Livre blanc

Le besoin absolu de sécuriser les terminaux

Commandité par : Apple

Tom Mainelli Michael Suby
Septembre 2023

LE POINT DE VUE D'IDC

La sécurité est une préoccupation si importante qu'elle empêche les décideurs informatiques de dormir la nuit. Ces derniers sont conscients que toute l'entreprise peut être compromise du jour au lendemain à cause d'une faille de sécurité, et ce, même si elle est parfaitement gérée et que ses produits ou services sont appréciés.

Malheureusement, le monde n'est pas plus sûr aujourd'hui qu'il l'était auparavant. 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, les départements informatiques doivent rester vigilants, tout en acceptant de travailler avec de nouveaux fournisseurs et de nouvelles technologies pour garantir la sécurité des employés, des clients et de leurs données.

La liste des défis auxquels les services d'informatique doivent faire face est longue, des centres de données aux terminaux (les ordinateurs), en passant par les réseaux qui les connectent et les logiciels qui les font fonctionner. Le présent livre blanc souligne l'importance de sécuriser les terminaux. En effet, la sécurité des centres de données, des réseaux et des logiciels n'a de sens que si les terminaux sont sécurisés.

Généralement, un terminal sécurisé nécessite 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 protection des terminaux. Toutefois, même lorsque les appareils sont verrouillés, les utilisateurs trouvent souvent le moyen de contourner les systèmes de sécurité afin d'accomplir leur travail. Et quand la sécurité pose problème aux utilisateurs, elle devient contre-productive.

Grâce aux avancées technologiques, il devient possible de préserver l'expérience utilisateur sans compromettre la sécurité. Les progrès réalisés en matière de détection des maliciels, 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.

MÉTHODOLOGIE

En juillet 2023, IDC a réalisé une enquête en ligne auprès de décideurs informatiques des États-Unis et du Canada afin de connaître leur point de vue sur la sécurité en général et, plus précisément, sur l'importance de la sécurisation des terminaux. Les répondants représentaient diverses entreprises d'au moins 500 employés œuvrant dans différents secteurs d'activité. Ces entreprises avaient recours à plusieurs systèmes d'exploitation, y compris Microsoft Windows, Apple macOS et Google ChromeOS. Les décideurs informatiques interrogés étaient responsables de sélectionner, d'acheter

ou de déployer des logiciels de sécurité pour leur entreprise, ou de superviser d'autres personnes ayant cette responsabilité.

SURVOL DE LA SITUATION

La sécurité demeure une priorité absolue pour la haute direction des entreprises. Les organisations avant-gardistes savent que la sécurité n'est pas une option. Il s'agit plutôt d'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 informatiques travaillant dans des entreprises d'au moins 500 employés, révèle que plus de 50 % des organisations interrogées partout dans le monde ont été victimes d'une attaque par rançongiciel ayant perturbé leurs activités au cours des 12 derniers mois. Plus d'un tiers d'entre elles ont affirmé que cette attaque avait nui à leurs activités pendant au moins une semaine. Malgré des protocoles de sécurité renforcés, les grandes entreprises ne sont pas épargnées par ce type d'attaques. Au contraire, les organisations les plus fortement touchées sont celles qui comptent de 1 000 à 2 499 employés (71 %), de 2 500 à 4 999 employés (72 %) et de 5 000 à 9 999 employés (70 %). Autrement dit, aucune entreprise n'est à l'abri.

Selon cette même étude, les terminaux constituent le principal point d'entrée des attaques par rançongiciel. Les points de compromission initiaux comprennent les navigateurs web (21 %), les supports amovibles (18 %), les pièces jointes aux courriels (17 %), les chaînes d'approvisionnement (17 %), les URL figurant dans les courriels (14 %) et les accès internes (8 %).

En raison du nombre croissant d'employés travaillant à distance ou dans des conditions hybrides, les rançongiciels et autres menaces de sécurité sont devenus plus difficiles à gérer pour les services de TI. Selon l'enquête Endpoint Security Survey menée en décembre 2022 par IDC, le personnel de 97 % des entreprises travaille à distance. Bien qu'on s'attende à ce que ce chiffre diminue au cours des 12 prochains moins, il restera très élevé à court terme.

Alors que les entreprises cherchent des solutions pour répondre au défi incessant que représente le travail à distance, les modèles à vérification systématique gagnent du terrain. Les meilleures pratiques consistent à établir une norme de base pour les contrôles de sécurité, puis à mettre en place une protection avancée pour les terminaux, 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.

