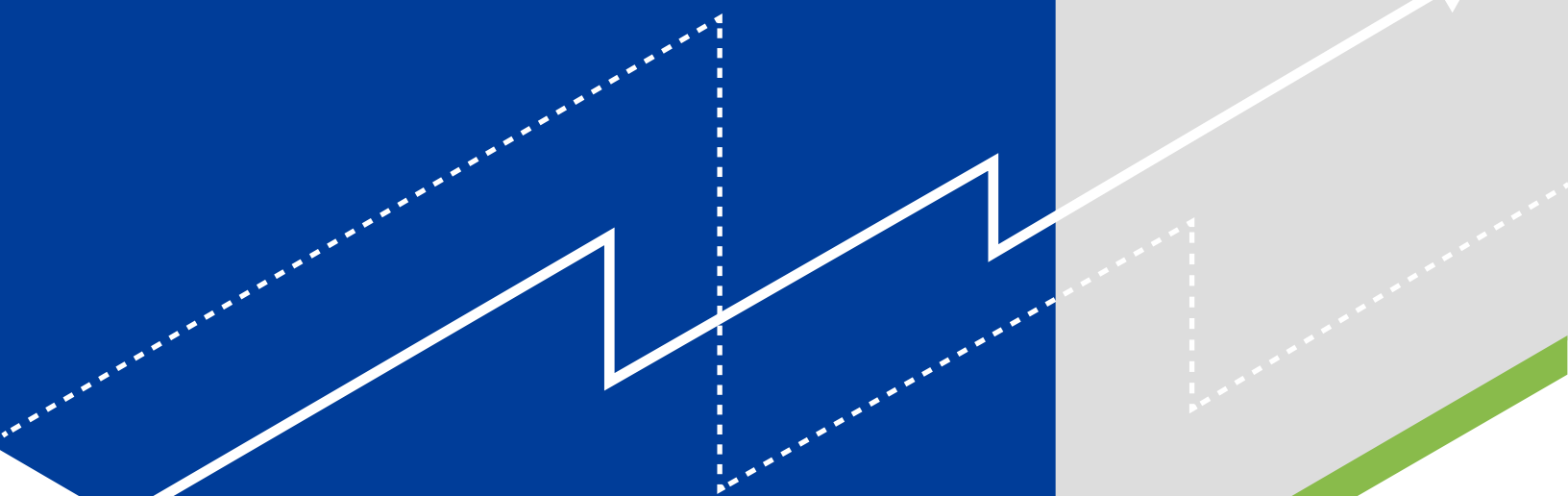
Un document de réflexion ciblé élaboré par Forrester Consulting pour Google

Repenser la sécurité des terminaux d'entreprise à l'ère du cloud computing



Directeur du projet :

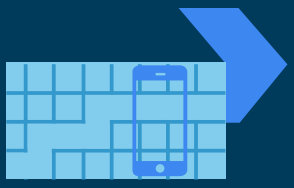
Karin Fenty, consultante senior sur l'impact marché

Étude associée :

Groupe d'étude Forrester sur la sécurité et les risques

FORRESTER®

Résumé



Les appareils personnels et les API sont de plus en plus importants pour la sécurité des terminaux.

Les fournisseurs cloud jouent un rôle important en aidant les entreprises à sécuriser les terminaux.

Au cours de la seule année 2016, le monde a fait l'objet de violations de sécurité qui ont compromis près de 2 milliards d'enregistrements.[1] Les terminaux de sécurité des collaborateurs sont de plus en plus ciblés : environ les deux tiers (64 %) des attaques externes recensées dans la région EMEA l'an dernier visaient un appareil d'entreprise, un appareil personnel ou un appareil mobile.[2] Ces violations constituent une perte de temps et d'argent pour les sociétés, affaiblissent la réputation de la marque et mettent en péril la confiance des clients et des collaborateurs.

