Livre blanc

Le besoin absolu de sécuriser les ordinateurs

Sponsorisé par : Apple

Tom Mainelli Michael Suby
Septembre 2023

LE POINT DE VUE D'IDC

La sécurité est une préoccupation telle que les décideurs IT n'en dorment pas la nuit. Ils sont conscients que toute l'entreprise, même si elle est parfaitement gérée et que ses produits ou services sont largement appréciés, peut être compromise du jour au lendemain à cause d'une faille de sécurité,

Et malheureusement, le monde est de moins en moins sûr. L'espionnage industriel, les « États voyous », le crime organisé et même de simples délinquants s'attaquent désormais aux technologies. Pour garder une longueur d'avance sur ces acteurs malveillants, le département IT doit rester vigilant, tout en acceptant de travailler avec de nouveaux fournisseurs et de nouvelles technologies pour garantir la sécurité des salariés, des clients et des données.

La liste des défis auxquels les départements IT doivent faire face est longue et s'étend des ordinateurs aux datacenters, en passant par les réseaux qui les connectent et les logiciels qui y sont installés. Ce livre blanc souligne l'importance de sécuriser les ordinateurs. En effet, la sécurité du datacenter, du réseau et des logiciels n'a de sens que si les ordinateurs sont sécurisés.

Généralement, un ordinateur sécurisé implique un compromis aux dépens de l'expérience utilisateur puisque les appareils sont verrouillés et donc, plus difficiles à utiliser. Il s'agit là de l'un des principaux défis liés à la sécurisation des ordinateurs. Toutefois, même lorsque les appareils sont verrouillés, les utilisateurs trouvent souvent le moyen de contourner les systèmes de sécurité afin d'accomplir leur travail. Lorsque la sécurité est un problème pour les utilisateurs, elle devient contre-productive.

Grâce aux progrès technologiques, il devient néanmoins possible de préserver l'expérience utilisateur sans compromettre la sécurité. Les progrès réalisés en matière de détection des malwares, de protection des données, d'authentification et d'intégration matériel-logiciel permettent aujourd'hui de ne plus sacrifier la productivité au profit de la sécurité.

Septembre 2023, IDC n° US51204723

METHODOLOGIE

En juillet 2023, IDC a réalisé une enquête en ligne auprès de décideurs IT aux États-Unis et au Canada (513 répondants) afin de connaître leur point de vue sur la sécurité en général et l'importance de la sécurisation des ordinateurs en particulier. Les répondants appartenaient à des entreprises d'au moins 500 salariés œuvrant dans différents secteurs d'activité. Ces entreprises géraient plusieurs systèmes d'exploitation, tels que Microsoft Windows, Apple macOS et Google ChromeOS Les décideurs IT interrogés avaient la responsabilité de sélectionner, d'acheter ou de déployer des logiciels de sécurité pour leur entreprise, ou de superviser des collaborateurs ayant cette responsabilité.

ÉTAT DES LIEUX

La sécurité reste une priorité absolue pour tous les dirigeants d'entreprise. Les entreprises clairvoyantes savent que la sécurité n'est pas une option, mais plutôt une nécessité pour toute entreprise qui souhaite prospérer dans un environnement où les menaces sont en constante évolution, sous l'impulsion d'acteurs malveillants parfaitement coordonnés et disposant de moyens financiers.

L'enquête Future Enterprise Resiliency and Spending Survey (FERS), réalisée en mars 2023 par IDC auprès de décideurs IT travaillant dans des entreprises d'au moins 500 salariés, révèle que 50% des entreprises interrogées dans le monde ont été victimes d'une attaque par ransomware ayant perturbé leur business au cours des 12 derniers mois. Plus d'un tiers a affirmé que cette attaque avait perturbé leur business pendant au moins une semaine. Malgré des protocoles de sécurité renforcés, les grandes entreprises ne sont pas à l'abri de ce type d'attaques. Au contraire, les entreprises les plus fortement impactées sont celles comptant 1 000 à 2 499 salariés (71%), 2 500 à 4 999 salariés (72%) et 5 000 à 9 999 salariés (70%). Autrement dit, aucune entreprise n'est à l'abri d'une telle attaque.

