la sécurité.
  - Cela peut contribuer à garantir que la sécurité est intégrée dans la vision et la stratégie du PDG, ainsi que la vision du directeur informatique pour une plate-forme numérique de bout en bout sécurisée dès sa phase de conception.
- L'IDC fait les recommandations suivantes pour stimuler l'engagement de la sécurité auprès du conseil d'administration :
  - au lieu d'être ponctuelle, la communication entre la sécurité et le conseil d'administration doit être récurrente, afin de démontrer son impact commercial et de soutenir l'élévation de la sécurité au rang de préoccupation du conseil d'administration.
  - Les responsables de la sécurité doivent se concentrer sur une formulation adaptée à leur conseil d'administration. Bien qu'elle varie d'une entreprise à l'autre, des mesures quantifiables telles que le risque, le coût et la valeur des ressources constituent une base universelle.
  - Les responsables de la sécurité doivent éviter de se concentrer sur la technologie et le jargon. Bien que la technologie puisse être essentielle au succès de la sécurité, du point de vue du conseil d'administration, l'accent sera mis sur les résultats de l'entreprise.

- Les meilleures plates-formes d'identité fournissent un moyen de cibler des résultats commerciaux tangibles :

EXPÉRIENCE UTILISATEUR
En utilisant l'EPM, vous n'avez plus besoin de mémoriser plusieurs combinaisons de nom d'utilisateur et de mot de passe (et découragez ainsi les méthodes de capture et de partage de mots de passe non sécurisées).

AMENER LA CONFIANCE NUMÉRIQUE POUR PERMETTRE LA TRANSFORMATION NUMÉRIQUE
La transformation numérique est très prometteuse, mais si les employés, les partenaires et les clients n'ont pas confiance en elle, cette valeur ne sera pas accessible. Il est essentiel que la sécurité soit impliquée dès le début de nouveaux projets et devienne un élément de la culture d'entreprise.

RESPECT DES DISPOSITIONS RÉGLEMENTAIRES
La possibilité de savoir qui a accès à quelles applications et données, et ce que ces utilisateurs ont fait de cet accès, est essentielle pour se conformer à des réglementations telles que le RGPD de l'UE.

GESTION FINANCIÈRE
Intégration et automatisation d'une plate-forme d'identité de bout en bout, par opposition à l'exploitation de solutions ponctuelles autonomes pour répondre à des besoins tels que MFA, SSO, PAM et EPM.

GESTION DES RISQUES
Grâce à la visibilité et au contrôle des personnes ayant accès aux applications et aux données.

L'importance des RSSI pour faire un bond en avant en termes de leadership commercial : une prédiction

2022 est le point limite pour que les responsables de la sécurité s'imposent comme leaders capables de fournir la confiance numérique nécessaire à la transformation numérique.

SCÉNARIO : IDC estime qu'une fois que la sécurité pourra mieux parler le langage de l'entreprise, de meilleures relations avec le conseil d'administration suivront naturellement.

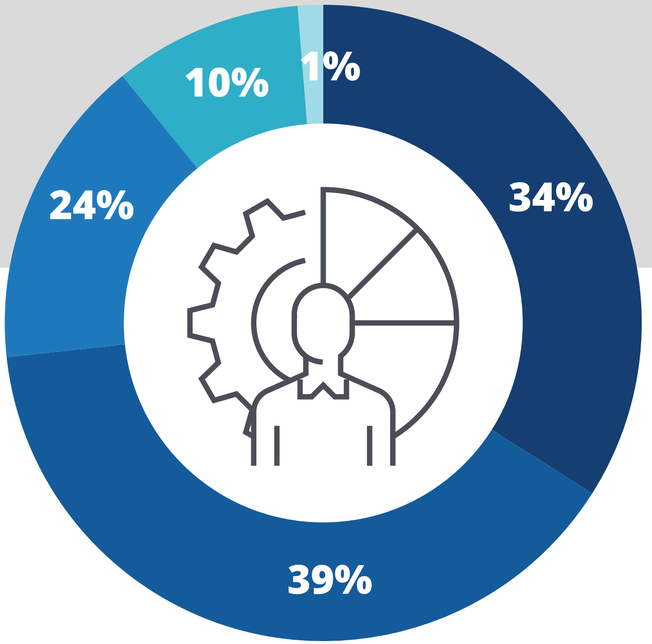
EXIGENCE : un responsable de la sécurité doit construire une équipe numérique de rêve, en lien avec la culture d'entreprise et ne disposant pas uniquement de compétences techniques.

OPPORTUNITÉ : la sécurité peut se positionner comme un élément central de la stratégie de l'entreprise en fournissant la confiance numérique nécessaire pour permettre la transformation numérique.

DÉFI : 74 % des responsables de la sécurité craignent de ne pas pouvoir franchir le pas ou de ne pas se rendre compte qu'il est nécessaire de le faire.

RISQUE : si le directeur informatique s'implique sous la contrainte, ou bien si un Directeur des Opérations est positionné plus haut dans la hiérarchie que le supérieur du RSSI , le rôle de la sécurité devient accessoire.