À mesure que les sociétés adoptent les services cloud et favorisent la mobilité des collaborateurs, les interactions numériques avec les ressources de la société sont davantage distribuées et virtualisées, ce qui rend flou le concept classique du terminal. L'optimisation des terminaux classiques et non classiques pour accéder aux services cloud est stratégique, notamment lorsqu'il s'agit de la sécurité. Pour protéger les données de la société et des clients, il est de plus en plus nécessaire pour les entreprises de repenser leur approche de la sécurité des terminaux.

En juin 2017, Google a chargé Forrester Consulting d'évaluer les défis de l'entreprise et les bonnes pratiques pour la sécurité des terminaux à l'ère du cloud computing. Forrester a mené une étude en ligne mondiale auprès de 1 221 décisionnaires en sécurité informatique travaillant dans des entreprises cloud. Notre étude a montré que les sociétés ont besoin d'adopter une vision plus large de la sécurité des terminaux incluant l'ensemble des appareils et des logiciels sur et hors réseau ayant accès aux données de la société.

PRINCIPALES CONCLUSIONS

- **L'adoption des services cloud et la mobilité croissante des collaborateurs nécessitent une approche plus globale de la sécurité des terminaux.** Les terminaux non classiques comme les appareils personnels des collaborateurs sont devenus plus importants pour la sécurité des terminaux avec la prévalence du SaaS, du BYOD et de l'acloudthentification unique. Dans un environnement cloud, il est également important de prendre en compte les API dans la stratégie globale de sécurité des terminaux d'entreprise, car les API agissent comme des points d'accès aux données d'entreprise.
- **Les stratégies actuelles de sécurité des terminaux ne sont pas à la hauteur des nouvelles exigences.** Malgré les inquiétudes universelles liées à la sécurité des API, seuls 44 % des décisionnaires en matière de sécurité considèrent les API comme faisant partie de leur stratégie de sécurité des terminaux. De même, bien que la plupart des sociétés autorisent les collaborateurs à accéder aux ressources via des appareils personnels, seules 43 % d'entre elles considèrent les smartphones personnels comme un élément de leur stratégie de terminal.
- **Les entreprises font intervenir des fournisseurs cloud pour proposer une aide unique.** Le nombre d'entreprises exploitant des plateformes de cloud public a plus que doublé au cours des trois dernières années.[3] Les entreprises font confiance aux fournisseurs cloud pour héberger leurs données et ces derniers peuvent apporter leur aide en contrôlant la manière dont les données sont échangées sur les API, ce qui permet de protéger les ressources de la société contre des acteurs malveillants. 7 sociétés sur 10 ont déjà confié la sécurité de leurs terminaux à des fournisseurs de services cloud.

Les sociétés modernes doivent redéfinir la sécurité des terminaux

Plus de la moitié des entreprises internationales (53 %) ont été confrontées à au moins un piratage ou une violation de sécurité au cours d'une période de 12 mois entre 2015 et 2016, soit une augmentation de 5 % par rapport à l'année précédente.[4] La sécurité des terminaux est essentielle pour lutter contre ces violations, dans la mesure où les assaillants externes ciblent plus communément les serveurs d'entreprise, les appareils d'entreprise et les appareils personnels.[5]

Notre étude mondiale menée auprès de 1 221 décisionnaires en matière de sécurité informatique a montré que les entreprises considèrent l'amélioration des capacités de détection et d'analyse comme essentielles pour la sécurité des terminaux. La détection des menaces et l'analyse du réseau font partie des résultats recherchés en priorité, comme la réduction des violations, le contrôle en temps réel des terminaux et la réduction des surfaces d'attaque (voir Illustration 1). Toutefois, la détection et le contrôle de tous les terminaux sont devenus plus compliqués à mesure que le volume et la diversité des terminaux accédant aux ressources de la société augmentent.

LES TERMINAUX NON TRADITIONNELS ET LES API SONT DES OCCASIONS MANQUÉES ET DES FACTEURS DE RISQUE

En autorisant l'accès aux données et aux applications à partir de tout appareil ou navigateur, le service cloud élargit la surface d'attaque de l'entreprise. Les utilisateurs finaux accèdent aux données de l'entreprise à partir d'un nombre croissant d'appareils se trouvant sur le réseau et hors de celui-ci, le plus souvent à partir du navigateur comme point d'accès central. Pour combler le fossé entre l'utilisateur et la plateforme cloud, les entreprises doivent protéger non seulement les serveurs et les appareils de l'entreprise, mais aussi les appareils personnels ayant accès aux ressources de l'entreprise et les API agissant comme des points d'accès centraux entre les connexions externes et les données de la société.