Étant donné tout ce qui précède, il n'est pas surprenant de constater que les répondants à l'enquête d'IDC ont très majoritairement choisi de prioriser le renforcement de la protection générale des données ainsi que la sécurisation des ordinateurs (voir figure 1).

On constate également dans le schéma ci-dessous que l'amélioration de la productivité des employés grâce à l'utilisation de meilleurs appareils constitue la troisième priorité informatique. Des trois principales priorités choisies par les répondants, l'utilisation de meilleurs appareils est celle la plus souvent citée. Le message à retenir est clair : la sécurité est importante, mais elle ne doit pas faire obstacle à la productivité. De plus, les meilleurs appareils doivent être équipés de systèmes de sécurité renforcés qui n'interfèrent pas avec le travail du personnel.

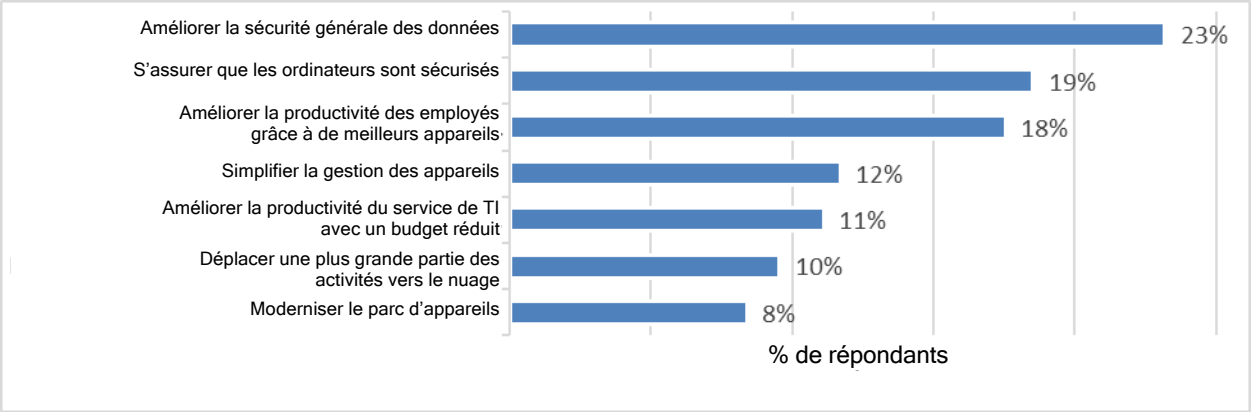
Lorsqu'interrogés sur le principal critère qu'ils prendraient en considération s'ils devaient choisir un nouveau fournisseur d'ordinateurs, les décideurs informatiques ont opté pour la sécurité, devant les performances, la prise en charge des applications utilisées et l'intégration avec l'infrastructure en place. Il convient par ailleurs de noter que les caractéristiques techniques des appareils étaient considérées comme un critère peu important.

La figure 1 résume les principales priorités des décideurs informatiques. La figure 2 indique les principaux critères pris en considération dans le choix d'un fournisseur d'ordinateurs.

FIGURE 1

Principales priorités informatiques : sécurité des données et des terminaux

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



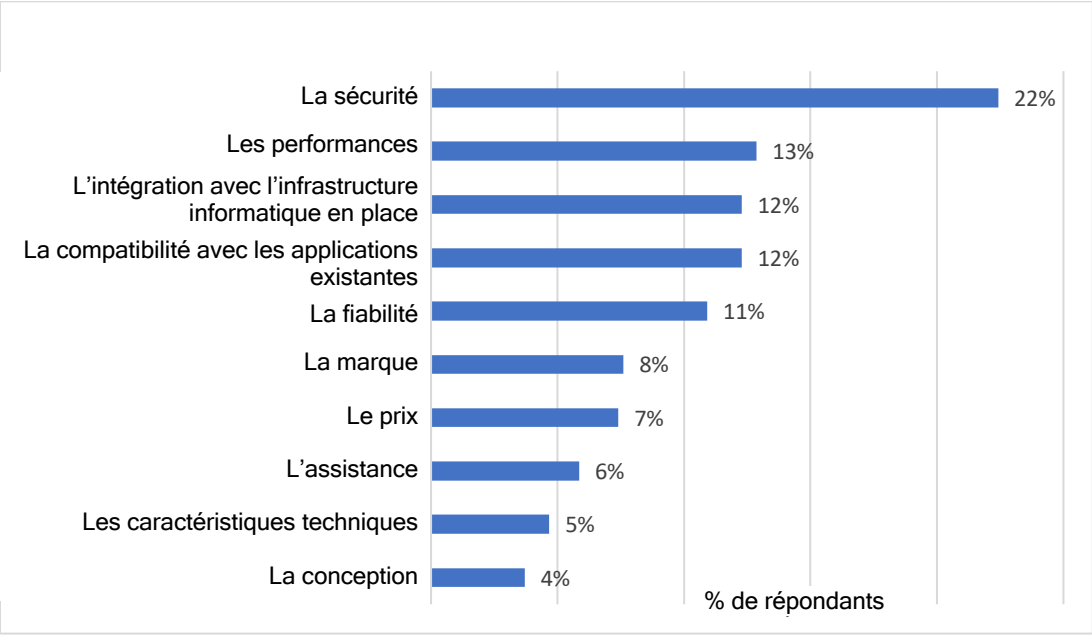
Source : Secure Endpoint Survey, IDC, n = 513

