jamf

Security 360 :
Rapport annuel sur les tendances

Introduction

L'année dernière, nous avons étudié l'impact de l'adoption des technologies de télétravail sur la posture de sécurité des entreprises au niveau mondial. À l'époque, de nombreuses organisations étaient encore en train de migrer vers des environnements de travail distants et hybrides. Cette année, nous mettons l'accent sur les évolutions du paysage des menaces et le risque que représentent ces tendances pour votre organisation.

Chaque année, le **Jamf Threat Labs** analyse les menaces qui pèsent sur les appareils utilisés sur le lieu de travail moderne. Le télétravail reste de mise, et notre perspective sur le paysage des menaces continue d'évoluer pour rester à la hauteur des exigences de conformité des terminaux et garantir la sécurité des données tout en préservant la vie privée des utilisateurs.

Le rapport de cette année explore cinq grandes tendances de sécurité qui concernent directement les organisations. En effet, les utilisateurs se connectant à distance à une multitude d'applications et de services hébergés dans des centres de données privés et publics, à l'aide d'un éventail d'appareils mobiles multiplateformes.

Les tendances de 2023 abordent :

Tendance 1 : L'ingénierie sociale reste la principale menace.

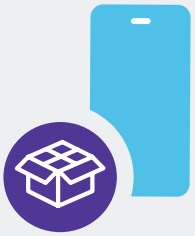
L'ingénierie sociale, et plus particulièrement les attaques par phishing, figure en tête de liste des principales menaces pour la cybersécurité. La généralisation du télétravail et la simplicité relative des campagnes de phishing forment un mélange explosif qui permet à de nombreux acteurs malveillants d'obtenir les identifiants des utilisateurs. Ces types d'attaque permettent aux utilisateurs non autorisés de s'approprier « les clés du royaume », selon l'expression consacrée, et donc d'accéder aux données stockées localement dans l'appareil. Ces attaques sont d'autant plus dangereuses (ou percutantes) qu'elles ne sont souvent qu'une étape dans une chaîne plus longue et servent de tremplin vers d'autres systèmes.

Les attaques par ingénierie sociale portent une certaine ironie. Malgré des configurations de sécurité robustes et conformes aux meilleures pratiques du secteur, aucune solution technique ne peut empêcher un utilisateur de communiquer ses identifiants à des acteurs malveillants qui se font passer pour une personne de confiance. La dispersion des environnements ne fait qu'aggraver la situation : de nombreux utilisateurs ne peuvent pas contacter leurs collègues de la sécurité informatique lorsqu'ils reçoivent un e-mail ou un SMS suspect réclamant une réponse immédiate.

Ces messages sont délibérément rédigés pour effrayer les victimes et les inciter à cliquer sur un lien aux effets divers : vol de jeton d'authentification, exécution de code malveillant pour exploiter une vulnérabilité de leur appareil ou redirection vers un faux site web qui les incitera à fournir leurs identifiants. Et malheureusement, au moment où elles contactent leur service informatique, il est souvent trop tard. **IBM signale**, par exemple, que le vol ou la compromission d'identifiants restait non seulement la cause de violation la plus fréquente mais, avec 327 jours, était également celle qui prenait le plus de temps à identifier.

Les attaques de phishing sont un peu à part : vous n'avez pas affaire à un acteur anonyme qui ment pour obtenir votre nom d'utilisateur et votre mot de passe. La tromperie peut prendre plusieurs formes pour aboutir au même résultat. Prenons l'exemple de l'evil twin (ou jumeau maléfique), une attaque courante dans les lieux équipés d'un point d'accès public (voir « Wi-Fi gratuit ») sont disponibles. Ce jumeau maléfique prend l'apparence d'un réseau sans fil légitime pour permettre à un adversaire de voler les données transmises par la victime à son insu. Cette attaque sera sans effet si le trafic de l'appareil est chiffré par **un VPN ou une solution d'accès réseau zero-trust (ZTNA).**

En 2022, 31 % des organisations ont eu au moins une **victime de phishing parmi leurs rangs.**



En 2022, on a découvert que 16 % des utilisateurs exposaient des données sensibles en se connectant à des **points d'accès à risque.**

Ensemble, ces deux données nous amènent à deux conclusions :

1. Les utilisateurs modifient beaucoup moins leurs appareils qu'auparavant, et…
2. Les malfaiteurs ciblent de plus en plus les appareils des entreprises.