Notre étude des entreprises utilisant les services cloud a révélé que la plupart des professionnels de sécurité n'ont pas adopté cette nouvelle perspective relative à la sécurité des terminaux. Ainsi, seul un petit nombre de sociétés sont confiantes dans le fait de pouvoir obtenir les résultats désirés. Plus précisément, nous avons fait les constatations suivantes :

› **Le navigateur est devenu un point d'accès central pour la messagerie et diverses autres applications métier.** Dans le cadre d'une transition vers le cloud, la sécurité des navigateurs est essentielle, car un nombre sans cesse croissant d'activités métier est exécuté au sein des navigateurs Web. Par exemple, 76 % des entreprises que nous avons sondées disposent d'options de messagerie reposant sur un navigateur et 70 % d'entre elles permettent aux collaborateurs d'accéder aux applications Office à partir d'un navigateur (Voir Illustration 2). En devenant une interface essentielle au fonctionnement de l'entreprise, le navigateur devient non seulement une cible pour les assaillants, mais constitue également un aspect important de la stratégie de sécurité des terminaux.

Illustration 1

Principales priorités en matière de sécurité des terminaux :

48 % Amélioration de nos capacités de détection des menaces

47 % Amélioration de la détection des logiciels malveillants

42 % Amélioration de l'analyse du réseau

Attentes principales vis-à-vis des technologies visant à protéger les terminaux :

75 % Amélioration des capacités de détection

75 % Réduction du nombre de violations/d'attaques

73 % Contrôle en temps réel des terminaux

72 % Réduction de la surface d'attaque

Panel : 1 221 décisionnaires en sécurité informatique travaillant dans des entreprises internationales qui utilisent des services cloud
Source : étude réalisée par Forrester Consulting pour Google, juillet 2017

72 à 77 % des travailleurs de l'information déclarent que le département informatique est responsable de la mise à jour des logiciels de sécurité, des systèmes d'exploitation et du chiffrement des documents sur leurs appareils mobiles.

FORRESTER®

› **De plus en plus de collaborateurs accèdent aux ressources de l'entreprise via des appareils personnels.** Par le biais de programmes BYOD officiels, d'options d'authentification unique et d'autres programmes visant à promouvoir la mobilité des collaborateurs, la vaste majorité des sociétés (84 %) autorisent les collaborateurs à accéder aux données de l'entreprise à partir de leurs ordinateurs, de leurs smartphones et de leurs tablettes personnels (voir Illustration 2). Ces appareils personnels élargissent la surface d'attaque de l'entreprise. Les données de Forrester montrent que même si les appareils personnels prennent de plus en plus d'importance dans le cadre d'une utilisation professionnelle, les collaborateurs s'attendent à ce que l'informatique permette de sécuriser leurs appareils mobiles par le biais de mises à jour logicielles et d'un chiffrement.[6]

› **Presque toutes les entreprises se soucient des API.** Les API revêtent une importance stratégique grandissante pour l'entreprise dans la mesure où elles permettent aux sociétés de se connecter à des ressources externes et internes, améliorant ainsi l'expérience du client et du collaborateur. Elles constituent également un aspect critique des stratégies de sécurité globales des terminaux puisqu'elles sont un point d'accès central aux données de l'entreprise. 97 % des personnes interrogées ont mentionné des inquiétudes liées à la sécurité des API, y compris des inquiétudes concernant les plateformes cloud, les protocoles réseau et les données en transit.