Selon cette même étude, les ordinateurs constituent le principal point d'entrée des attaques par ransomware. Les points d'attaque initiaux sont les navigateurs Web (21%), les supports de stockage amovibles (18%), les pièces jointes aux e-mails (17%), les supply chain (17%), les URL figurant dans les e-mails (14%) et les accès par des initiés (8%).

En raison du nombre croissant de salariés travaillant à distance ou en mode hybride, les ransomwares et autres menaces de sécurité sont devenues plus difficiles à gérer pour le département IT. Selon l'enquête Endpoint Security Survey conduite en décembre 2022 par IDC, 97% des entreprises fonctionnent avec une partie de leurs collaborateurs à distance. Même si ce chiffre risque de diminuer au cours des 12 prochains moins, il restera très élevé à l'avenir.

Alors que les entreprises cherchent des solutions pour répondre au défi permanent posé par le travail à distance, les stratégies zero trust sont de plus en plus souvent utilisées. Les meilleures pratiques consistent à mettre en place des contrôles de sécurité, une protection avancée pour les ordinateurs, une certification des appareils (permettant de s'assurer que les appareils qui se connectent au réseau sont autorisés à le faire) et une authentification renforcée des utilisateurs.

Compte tenu de tout ce qui précède, il n'est pas surprenant de constater que les répondants à l'enquête d'IDC ont très majoritairement choisi de renforcer en priorité la sécurité générale des données ainsi que la sécurisation des ordinateurs, comme le montre le Graphique 1.

Il convient également de noter que l'amélioration de la productivité des salariés grâce à l'utilisation de meilleurs appareils figure au troisième rang des priorités des répondants. Lorsqu'ils ont été interrogés sur leurs trois principales priorités, l'utilisation de meilleurs appareils a été la réponse la plus souvent citée. Le message essentiel à retenir est clair : la sécurité est importante, mais elle ne doit se faire au détriment de la productivité des collaborateurs et les meilleurs appareils doivent être équipés de systèmes de sécurité renforcés qui ne perturbent pas les salariés.

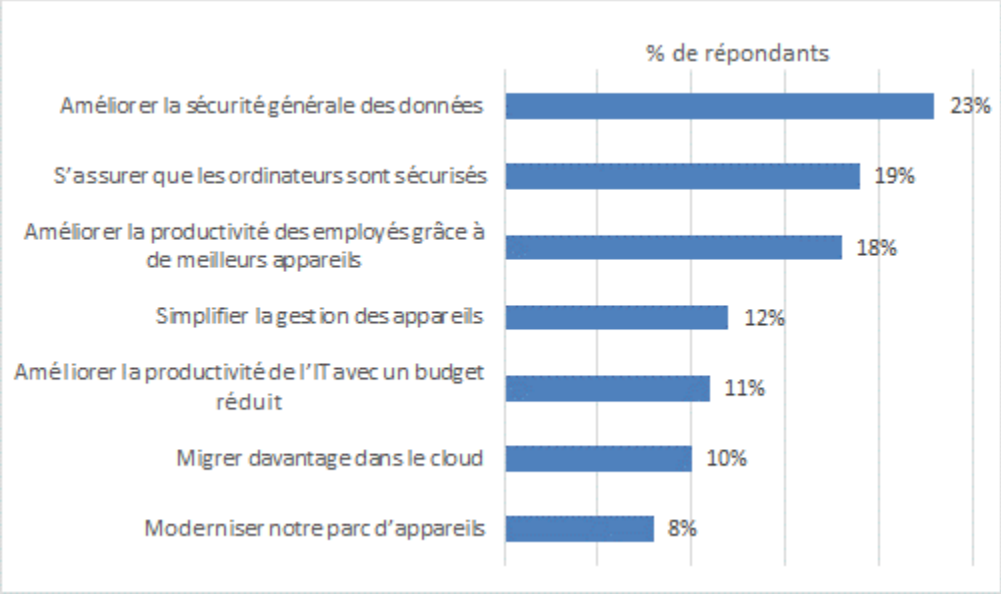
Lorsque les décideurs IT ont été interrogés sur le principal critère de choix pour un nouveau fournisseur d'ordinateurs, la sécurité est arrivée en première position devant les performances, le support pour les applications utilisées et l'intégration avec l'infrastructure en place. Il convient surtout de noter que les spécifications sont considérées comme un critère peu important.