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

FIGURE 2

Principaux critères pris en considération dans le 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

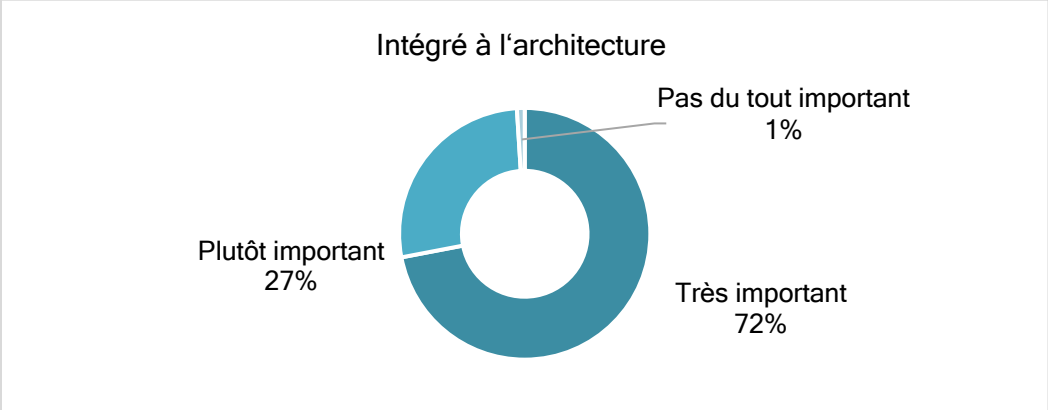
Remarque : Les données mentionnées sont basées sur la principale priorité (priorité n° 1) indiquée par les répondants

La sécurité et la protection des données intégrées ont souvent été citées par les répondants. En effet, à la question « Quelle importance accordez-vous à l'intégration de mécanismes de sécurité à même les composants (notamment la puce, le micrologiciel et le système d'exploitation) des ordinateurs pour les protéger contre les menaces actuelles et celles de demain? », 72 % des répondants ont affirmé que l'intégration était très importante et 27 % qu'elle était plutôt importante. Seulement 1 % des répondants ont déclaré qu'elle n'était pas importante du tout. En examinant de plus près les réponses recueillies, on remarque que la sécurité intégrée est plus souvent considérée comme un critère très important dans le secteur des soins de santé (84 %) et 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 capacités de chiffrement des données à même l'architecture 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, consulter la figure 3.

FIGURE 3

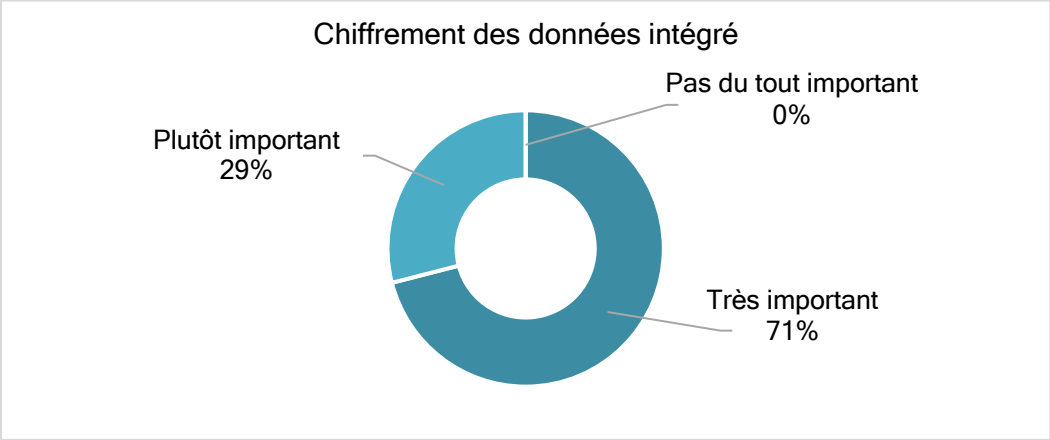
Importance de la sécurité et du chiffrement des données intégrés