› **Malgré ces tendances, la plupart des équipes de sécurité n'ont pas intégré les appareils personnels et les API dans leurs stratégies relatives aux terminaux.** Les entreprises n'ont pas fait évoluer leurs stratégies de sécurité de manière à prendre en compte les nouvelles exigences liées à l'ère du cloud computing. Si la plupart des entreprises s'efforcent de sécuriser les terminaux tels que les plateformes cloud, les serveurs et les ordinateurs portables de l'entreprise, seules 43 à 46 % d'entre elles prennent en compte les ordinateurs portables et les smartphones personnels, ainsi que les API, dans la stratégie de sécurité de leurs terminaux. Par conséquent, seuls 35 % des professionnels de sécurité pensent que leur entreprise est très efficace en matière de gestion des ressources de l'entreprise, et seuls 32 % ont déclaré la même chose au sujet de l'analyse des terminaux à la recherche d'activités malveillantes (voir Illustration 3).

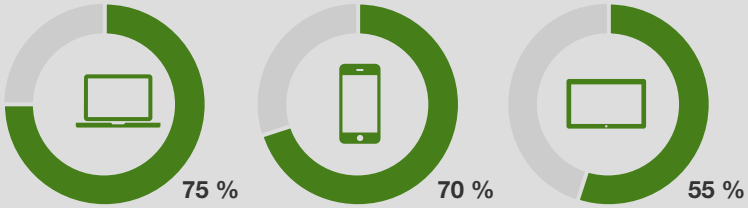
97 % des personnes ont cité les inquiétudes liées à la sécurité des API.

Les principales préoccupations en matière d'API sont les suivantes :

- **55 %** Inquiétudes relatives à la plateforme cloud
- **53 %** Attaques du protocole réseau exposant les données en transit
- **52 %** Risque lié aux tiers

Illustration 2

« Votre entreprise autorise-t-elle les collaborateurs à utiliser les appareils personnels suivants pour accéder aux ressources de la société, que ce soit via un programme BYOD, l'authentification unique ou un autre programme ? »



Ordinateurs portables/ Stations de travail | **Smartphones** | **Tablettes**

16 % S/O : accès aux ressources de la société interdit sur les appareils personnels

« Parmi les propositions suivantes, quels sont les outils auxquels les collaborateurs de votre entreprise accèdent via un navigateur Web ? » (cinq principales réponses)

76 % E-mail

70 % Applications Office (par ex., feuilles de calcul, documents)

69 % Intranet des collaborateurs

63 % Systèmes de gestion de la relation client (CRM)

59 % Applications de synchronisation et de partage de fichiers

Panel : 1 221 décisionnaires en sécurité informatique travaillant dans des entreprises internationales qui utilisent des services cloud
Source : étude réalisée par Forrester Consulting pour Google, juillet 2017

Les appareils personnels, les applications métier centrées sur les navigateurs et les API élargissent la surface d'attaque des entreprises et génèrent des inquiétudes en matière de sécurité.

FORRESTER®

Illustration 3

Technologies considérées comme faisant partie des stratégies de sécurité des terminaux de l'entreprise :

74 % Plateformes cloud

71 % Serveurs

68 % Ordinateurs portables/Stations de travail de l'entreprise ou approuvés

60 % Applications

57 % Appareils mobiles de l'entreprise ou approuvés

54 % Appareils virtuels

46 % Ordinateurs portables/Stations de travail personnels/non approuvés des collaborateurs

44 % API

43 % Appareils mobiles personnels/non approuvés des collaborateurs

Pourcentage considéré comme très efficace pour obtenir des résultats :

35 % Gestion de l'accès aux ressources de l'entreprise

32 % Analyse des terminaux à la recherche d'activités malveillantes

La plupart des sociétés ne prennent pas en compte les terminaux non traditionnels dans leurs stratégies, ce qui laisse une faille dans leur sécurité.