Le Graphique 1 résume les priorités des décideurs IT. Le Graphique 2 indique les principaux critères de choix d'un fournisseur d'ordinateurs.

GRAPHIQUE 1

Principales priorités informatiques : sécurité des données et ordinateurs

Q. Parmi les différents domaines énoncés ci-après, quels sont ceux que vous considérez comme prioritaires ?



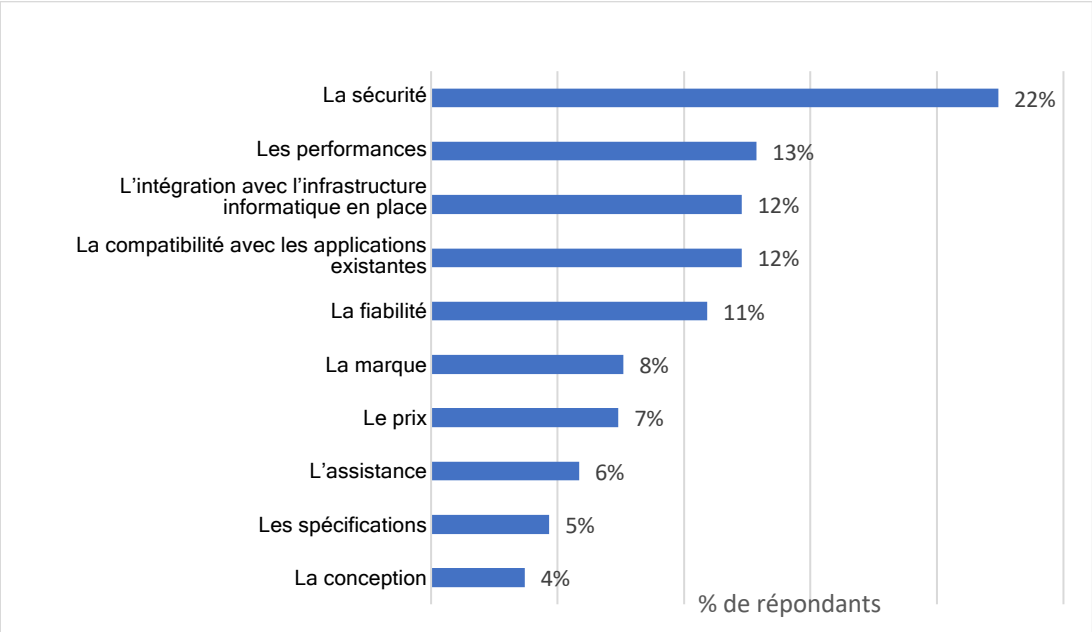
Source : Secure Endpoint Survey, IDC, n = 513

Remarque : Les données mentionnées sont basées sur la principale priorité (priorité n° 1) indiquée par les répondants

GRAPHIQUE 2

Principaux critères de choix d'un fournisseur d'ordinateurs

Q. Quels sont les critères qui vous semblent les plus importants dans le choix d'un ordinateur pour votre entreprise ?



Source : Secure Endpoint Survey, IDC, n = 513

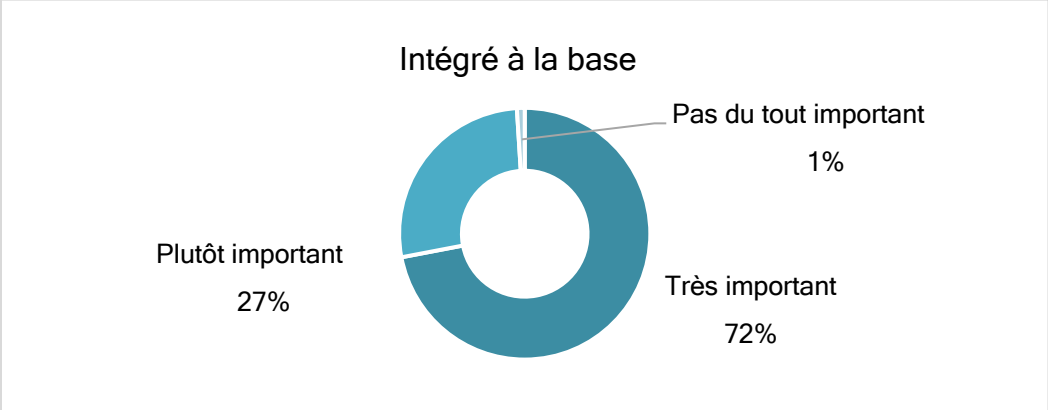
Remarque : Les données mentionnées sont basées sur la principale priorité (priorité n° 1) indiquée par les répondants