Source : Jamf Threat Labs

Selon Statistica, on compte **432,5 millions de hotspots Wi-Fi publics disponibles dans le monde.** Et en 2022, on a découvert que 16 % des utilisateurs exposaient des données sensibles en se connectant à des points d'accès à risque. En supposant qu'un seul utilisateur se connecte à chacun de ces points d'accès, cela représente 432,5 millions d'utilisateurs qui transfèrent des données via des connexions non sécurisées.

Ces chiffres ne font pas de distinction entre usage personnel et professionnel. Ils ne tiennent pas non plus compte des solutions de sécurité qui peuvent contribuer à déjouer les attaques de phishing, comme les logiciels de filtrage de contenu qui bloquent l'accès aux URL malveillantes.

Surtout, selon l'EC-Council, elles ne tiennent pas compte de la **meilleure façon de protéger votre personnel.** Pour lutter contre l'ingénierie sociale et les attaques de phishing sur tous les supports de communication, l'une des meilleures défenses n'est pas technique, mais administrative : c'est la **sensibilisation à la cybersécurité.** En intégrant un programme de formation complet à vos processus d'onboarding, suivi de mises à jour fréquentes portant sur les attaques en cours, vous armerez vos utilisateurs des connaissances nécessaires pour identifier les menaces et évaluer les risques liés aux tentatives de phishing.

L'investissement dans la formation des parties prenantes de l'entreprise doit être un pilier essentiel de la stratégie de sécurité d'une entreprise. Cela implique de mettre à disposition des utilisateurs finaux une formation continue et polyvalente, qui couvre l'éventail des bonnes pratiques et les familiarise avec les dernières menaces les plus susceptibles de les affecter. Ils auront ainsi toutes les cartes en main pour identifier les nouvelles formes d'attaque et agir en amont pour améliorer leur cyberhygiène, au travail comme dans la vie de tous les jours.

Le top 10 des attaques de phishing :

1 **E-mail :**
Les malfaiteurs envoient des e-mails semblant provenir d'une source fiable et digne de confiance.

2 **Vishing :**
Ces attaques de phishing vocal optent pour la livraison d'attaque orientée téléphone (TOAD), souvent en usurpant le numéro d'un appelant de confiance. Certains appels frauduleux prétendent provenir du FBI, par exemple.

3. **Smishing :**
Plutôt qu'un appel téléphonique, les malfaiteurs utilisent cette fois des SMS contenant des liens ou des pièces jointes pour compromettre les utilisateurs d'appareils mobiles.

4 **Réseaux sociaux/Pêcheur :**
Les nouvelles technologies sont autant de nouveaux vecteurs d'attaque, et de nombreuses attaques ciblent les utilisateurs de différents réseaux sociaux. Le pêcheur, ou angler en anglais, se fait passer pour un membre du service client d'une entreprise, souvent avec un faux compte, pour cibler les clients qui demandent de l'aide.

5 **Spear phishing, ou phishing ciblé :**
Cette variante ciblée du phishing par e-mail vise des individus spécifiques au sein d'une organisation, par exemple un employé du service de la paie.

6. **Whaling, ou pêche au gros :**
Semblable au spear phishing, cette attaque affine encore son champ d'action pour cibler spécialement les cadres et les dirigeants d'une organisation.

7. **HTTP/S :**
Ces attaques s'appuient sur des sites web dont l'URL contient souvent des fautes d'orthographe difficiles à déceler au premier coup d'œil, comme « iamf.com » au lieu de « jamf.com ». Ces domaines peuvent être sécurisés par SSL pour contourner les fonctionnalités de sécurité des navigateurs modernes.

8. **Falsification de site web :**
Ce type d'attaque accompagne souvent les attaques HTTP/S. Le site web associe une URL malveillante à une apparence légitime : le texte, les logos, les couleurs et les fonctionnalités d'origine reflètent le site qu'il imite pour inspirer la confiance.

9. **Point d'eau :**
Combinant phishing ciblé et tactique, les attaques au point d'eau ciblent des groupes spécifiques d'utilisateurs en piratant un site web qu'ils visitent fréquemment. L'attaque vise à compromettre le site web lui-même, en l'infectant avec des logiciels malveillants, de façon à infecter les visiteurs du site.

10. **Pop-up :**
À l'instar des pop-ups d'antan, cette variante du phishing demande aux acteurs malveillants de pirater un site web puis d'utiliser des publicités intégrées ou les notifications activées par les utilisateurs pour délivrer une charge utile qui va infecter les visiteurs.