Panel : 1 221 décisionnaires en sécurité informatique travaillant dans des entreprises internationales qui utilisent des services cloud
Source : étude réalisée par Forrester Consulting pour Google, juillet 2017

Les fournisseurs de services cloud sont de plus en plus importants pour la sécurité des terminaux

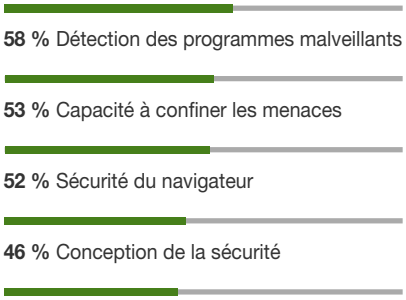
Tandis que le champ d'action de la sécurité des terminaux s'étend, les entreprises ont besoin d'analyser et de contrôler des terminaux ayant accès aux ressources de la société de plus en plus nombreux et variés. À mesure que les sociétés adoptent une stratégie davantage centrée sur le cloud pour la mise à disposition d'infrastructures et d'applications, elles peuvent exploiter les ressources et l'expertise de fournisseurs de services cloud. Voici les résultats de notre étude :

- **Sept entreprises sur dix se tournent vers les fournisseurs cloud pour les solutions et les outils de sécurité des terminaux.** En transférant un nombre croissant de données et de fonctionnalités vers le cloud, les entreprises font appel aux outils proposés par leur fournisseur cloud pour sécuriser leurs données. De plus en plus, les fournisseurs cloud sont chargés de superviser l'authentification, la gestion des correctifs et la surveillance de ces environnements cloud pour le compte de leurs clients. En fait, Forrester prévoit une augmentation des dépenses de sécurité Iaas/Paas natives de 41 % au cours des cinq prochaines années.[7]
- **La sécurité des API est un facteur déterminant dans la sélection des fournisseurs cloud.** Les fournisseurs de services cloud peuvent améliorer la sécurité en forçant l'interaction des utilisateurs avec les données via une API sécurisée. Par ce biais, ils contrôlent ainsi l'accès et la modification des données, qui sont les ressources à protéger. Tout comme le navigateur est l'interface principale des terminaux classiques, l'API est le point d'accès au cloud . En fait, la sécurité des API est le second critère le plus important utilisé par les personnes interrogées pour sélectionner un fournisseur cloud, après les systèmes de protection et de surveillance de l'infrastructure.
- **Les acheteurs de solutions de sécurité privilégient la détection des programmes malveillants, le confinement des menaces et la sécurité du navigateur dans les outils de sécurité des terminaux.** La manière dont les fournisseurs appréhendent la conception de la sécurité et leur réputation sont également des critères essentiels pour la sélection des outils de sécurité des terminaux. (voir Illustration 4) Les fournisseurs de services cloud sont les mieux placés pour répondre à ces besoins en raison de leur vision centralisée des environnements de terminaux et de leur capacité à distribuer de manière rapide et efficace les données relatives aux menaces ou les correctifs vers les terminaux. Une visibilité et une capacité accrues à réagir rapidement et à rétablir l'intégrité d'un terminal permettent aux entreprises de prévenir les attaques et de réduire les interruptions d'activité lorsqu'elles surviennent. Pour ces raisons, 71 % des personnes interrogées utilisent actuellement une solution de terminal proposée par un fournisseur Cloud, alors que 49 % utilisent des solutions de fournisseurs spécialisés.

71 % des personnes interrogées utilisent des solutions issues de fournisseurs cloud pour la sécurité des terminaux.

Illustration 4

Aspects les plus importants à prendre en considération concernant les outils de sécurité des terminaux des utilisateurs : (cinq principales réponses)



Panel : 1 221 décisionnaires en sécurité informatique travaillant dans des entreprises internationales qui utilisent des services cloud
Source : étude réalisée par Forrester Consulting pour Google, juillet 2017

La détection des programmes malveillants, le confinement des menaces et la sécurité du navigateur sont des aspects importants des outils de terminaux.

43 % considèrent la sécurité d'accès aux API comme un des critères les plus importants dans la sélection d'un fournisseur cloud.

FORRESTER®

Principales recommandations

La protection des terminaux requiert une plateforme résiliente et résistante qui peut être mise à jour rapidement, cloisonner les tâches utilisateur et appliquer des protections afin de protéger de manière globale le système ou l'appareil d'une utilisation abusive, même par inadvertance. Les pirates informatiques exploitent une myriade de techniques pour compromettre ces appareils. Il est donc crucial de mettre en place des systèmes de réduction des risques au niveau de chaque couche de la pile de sécurité du terminal.