L'intégration de la sécurité et de la protection des données ont été les plus citées par les répondants. À la question « Quelle importance accordez-vous à l'intégration de mécanismes de sécurité dans les ordinateurs, y compris au niveau du processeur, du firmware et de l'OS, afin de les protéger contre les menaces actuelles et celles de demain ? », les réponses allaient clairement dans le sens d'une telle intégration, 72% des répondants ayant affirmé qu'elle était très importante et 27% qu'elle était plutôt importante. Seulement 1% des répondants a affirmé qu'elle n'était pas importante du tout. En examinant de plus près les réponses obtenues, on constate que la sécurité intégrée est plus souvent considérée comme un critère très important dans le secteur de la santé (84%) et celui de la finance (75%). Les réponses obtenues concernant la protection des données sont similaires. Lorsque nous avons demandé aux répondants s'ils estimaient que l'intégration de fonctionnalités de chiffrement des données au sein des ordinateurs était importante, 71% d'entre eux ont répondu qu'elle était très importante, 29% qu'elle était plutôt importante et aucun (0%) qu'elle n'était pas importante. Pour plus de détails sur l'importance accordée à l'intégration de la sécurité et du chiffrement des données, voir le Graphique 3.

GRAPHIQUE 3

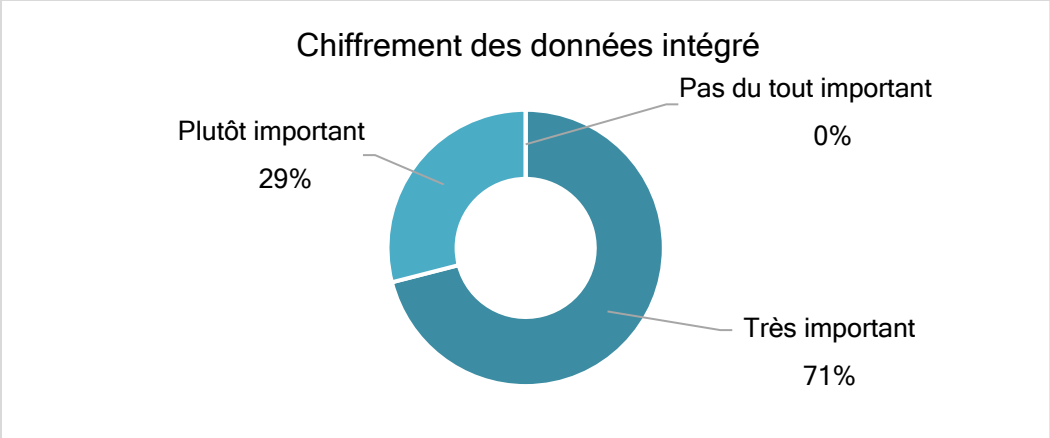
Importance de l'intégration de la sécurité et du chiffrement des données

Q. Quelle importance accordez-vous à l'intégration de mécanismes de sécurité dans les ordinateurs, y compris au niveau du processeur, du firmware et de l'OS, afin de les protéger contre les menaces actuelles et celles de demain ?



Source : Secure Endpoint Survey, IDC, n = 513

Q. Quelle importance accordez-vous à l'intégration de fonctionnalités de chiffrement des données au sein des ordinateurs ?