Q. Quelle importance accordez-vous à l'intégration de mécanismes de sécurité à même les composants (notamment la puce, le micrologiciel et le système d'exploitation) des ordinateurs pour 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 capacités de chiffrement des données à l'architecture des ordinateurs?



Source : Secure Endpoint Survey, IDC, n = 513

Bien qu'il soit important d'intégrer des mécanismes de sécurité et des capacités de chiffrement des données à l'architecture des ordinateurs, les experts savent que le maillon faible de tout système de sécurité est l'utilisateur lui-même. L'authentification des utilisateurs est donc particulièrement importante. Heureusement, les fournisseurs se sont efforcés de progresser dans ce domaine. Or, les résultats de l'enquête démontrent que de nombreuses entreprises ont pris du retard à cet égard.

Malgré tout, 68 % des répondants ont affirmé que leur entreprise exigeait l'emploi de mots de passe complexes, et 63 % ont révélé avoir recours à des systèmes d'authentification à deux facteurs. En revanche, seulement 23 % utilisaient un système d'authentification unique et 20 % faisaient appel à des systèmes de sécurité biométriques (empreinte digitale ou reconnaissance faciale). Soulignons aussi 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 n'était pas plus 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 est un système d'identification numérique reposant sur l'utilisation de clés étroitement associées et garantissant une meilleure sécurité que les mots de passe. Puisque cette technologie est encore récente, seulement 14 % des répondants s'en servent, mais les autres décideurs informatiques devraient s'y intéresser. La figure 4 donne plus de détails sur les systèmes d'authentification utilisés.

FIGURE 4

Méthodes d'authentification des utilisateurs

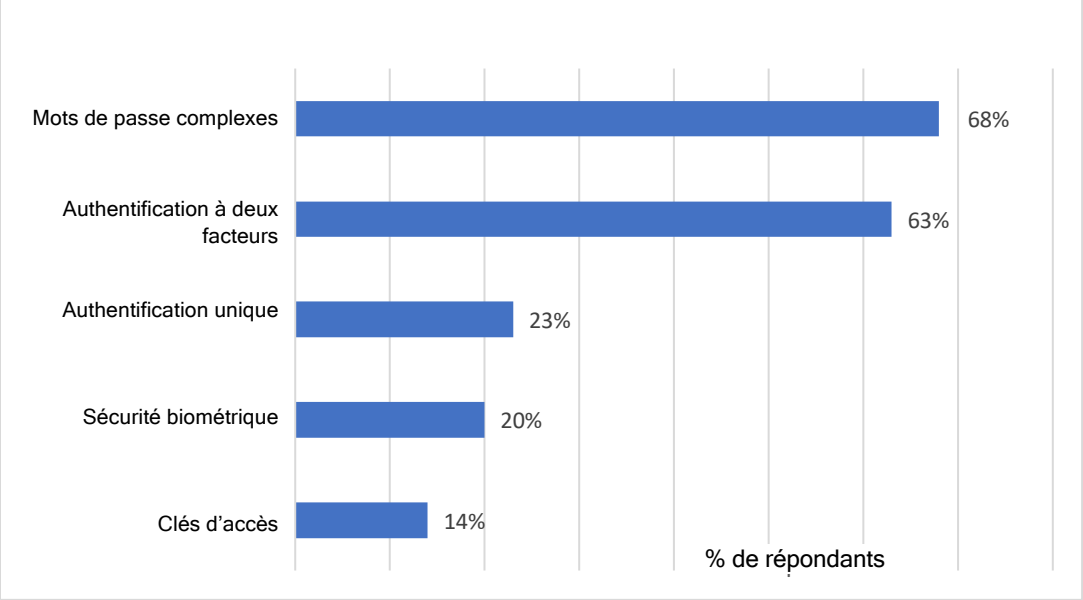
Q1. Votre entreprise exige-t-elle de ses employés qu'ils utilisent des mots de passe complexes pour se connecter à leur ordinateur?