Plus les entreprises adoptent des applications et des infrastructures centrées sur le cloud, plus les fournisseurs de services cloud jouent un rôle important parmi les autres spécialistes tiers et solutions ponctuelles. Les professionnels de sécurité au sein des entreprises utilisant des services cloud doivent tenir compte des recommandations suivantes :

La gestion de la vulnérabilité est essentielle pour l'ensemble de la pile de sécurité des terminaux. La pile de sécurité des terminaux inclut tous les éléments, de l'appareil au système d'exploitation en passant par le firmware et les logiciels installés. Le fait de travailler avec un fournisseur de services cloud fiable pouvant vous aider à gérer et à déployer des mises à jour sur l'ensemble de la pile de sécurité des terminaux réduit la complexité liée à la gestion d'un environnement comportant divers terminaux.

Tenez compte de la connexion entre les navigateurs et les API dans votre stratégie relative aux terminaux. Les navigateurs et les API sont les deux interfaces les plus proches se trouvant entre les utilisateurs et les ressources cloud. Collaborer avec un fournisseur unique pouvant assurer la prise en charge des deux côtés de ce canal de communication garantit que les améliorations proposées sont compatibles et coordonnées.

La résilience est un facteur essentiel de la protection des données utilisateur. Chaque couche de la pile de sécurité des terminaux est la porte ouverte aux attaques. La sécurité des terminaux requiert une approche descendante pour confiner les menaces en commençant par des concepts, tels qu'une « same-origin policy » pour la protection des données de navigation de l'utilisateur, l'isolement des processus, la vérification du démarrage et des configurations de base fiables à partir desquelles un terminal peut être récupéré. Assurez-vous que votre stratégie de sécurité des terminaux tient compte de chacune de ces protections pour garantir la résilience de votre terminal en termes de protection des données utilisateur.

Exploitez l'expertise de votre fournisseur cloud en matière de sécurité. Les fournisseurs cloud gèrent la partie matérielle pour fournir à de nombreuses entreprises la virtualisation dont elles ont besoin. La gestion sécurisée de ces appareils nécessite les meilleurs spécialistes et une expertise mondiale que les fournisseurs cloud vous proposent par le biais d'outils et d'intégrations de terminaux. Lors de la prise en compte des protections pour votre environnement cloud, vos fournisseurs cloud doivent être en mesure de proposer des outils et une expertise de meilleure qualité dans l'environnement qu'ils gèrent que des spécialistes tiers.

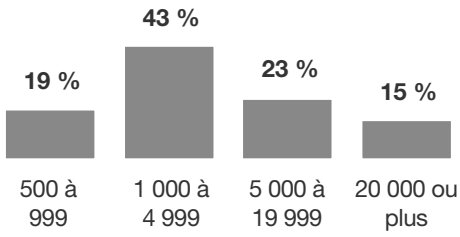
FORRESTER®

Annexe A : Méthodologie

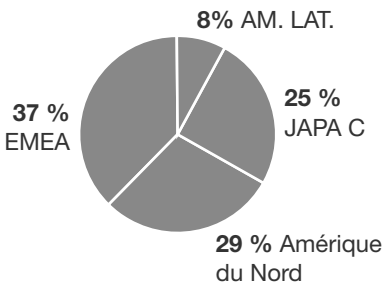
Pour cette étude, Forrester a réalisé une enquête en ligne auprès de 1 221 personnes travaillant dans des entreprises en Amérique du Nord (États-Unis et Canada), dans la région EMEA (Royaume-Uni, Allemagne, France, Italie et Pays-Bas), dans la région APAC (Japon, Inde et Australie) et en Amérique latine (Brésil et Mexique) pour évaluer les tendances et technologies en matière de sécurité des terminaux et de surveillance de la sécurité. Les participants à cette enquête incluaient des décisionnaires en sécurité informatique et des personnes chargées de la sécurité/du risque. Les questions posées aux participants concernaient leurs priorités en termes d'analyse des terminaux, leurs approches, leurs difficultés et leurs besoins technologiques. Les personnes interrogées ont reçu une petite compensation en remerciement du temps passé à répondre à l'enquête. L'étude a commencé en juin 2017 et s'est terminée en juillet 2017.