Source : Secure Endpoint Survey, IDC, n = 513

Bien qu'il soit important d'intégrer des mécanismes de sécurité ainsi que des fonctionnalités de chiffrement des données dans les ordinateurs, les experts en sécurité savent que le maillon faible de tout système de sécurité sont les utilisateurs eux-mêmes. Pour cette raison, l'authentification des utilisateurs est particulièrement importante et les fournisseurs se sont efforcés de progresser dans ce domaine. Malheureusement, les résultats de l'enquête montrent que de nombreuses entreprises ont pris du retard dans ce domaine.

Malgré tout, 68% des répondants ont affirmé que leur entreprise exigeait d'utiliser des mots de passe complexes et 63% ont affirmé qu'ils utilisaient des systèmes d'authentification à deux facteurs. En revanche, seulement 23% utilisent un système d'authentification unique (SSO) et seulement 20% utilisent des systèmes de sécurité biométriques (empreinte digitale ou reconnaissance faciale). Il convient également de noter que 56% des répondants ont déclaré que l'authentification biométrique était beaucoup plus sûre que l'authentification par mot de passe, 35% ont affirmé qu'elle était un peu plus sûre, 9% qu'elle était aussi sûre et aucun qu'elle était moins sûre.

Récemment, une nouvelle technologie d'authentification a fait son apparition : la clé d'accès. Une clé d'accès (ou passkey en anglais) est un système d'identification numérique reposant sur l'utilisation de clés étroitement associées et garantissant une meilleure sécurité que les mots de passe. Étant donné que cette technologie est encore récente, seulement 14% des répondants l'utilisent, mais les autres décideurs IT devraient s'y intéresser. Le Graphique 4 donne plus de détails sur les systèmes d'authentification utilisés.

GRAPHIQUE 4

Méthodes d'authentification des utilisateurs

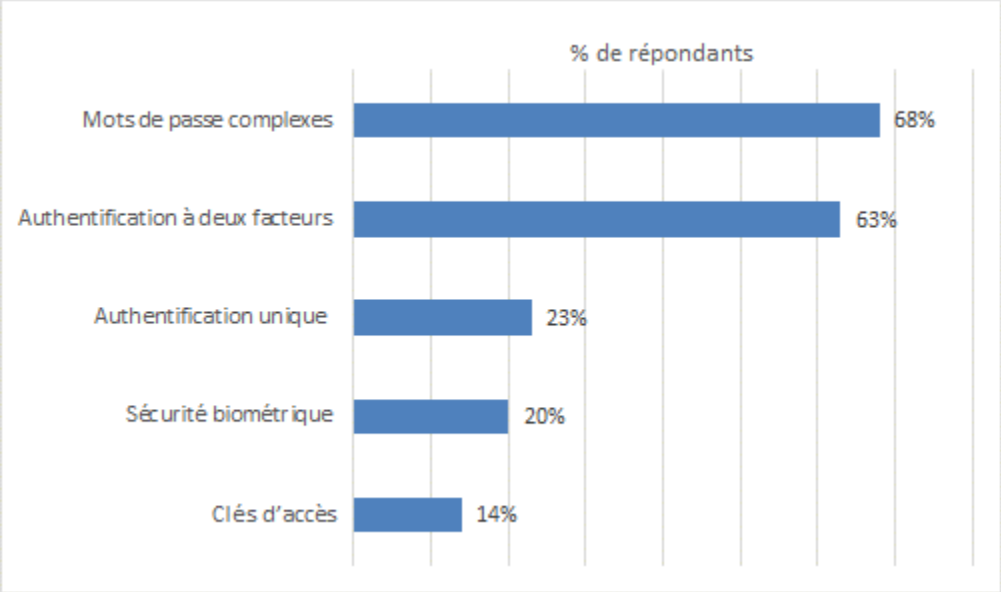
Q1. Votre entreprise exige-t-elle de ses salariés qu'ils utilisent des mots de passe complexes pour se connecter à leur ordinateur ?

Votre entreprise met-elle actuellement à disposition des ordinateurs dotés d'un système de sécurité biométrique, tel qu'un lecteur d'empreintes digitales ?

Q3. Votre entreprise a-t-elle commencé à étudier les avantages des clés d'accès ?

Q4. Votre entreprise exige-t-elle l'utilisation d'une méthode d'authentification à deux facteurs ?