Q2. 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? (Oui/Non)



Source : Secure Endpoint Survey, IDC, n = 513

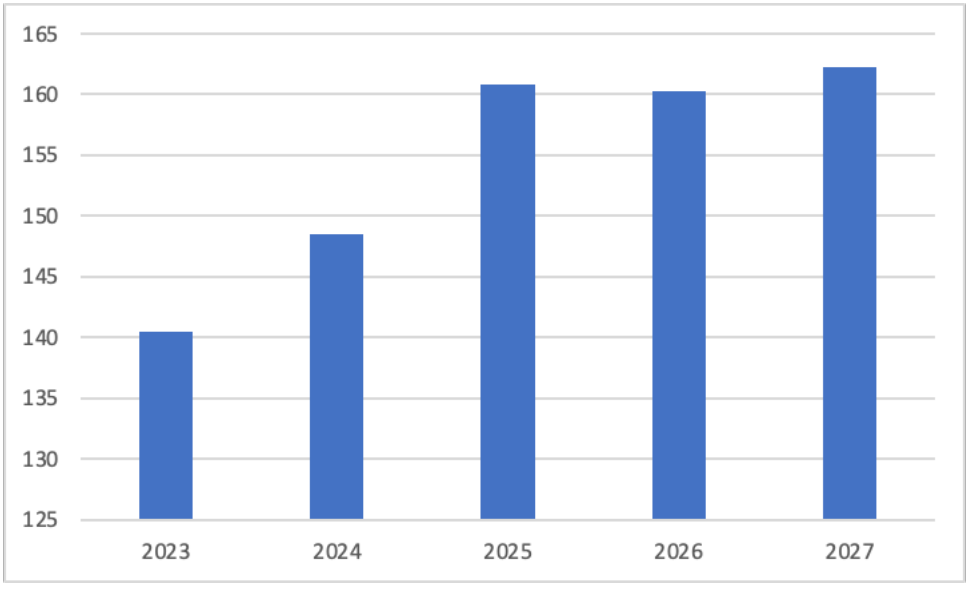
Pourcentage de réponses affirmatives

Un nombre incroyablement élevé de répondants n'avaient 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 cohérente à tous les niveaux. Une fois cette base établie, il sera possible d'envisager une authentification unique associée à un protocole d'authentification-cadre suffisamment solide. Enfin, lors du prochain renouvellement d'appareils, 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 employés 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. De nombreuses entreprises disposent d'un parc d'appareils vieillissants qui doivent être remplacés. Même si une partie importante des terminaux ont été achetés en 2020, ces machines auront bientôt plus de quatre ans. Depuis leur achat, 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 acquis 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 en ligne devenues aujourd'hui indispensables. Après plusieurs années de fléchissement, le marché des ordinateurs personnels devrait connaître une nouvelle phase de croissance selon les prévisions du Personal Computing Device Tracker d'IDC. Remarque : Les « unités commerciales » sont des ordinateurs achetés par des organisations ou des personnes autres que les consommateurs. Pour consulter les prévisions de vente d'ordinateurs commerciaux d'IDC, consulter la figure 5.

FIGURE 5

Prévisions de ventes d'ordinateurs commerciaux à l'échelle mondiale



Source : IDC PCD Tracker, août 2023

Pour rester concurrentielles sur le marché, en plus d'attirer et de retenir les meilleurs talents, les entreprises doivent régulièrement réévaluer les besoins informatiques de leurs employés. Si les entreprises devaient autrefois trouver un juste milieu entre la sécurité et la satisfaction des employés, il est aujourd'hui possible de ne faire aucun compromis en choisissant le bon fournisseur. Enfin, la mise en pratique des principes d'accès à vérification systématique peut également être envisagée **en tant que meilleure pratique** lors du déploiement de nouveaux ordinateurs. Cette stratégie de sécurité repose sur l'idée 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 à vérification systématique a recours à des technologies et des processus permettant d'attester de l'état de sécurité d'un appareil (de manière optimale, depuis la puce jusqu'aux applications informatiques et logiciels de sécurité critiques), du réseau (p. ex., réseau public Wi-Fi ou réseau privé) et de l'identité de l'utilisateur.