Tendance 2 : La vie privée des utilisateurs s'invite à la table de la sécurité

À l'instar d'Apple et Jamf, des constructeurs et des développeurs défendent depuis un certain temps déjà la protection de la vie privée. D'une manière générale, les autres fournisseurs de technologie n'ont jamais accordé à la protection de la confidentialité la même importance qu'aux autres mesures de sécurité dans leurs offres matérielles et logicielles.

Tout comme une fuite de données commerciales, une violation peut faire de nombreuses victimes sur le champ de bataille de la protection des données privées des utilisateurs. Pensez que les données personnelles ne sont pas seulement collectées sans l'autorisation de l'utilisateur. Elles peuvent être compromises de plusieurs manières :

- Les États-nations utilisent du code malveillant pour espionner les flux de communication en surveillant le micro de la caméra des appareils ou en enregistrant la saisie au clavier des victimes.
- Ces données sont ensuite exploitées à des fins personnelles ou financières, pour mener des campagnes d'ingénierie sociale et pour faire chanter les victimes.
- Les entreprises s'enrichissent en vendant les données collectées sans le consentement de l'utilisateur à des annonceurs ou des partenaires tiers.

Il arrive également que des organisations qui collectent des données personnelles dans le cadre de procédures opérationnelles légitimes se retrouvent en difficulté. C'est le cas, par exemple, si elles n'ont pas suffisamment protégé les données personnelles contre les menaces externes ou internes, ou n'ont pas respecté leurs obligations réglementaires. Et dans certaines situations, les **organisations ne sont même pas conscientes de la menace,** comme en atteste le fait que « 5 % des organisations avaient une application potentiellement indésirable dans leur flotte d'appareils en 2022 ».

À première vue, le chiffre de 5 % peut paraître faible. Mais l'évaluation des risques ne s'arrête pas aux chiffres. Elle tient compte de nombreux aspects :

- Identification des actifs ciblés
- Vecteurs d'attaques éventuellement présents
- Types d'attaques possibles
- Probabilité de l'attaque
- Impact potentiel en cas d'exploitation ou de compromission

Pour résumer, c'est en considérant tous ces éléments que les organisations pourront évaluer les risques présents et leur impact potentiel sur la continuité des activités. Comment cela s'applique-t-il aux données personnelles ?

« **0,4 %** des appareils Android possédaient une application potentiellement indésirable en **2022**, contre **0,1 %** des appareils iOS. »

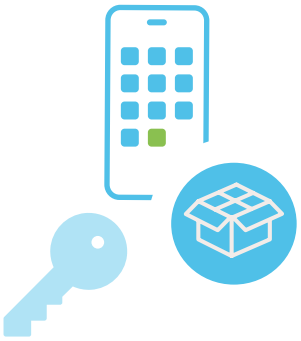
Android est un écosystème ouvert qui ouvre la porte à des applications plus risquées. Apple a créé un écosystème d'applications encadré et protège plus étroitement la vie privée des utilisateurs, ce qui limite l'introduction de ces applications à risque.

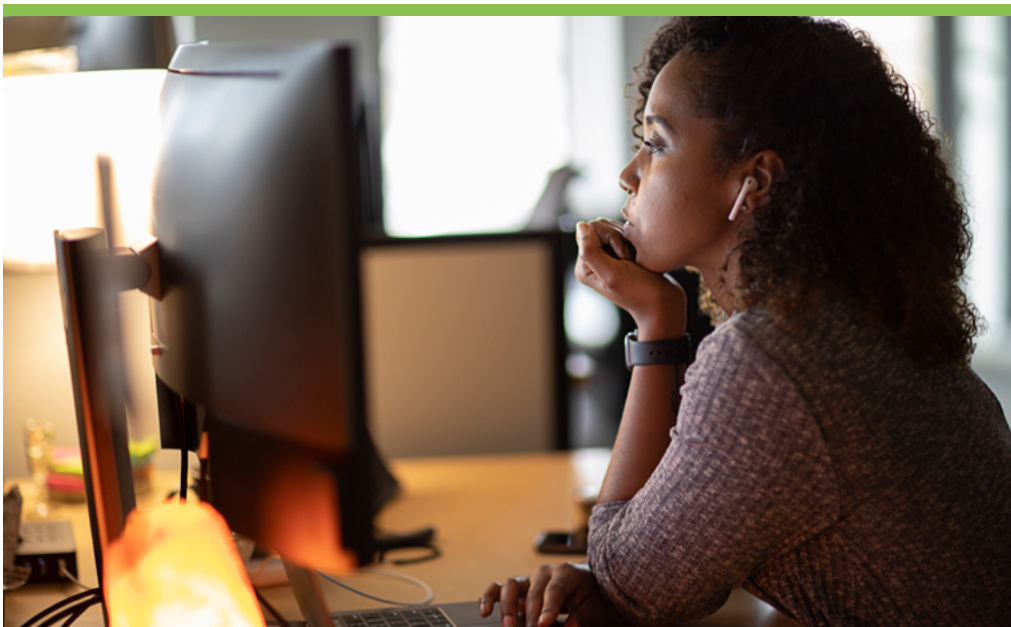
Le dernier point concerne l'impact potentiel d'une exploitation ou d'une compromission, et il ne doit pas être sous-estimé car il touche directement au cœur des contrôles réglementaires et à la manière dont ils atténuent les risques. (Vous trouverez davantage d'informations sur la conformité dans la suite de ce rapport.)