Q5. Votre entreprise utilise-t-elle un système d'authentification unique (SSO) ? (oui/non)



Source : Secure Endpoint Survey, IDC, n = 513

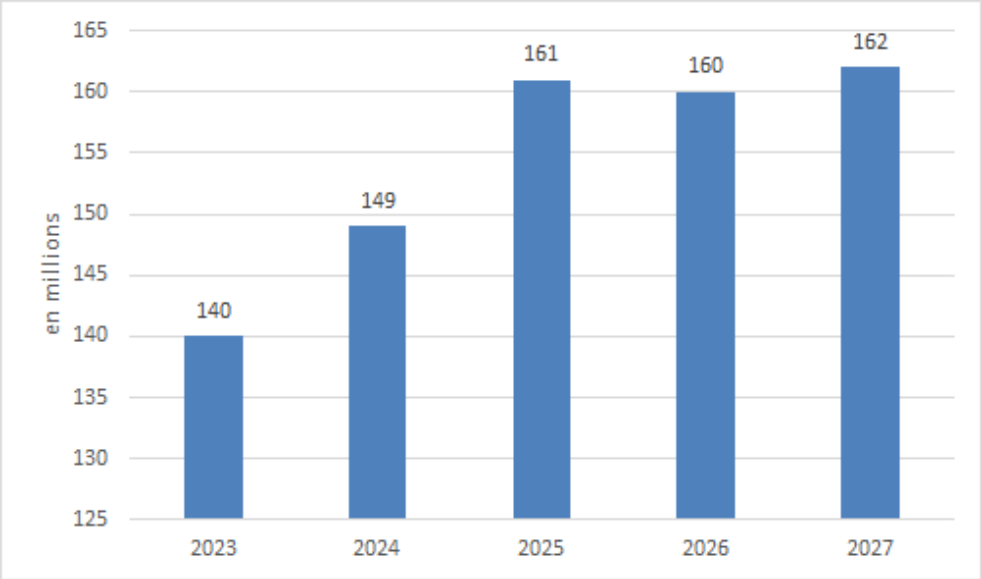
Pourcentage de réponses affirmatives

Parmi les répondants, un nombre incroyablement élevé d'entre eux n'a même pas mis en place un protocole d'authentification de base, c'est-à-dire une authentification par mot de passe complexe (32%) ou une authentification à deux facteurs (37%). **L'une des meilleures pratiques à respecter** consiste à s'assurer que l'entreprise impose une méthode d'authentification à tous les niveaux. Une fois cette base établie, il sera possible d'envisager une authentification SSO associée à un protocole d'authentification solide. Enfin, lors du prochain renouvellement des machines, il conviendra d'étudier la possibilité d'utiliser des ordinateurs capables de prendre en charge des méthodes d'authentification plus sûres, telles que des systèmes biométriques ou des clés d'accès. Grâce à une authentification biométrique et l'utilisation de clés d'accès, les salariés pourront rapidement se connecter en toute sécurité à leur ordinateur, puis accéder immédiatement à leurs applications et à des sites Web.

Le prochain renouvellement d'ordinateurs est le dernier point que nous souhaitions aborder sur ce sujet. De nombreuses entreprises disposent d'un parc de machines vieillissantes qui doivent être remplacées. Même si une partie importante des ordinateurs utilisés a été achetée en 2020, ces machines auront bientôt plus de quatre ans. Depuis cette date, des progrès ont été réalisés dans le domaine de la sécurité matérielle afin de lutter contre les menaces modernes. Par ailleurs, la plupart de ces ordinateurs ont été achetés avant la généralisation du travail à distance et hybride, ce qui signifie qu'ils ne disposent généralement pas d'une caméra, d'un microphone et de haut-parleurs d'une qualité suffisante pour les applications de conférence et de collaboration web devenues aujourd'hui indispensables. Après plusieurs années de fléchissement, le marché des ordinateurs personnels devrait connaître une nouvelle phase de croissance selon les prévisions issue du Personal Computing Device Tracker d'IDC. Remarque : Les « unités commerciales » sont des ordinateurs achetés par des organisations ou des personnes autres que des consommateurs. Pour consulter les prévisions de vente d'ordinateurs commerciaux d'IDC, voir le Graphique 5.