Envisager d'utiliser Mac en entreprise

De plus en plus de départements informatiques acceptent aujourd'hui que Mac soit utilisé pour les raisons mises en évidence par l'enquête d'IDC. Parmi les répondants prenant en charge différents systèmes d'exploitation, 76 % estiment que Mac est plus sécuritaire que les autres ordinateurs. Par ailleurs, au cours des 12 prochains moins, la principale raison qui les conduira à se procurer un plus grand nombre de Mac sont : le fait qu'ils considèrent que Mac est plus sécuritaire (47 %) et qu'il est plus facile à déployer et à gérer (36 %).

Apple a pour objectif de fournir une expérience client d'une qualité exceptionnelle, tout en renforçant la sécurité de ses appareils en intégrant des mécanismes de sécurité à ses puces et ses logiciels. Par exemple, la fonctionnalité Touch ID est un mécanisme de sécurité biométrique intégré. Secure Enclave quant à lui, est un système de sécurité intégré aux puces 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, Mac intègre des fonctionnalités comme le démarrage sécurisé et le volume système signé. Le démarrage sécurisé permet de s'assurer que seule la version cryptographiquement certifiée de macOS est lancée au démarrage, et le volume système signé protège l'intégrité du système d'exploitation pendant son exécution. Les logiciels obsolètes représentent également un risque de cybersécurité qu'Apple cherche à réduire en automatisant et en sécurisant de bout en bout le déploiement et l'installation des mises à jour logicielles.

Certains logiciels tiers jouent un rôle essentiel dans le travail des employés. Il est toutefois important de veiller à ce qu'ils ne contiennent aucun maliciel. Pour lutter contre les maliciels, Apple a choisi d'opter pour la sécurité multicouche. Le Mac App Store d'Apple analyse chaque application afin de détecter la présence éventuelle de maliciels. Comme 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 examine également les applications pour rechercher tout maliciel potentiel. La fonctionnalité 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-maliciel 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 transit ou en cours d'utilisation.

Puisque les acteurs malveillants sont particulièrement doués en ingénierie sociale, les utilisateurs doivent se montrer vigilants face à ce type de menace. Apple les aide dans cette tâche difficile grâce aux avertissements déclenchés dans Safari lors de la visite d'un site web frauduleux. En outre, les identifiants d'authentification étant la principale cible des tentatives de vol, les entreprises peuvent utiliser les clés d'accès d'Apple pour moderniser leurs systèmes d'authentification, sans porter préjudice à 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 (GAM). Apple Business Manager permet de déployer automatiquement les appareils et de les associer à des solutions de GAM, et les API de sécurité des terminaux pour Mac permettent aux développeurs de construire des solutions destinées à surveiller, 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 unique pris en charge par les fournisseurs d'identités les plus récents.

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

DÉFIS/OCCASIONS

Malgré des risques en constante évolution, les services d'informatique doivent 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 nombreuses équipes de TI sont également chargées d'améliorer la productivité et la satisfaction des employés 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 employés) peuvent sembler insurmontables. Mais elles constituent également une formidable opportunité. Les personnes responsables auront en effet l'occasion de reconsidérer le matériel, les logiciels et les services qu'elles ont intérêt à acheter, les fournisseurs avec lesquels elles peuvent travailler ainsi que les modalités de déploiement de ces ressources auprès d'une main-d'œuvre de plus en plus hybride. Finalement, il est grand temps de revoir les modes de calcul du coût total de possession (CTP) 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 des services de TI. À l'heure où les budgets informatiques sont limités et une partie importante du matériel doit être 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 employés, 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 convaincante.

À propos d'IDC

IDC est un important acteur de la recherche, du conseil et de l'événementiel sur les marchés des technologies de l'information, des télécommunications et des technologies grand public. L'entreprise 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 internationale, régionale et locale sur les occasions et les tendances technologiques dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC offre des analyses stratégiques pour aider ses clients à atteindre leurs objectifs clés. IDC est une filiale d'IDG, chef de file 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
+ 1 508 872-8200
Twitter : @IDC
blogs.idc.com
www.idc.com

Mentions de droit d'auteur

Publication externe des données et informations d'IDC – toute information d'IDC destinée à être utilisée dans le cadre de publicités, de communiqués de presse ou de supports promotionnels doit préalablement faire l'objet du consentement écrit du vice-président ou du directeur du bureau local d'IDC concerné. Une ébauche du document proposé doit accompagner une telle demande. IDC se réserve le droit de refuser l'approbation de toute utilisation externe, quelle qu'en soit la raison.

Droit d'auteur 2023 IDC. Toute reproduction sans autorisation écrite est strictement interdite.