Les contrôles visant la protection de la vie privée sont en train de devenir aussi importants que les contrôles de sécurité. Il s'agit non seulement d'assurer la conformité demandée, mais aussi de limiter l'exposition des données privées des utilisateurs dans le cadre d'une stratégie de sécurité plus large. Cette exigence doit s'étendre à l'ensemble des solutions, processus, acteurs et workflows d'une organisation. Il faut en effet assurer la sécurité globale des données au moment de la création ou de la mise en œuvre de tous les composants dans l'entreprise – et non pas a posteriori.

Les solutions de gestion permettent d'aligner les règles de l'entreprise sur les exigences réglementaires. Elles allègent également la charge de gestion du service informatique en définissant un ensemble d'applications d'entreprise. Cette approche sécurise tous les types de données dans l'ensemble de l'infrastructure, quel que soit le type d'appareil ou sa localisation.

Pouvoir gérer différents modèles de propriété donne aux entreprises la possibilité de trouver un juste équilibre. Elles sécurisent les applications et les données, et elles appliquent des configurations sécurisées aux appareils qui doivent accéder aux ressources protégées. Mais elles laissent également aux utilisateurs le contrôle sur leurs données privées et leurs applications personnelles. Les entreprises protègent leurs données sensibles et confidentielles, sans toucher aux données privées des utilisateurs. Ces derniers **contrôlent le niveau d'accès** à ces données pour une protection renforcée de la confidentialité, et ce, quel que soit le modèle en vigueur dans l'entreprise : BYOD, appareil d'entreprise en CYOD/COPE et approches mixtes.





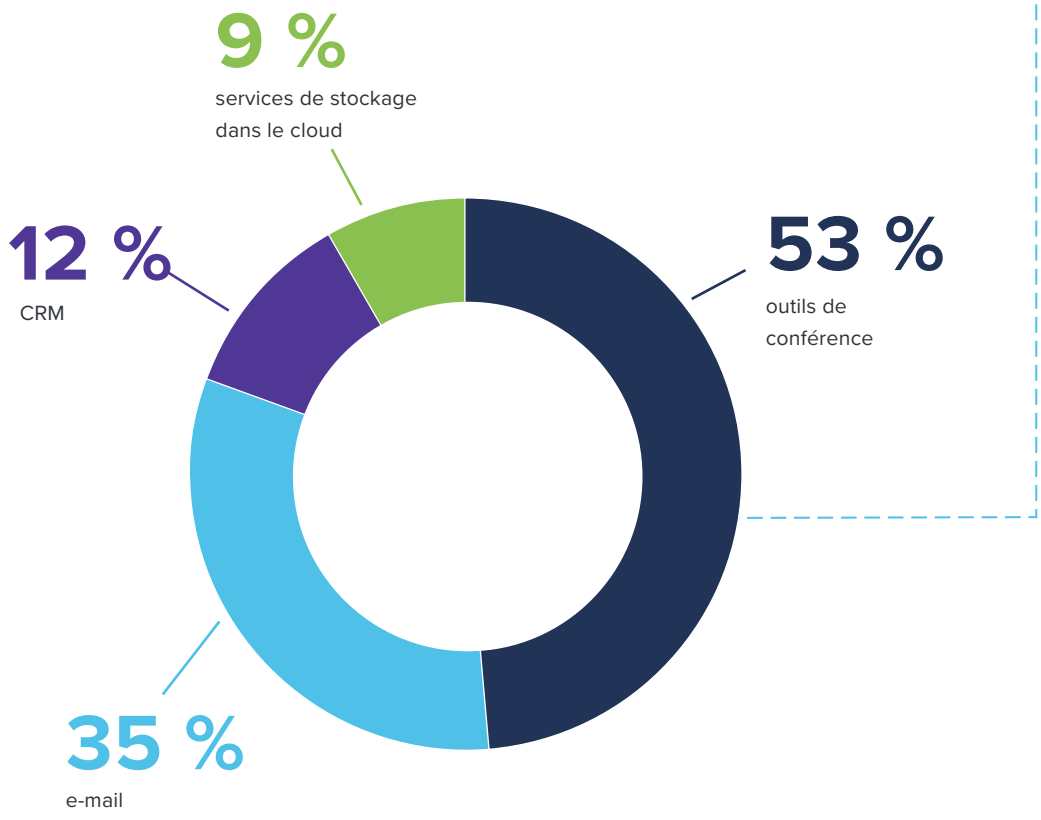
Tendance 3 – Les acteurs malveillants font converger leurs attaques pour créer de nouvelles menaces