DANS QUELLE MESURE PENSEZ-VOUS QUE L'ÉTENDUE DU RÔLE DU RSSI VA CHANGER EN 2020 ?



- Aucune modification du champ d'application du RSSI
- Un changement de portée (davantage orienté technologie) mais toujours une position unique
- Un changement de portée (davantage orienté métier) mais toujours une position unique
- Une séparation nette entre une personne orientée vers les affaires et une personne orientée vers la technologie
- Je ne sais pas

Source : European Security Strategies Survey d'IDC, 2019 (n = 700)

RECOMMENDATIONS

Recommandations

01

Les plates-formes d'identité basées sur les bonnes pratiques permettent d'améliorer l'expérience des utilisateurs en mettant l'accent sur la sécurité et en adoptant des principes de sécurité dès la conception. Concentrez-vous sur l'expérience utilisateur des employés, des partenaires et des clients et sur la manière dont la sécurité peut faciliter la vie dans la poursuite des objectifs de l'entreprise, afin de gagner l'adhésion pour une bonne hygiène de sécurité.

02

Les équipes de sécurité peuvent renforcer leur influence en démontrant que l'identité est un accélérateur de transformation numérique, une priorité au niveau du PDG pour les entreprises européennes. Cela peut aider les responsables de la sécurité à gagner de l'influence au niveau du conseil d'administration, un domaine où ils peinent généralement.

03

Les équipes chargées de la sécurité et de la confidentialité doivent reconnaître que l'identité est un moyen d'ajouter de la valeur à l'entreprise en protégeant la réputation de la marque par le biais de la conformité réglementaire. C'est un impératif pour les entreprises européennes, étant donné que l'identité est un pilier central de la conformité et des réglementations, comme le RGPD.

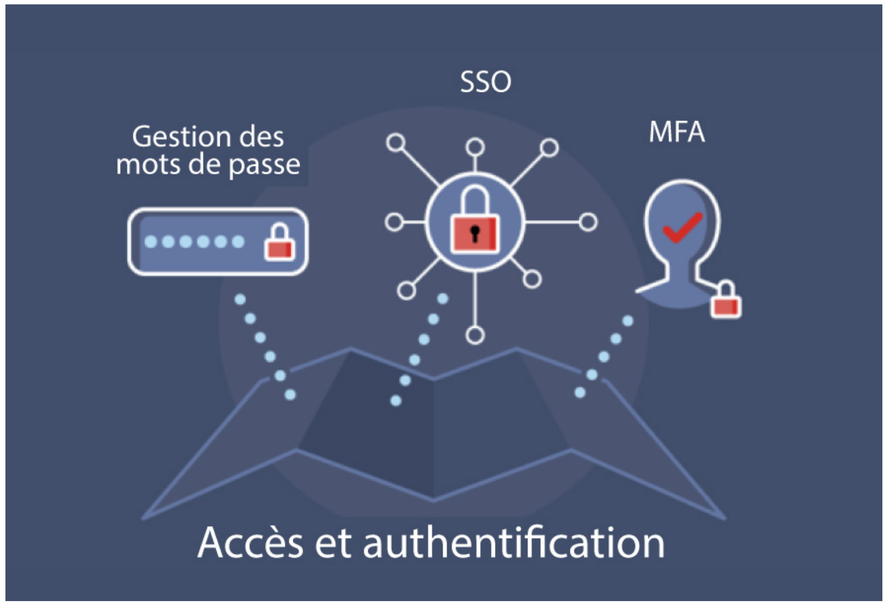
04

L'adoption d'une approche de plate-forme de bout en bout en matière d'identités peut contribuer à réduire les coûts, à améliorer l'efficacité opérationnelle et à améliorer l'utilisation des ressources humaines. Ce type de mesures aide les équipes de sécurité à communiquer avec le conseil pour démontrer leur valeur.

05

L'identité offre un moyen d'optimiser la gestion des risques, le principal avantage commercial que les entreprises européennes attendent de la sécurité. Concentrez-vous sur la manière dont l'identité traite les risques tels que les menaces internes, les interactions avec des tiers et l'abus d'informations d'identification.

LastPass pour les entreprises



LastPass pour les entreprises

Connecter simplement et en toute sécurité les employés à leur travail.

Le service informatique doit assurer la sécurité de l'entreprise, sans nuire à la productivité.

De l'authentification à l'accès aux mots de passe, LastPass gère chaque point d'entrée dans votre entreprise, afin que vous puissiez atténuer les risques tout en améliorant la productivité des employés.

Contrôles de sécurité complets

Intégrations plug-and-play

Authentification adaptative

Gestion et rapports faciles pour les utilisateurs

Contrôles de sécurité basés sur le lieu, le dispositif et le temps

Expérience utilisateur sans friction

Intégrations flexibles

Sécurité par conception

Déploiement, gestion et expérience transparents

Plus de 61 000 entreprises utilisent LastPass

Plus de 17,8 millions d'utilisateurs

Gérez chaque point d'entrée

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.

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 01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com