GRAPHIQUE 5

Prévisions de ventes d'ordinateurs commerciaux dans le monde



Source : IDC PCD Tracker, août 2023

Pour rester compétitives sur le marché et attirer/retenir les meilleurs talents, les entreprises doivent réévaluer régulièrement les besoins en ordinateurs de leurs salariés. Si les équipes IT devaient autrefois trouver un juste milieu entre la sécurité et la satisfaction des collaborateurs, il est aujourd'hui possible de ne faire aucun compromis en choisissant le bon fournisseur d'ordinateur. Enfin, la mise en place des principes de l'accès zero trust peut également être envisagée **en tant que meilleure pratique** lors du déploiement de nouveaux ordinateurs. Cette stratégie de sécurité part du principe qu'on ne peut faire confiance à aucun appareil qui tente d'accéder aux ressources de l'entreprise avant de l'avoir vérifié. Le modèle zero trust utilise des technologies et des processus permettant d'attester de l'état de sécurité d'un appareil (de manière optimale, depuis le processeur jusqu'aux applications et logiciels de sécurité), du réseau (p. ex., réseau public Wi-Fi ou réseau privé) et de l'identité de l'utilisateur.

Envisager d'utiliser des Mac dans l'entreprise

De plus en plus de départements IT acceptent aujourd'hui que des Mac soient utilisés pour les raisons mises en exergue par l'enquête d'IDC. Parmi les répondants qui prennent en charge plusieurs OS différents, 76% estiment que les Mac sont plus sécurisés que les autres ordinateurs. De plus, au cours des 12 prochains moins, la principale raison qui les conduira à acheter un plus grand nombre de Mac est liée au fait qu'ils estiment que les Mac sont plus sécurisés (47%) et qu'ils sont plus faciles à déployer et à gérer (36%).

Apple s'attache à fournir une expérience client d'une qualité exceptionnelle, tout en renforçant la sécurité de ses appareils grâce à l'intégration de mécanismes de sécurité dans ses processeurs et ses logiciels. Par exemple, la fonctionnalité Touch ID est un mécanisme de sécurité biométrique intégré. Secure Enclave est un système de sécurité intégré aux processeurs Apple qui permet de chiffrer et de protéger le code d'accès utilisé pour sécuriser les données de Touch ID.

Témoignage d'un client d'Apple

« L'intégration des fonctions de confidentialité et de sécurité dans le produit lui-même est l'une des caractéristiques les plus importantes des produits d'Apple. Ces fonctions ne sont pas le fruit d'une réflexion après coup et c'est ce que nous apprécions tout particulièrement. » — Linda Jojo, Vice-présidente exécutive et directrice de la clientèle de United Airlines

Pour lutter contre les risques de compromission du système d'exploitation et des séquences de démarrage, les Mac sont équipés des utilitaires Secure Boot et Signed System Volume. Secure Boot permet de s'assurer que seule la version cryptographiquement certifiée de macOS est lancée au démarrage et Signed System Volume protège l'intégrité de l'OS pendant son exécution. Les logiciels obsolètes représentent également un risque de cybersécurité qu'Apple cherche à minimiser en automatisant et en sécurisant de bout en bout le déploiement et l'installation des mises à jour des logiciels.

Certains logiciels jouent un rôle essentiel dans la productivité des collaborateurs, mais ils doivent également ne contenir aucun malware. Pour lutter contre les malwares, Apple a choisi d'intégrer la sécurité sur plusieurs couches. Le Mac App Store d'Apple analyse chaque application afin de détecter la présence éventuelle de malwares. Depuis que les logiciels utilisés sur Mac peuvent également être téléchargés depuis le Web, Apple exige des développeurs qu'ils soumettent leurs applications à son service de notarisation qui analyse également les applications pour rechercher tout malware potentiel. La fonction Gatekeeper intégrée à macOS permet de vérifier que le logiciel a bien été notarisé et empêche l'exécution d'applications non signées. De plus, Xprotect, l'outil anti-malware d'Apple, bloque et supprime tout logiciel malveillant connu.