Quelques bonnes nouvelles sur le front des logiciels malveillants sur macOS : le nombre total d'infections n'a montré aucun signe de croissance par rapport à l'année précédente. Ce n'est pas tout : en 2022, les **nouvelles infections par logiciel malveillant ont diminué**, passant d'un peu plus de 150 millions à environ 100 millions, selon AV-Atlas qui consigne en continu les programmes malveillants et les applications potentiellement indésirables (PUA).

En revanche, le trafic réseau malveillant, surveillé via les indicateurs de compromission (IoC) observables dans les schémas de communication entre l'appareil et les serveurs Internet, gagne sans cesse du terrain. On ne l'observe en général que dans les environnements de production et il ne peut être identifié par une simple évaluation du code statique. C'est pour cette raison qu'il faut surveiller activement la santé des terminaux lors de l'évaluation des facteurs de risque.

Le fait que des acteurs malveillants associent diverses attaques n'est pas nouveau en soi. On constate toutefois que cette approche convergée est de plus en plus souvent utilisée pour cibler les employés en télétravail et obtenir un accès non autorisé à des services et des ressources protégés. Au cours d'un même mois de 2022, 53 % des appareils compromis avaient accédé à des outils de conférence, tandis que 35 % avaient pu se connecter à la messagerie d'entreprise, 12 % à un CRM et 9 % à des services de stockage dans le cloud.

Au cours d'un même mois de 2022, **53 %** des appareils compromis avaient accédé à des outils de conférence, tandis que **35 % avaient pu se connecter à la messagerie d'entreprise, 12 % à un CRM** et **9 % à des services de stockage dans le cloud.**



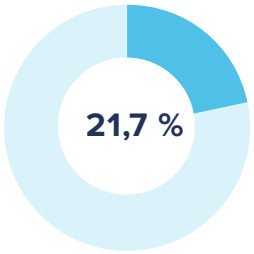
Exemple d'attaque sophistiquée

Un employé reçoit un message semblant provenir d'un collègue. Il s'agit en réalité de phishing ciblé. Le message comprend un lien vers un « document de travail » qui injecte un code malveillant sur l'appareil de la victime. Ce code recueille ses identifiants et dépose un ransomware. L'attaquant prend en otage les données sensibles de l'utilisateur et utilise les identifiants pour obtenir un accès plus large à l'infrastructure de l'organisation. Enfin, il réalise encore deux autres opérations : il ajoute le terminal à un réseau de zombies qui sera utilisé pour attaquer d'autres organisations, et il recherche d'autres appareils à infecter pour accroître son réseau.

S'il y a un message à retenir, c'est que les attaques peuvent prendre plus d'une forme, s'étendent sur des périodes variables et passent souvent inaperçues. Certaines chaînes d'attaques se produisent peu de temps après la compromission – c'est notamment le cas des ransomwares. D'autres, en revanche, sont plus tactiques et demandent plus de temps, comme la construction d'un botnet dans le but de mener des attaques par déni de service distribué (DDoS).

Il est difficile de se protéger contre cette convergence, car les victimes ignorent souvent l'ampleur de l'attaque jusqu'à ce que la vague suivante les frappe. Néanmoins, il existe des pratiques qui peuvent atténuer certains risques et limiter fortement l'impact exercé par d'autres. La surveillance active des terminaux et la collecte de données télémétriques sur leur état de santé offrent de précieux renseignements aux administrateurs. Elles apportent une visibilité détaillée sur les appareils selon plusieurs critères, dont l'application des correctifs. C'est d'autant plus utile que des comportements suspects peuvent trahir une compromission de l'appareil indétectable par l'utilisateur final.