Annexe B : Échantillonnage/Données

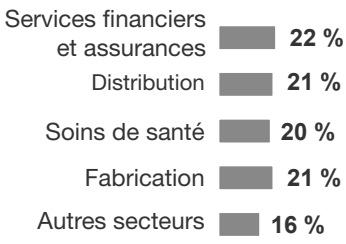
Taille de l'entreprise



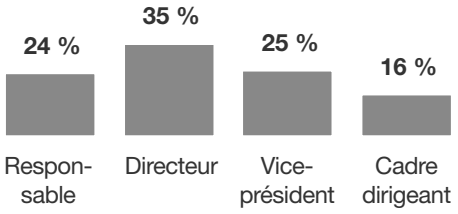
Région



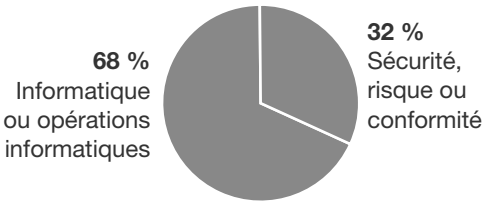
Industrie



Personnes interrogées



Rôle



100 % des sociétés interrogées utilisent actuellement des services SaaS, IaaS, PaaS ou de cloud privés

Panel : 1 221 décisionnaires en sécurité informatique travaillant dans des entreprises internationales qui utilisent des services cloud
Remarque : la somme des pourcentages peut ne pas être égale à 100 du fait de l'arrondissement des valeurs.
Source : étude réalisée par Forrester Consulting pour Google, juillet 2017

FORRESTER®

Annexe C : Autres références

ÉTUDES FORRESTER CONNEXES

« The Top Security Technology Trends To Watch, 2017, » Forrester Research, Inc., 26 avril 2017.

« Top Cybersecurity Threats In 2017 », Forrester Research, Inc., 26 janvier 2017.

« The 2016 State Of Endpoint Security Adoption », Forrester Research, Inc., 25 avril 2016.

Annexe D : Notes de bas de page

[1] Source : « Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2016 », Forrester Research, Inc., 15 février 2017. Les 2 milliards d'enregistrements notés intègrent également une estimation actualisée de 1 milliard d'enregistrements pour la violation de données de Yahoo découverte en 2016. Consultez : « Protect Your Intellectual Property And Customer Data From Theft And Abuse ». Forrester Research, Inc., 12 juillet 2017.

[2] Panel : 225 décisionnaires en matière de sécurité travaillant dans des entreprises internationales de plus de 1 000 collaborateurs. Source : enquête Business Technographics menée par Forrester sur la sécurité au niveau mondial, 2017.

[3] En Amérique du Nord et dans la région EMEA, la proportion des entreprises de 1 000 collaborateurs ou plus utilisant les services cloud publics est passée de 15 à 33 % de 2014 à 2016. Source : « Benchmark Your Enterprise cloud Adoption », Forrester Research, Inc., 3 janvier 2017.

[4] Source : « Planning For Failure: How To Survive A Breach », Forrester Research, Inc., 9 septembre 2016.

[5] Source : « The State Of Enterprise Mobile Security: 2016 To 2017, » Forrester Research, Inc., 12 janvier 2017.

[6] Panel : 1 983 travailleurs de l'information du secteur des services financiers mondiaux, de la production, des soins de santé et des entreprises de vente au détail. Source : étude Business Technographics de Forrester Data portant sur le personnel utilisant des solutions de mobilité et de télécommunications au niveau mondial, 2016.

[7] Source : « The Cloud Security Market Grows From $1.5 Billion In 2017 To $3.5 Billion In 2021 », Forrester Research, Inc., 6 juillet 2017.