Les données font partie des actifs les plus précieux des entreprises et doivent être protégées en conséquence. L'association du chiffrement FireVault assisté par une puce, des protocoles VPN pris en charge par Apple et du chiffrement de bout en bout intégré aux services d'Apple (p. ex., iMessage et iCloud) garantit que les données sont protégées lorsqu'elles sont au repos, en mouvement et en cours d'utilisation.

Les hackers étant particulièrement doués en ingénierie sociale, les utilisateurs doivent se montrer particulièrement vigilants face à ce type de menace. Apple les aide dans cette tâche difficile grâce aux notifications déclenchées dans Safari lorsqu'ils se rendent sur un site Web frauduleux. En outre, les identifiants d'authentification étant la principale cible des tentatives de vol, les entreprises pourront utiliser les clés d'accès d'Apple pour moderniser leurs systèmes d'authentification, sans sacrifier l'expérience utilisateur.

Un système de sécurité renforcé n'a de sens que si les appareils sont correctement gérés. C'est pourquoi Apple propose différents outils pour la gestion des appareils, y compris un cadre de gestion intégré avec une solution de gestion des appareils mobiles (MDM). Apple Business Manager permet de déployer automatiquement les appareils et de les associer à des solutions MDM et les API de sécurité des ordinateurs pour Mac permettent aux développeurs de construire des solutions destinées à suivre, analyser et contrer les menaces de sécurité. Apple propose également des intégrations pour la gestion des identités à l'aide d'un cadre d'authentification SSO qui fonctionne avec les fournisseurs d'identités (IdP) les plus récents.

Enfin, Apple fournit ces fonctionnalités de sécurité pour macOS, y compris les mises à jour des logiciels mineures et majeures, sans aucun coût supplémentaire pour les entreprises ou les particuliers.

DEFIS/OPPORTUNITES

Malgré des risques en constante évolution, le département IT doit en faire plus avec moins : moins d'argent, moins de personnel et moins de ressources. Outre la nécessité de gérer le risque de sécurité permanent, de nombreux départements IT sont également chargés d'améliorer la productivité et la satisfaction des salariés au moyen du matériel, des logiciels et des services mis à leur disposition. Au premier abord, ces deux tâches simultanées (renforcement de la sécurité et amélioration de la productivité et de la satisfaction des salariés) peuvent sembler insurmontables. Mais elles constituent également une formidable opportunité pour le département IT. Ce dernier aura en effet l'occasion de reconsidérer le matériel, les logiciels et les services à acheter, les fournisseurs avec lesquels travailler ainsi que les modalités de déploiement de ces ressources auprès d'un personnel de plus en plus hybride. En outre, il est grand temps de revoir les modes de calcul du coût total de possession (TCO) afin que celui-ci corresponde davantage aux pratiques actuelles en matière d'achat et d'utilisation des technologies.

CONCLUSION

La sécurité est et restera l'une des principales préoccupations du département IT. À l'heure où les budgets IT sont limités et une partie importante du matériel doit être prochainement renouvelée, les entreprises ont intérêt à se demander quel fournisseur mérite leur argent. Songez à mettre en œuvre les meilleures pratiques en matière d'authentification et de déploiement automatique et à acheter le matériel qui vous le permettra. Ne privilégiez pas la sécurité au détriment de la productivité et de la satisfaction des collaborateurs, alors qu'il existe des fournisseurs proposant des ordinateurs intégrant des fonctions de sécurité et de chiffrement des données sur lesquelles vous pouvez compter pour garantir à la fois la sécurité et une expérience utilisateur positive

À propos d'IDC

IDC est un acteur majeur de la recherche, du conseil et de l'événementiel sur les marchés des technologies de l'information, des télécommunications et des technologies grand public. IDC aide les professionnels évoluant sur les marchés informatiques et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1 100 analystes d'IDC proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologiques dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs. IDC est une filiale d'IDG, leader mondial dans les domaines des médias, de la recherche et des événements liés à la technologie.

Siège social mondial :

140 Kendrick Street
Building B
Needham, MA 02494, États-Unis
États-Unis
+1.508.872.8200
Twitter : @IDC
blogs.idc.com
www.idc.com