Puisqu'on aborde la question des correctifs, la gestion du cycle de vie des applications est un enjeu de taille lorsqu'il s'agit d'atténuer les risques liés aux vulnérabilités des systèmes. En effet, des applications correctement sécurisées contribuent grandement à se protéger contre les menaces connues. Pensez également que les app stores tiers fournissent souvent des versions d'applications grand public truffées de code malveillant, et destinées à infecter les appareils des utilisateurs. Ces versions gratuites de logiciels payants servent bien souvent d'appât pour attirer les victimes.



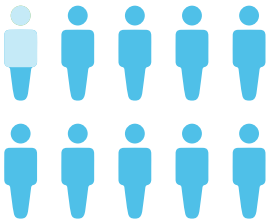
21,7 % des appareils Android ont accédé à des app stores tiers, contre **0,002 %** des **appareils iOS.**

Les boutiques d'applications tierces sont couramment employées pour contourner le processus d'évaluation qui protège les appareils et les utilisateurs.

0,02 % des appareils Android étaient rootés et **0,001 %** des **appareils iOS** étaient **jailbreakés** en 2022.

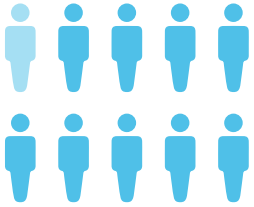
Le pourcentage est faible, mais vous remarquerez que la proportion d'appareils Apple touchés est deux fois plus élevée que celle des appareils Apple. Et rapporté au nombre invraisemblable d'appareils Android et Apple en circulation dans le monde, ce chiffre traduit un phénomène d'une ampleur considérable.

Certains systèmes d'exploitation (OS) autorisent le chargement latéral d'applications. Mais avec d'autres, comme iOS, il faut d'abord jailbreaker l'appareil – autrement dit, neutraliser la protection qui empêche l'exécution de code non signé. Le verrouillage des appareils n'est qu'une partie de l'équation. Il est crucial d'identifier les appareils jailbreakés en temps réel afin de remédier efficacement à ce vecteur de menace.



0,004 % des utilisateurs et **0,3 %** des organisations avaient un appareil **jailbreaké** ou **rooté** en 2022.

Statistiques de l'année dernière :

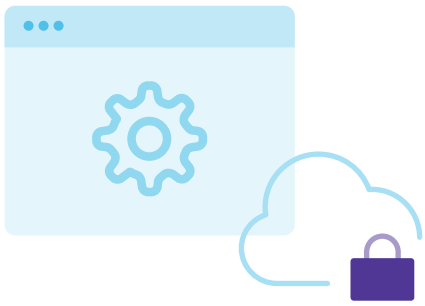


Moins de 1 % des organisations étaient en possession d'un appareil **jailbreaké** ou **rooté** en 2021.

Attaques de la chaîne d'approvisionnement

Les attaques contre la chaîne d'approvisionnement ou des **tiers** ont de vastes répercussions. Elles affectent en profondeur plusieurs couches de chaque organisation du pipeline, avant d'atteindre **leur véritable cible.** Leurs effets sont souvent considérables et touchent les entreprises du monde entier, quelle que soit la solidité de leur posture de sécurité.

Elles sont également difficiles à prévenir, principalement parce que les entreprises n'ont pas l'autorité nécessaire pour exiger de chaque acteur et sous-traitant de la filière qu'il atténue efficacement les facteurs de risque. Malheureusement, votre organisation ne peut échapper à ces difficultés. Face à cette situation, l'Agence américaine de cybersécurité et de sécurité des infrastructure (CISA) et l'Institut national des normes et de la technologie (NIST) ont publié un document technique conjoint intitulé **se défendre contre les attaques de la chaîne d'approvisionnement logiciel**. Ce document explique qu'un élément clé pour « renforcer la capacité d'une organisation à prévenir, atténuer et prendre en charge de telles attaques » consiste à respecter les bonnes pratiques du secteur dans le cadre d'une stratégie de sécurité globale de défense en profondeur. Cette stratégie doit inclure l'examen des processus de sécurité des fournisseurs par des contrôleurs indépendants et la vérification des mesures d'atténuation prises par vos partenaires (et par les leurs).



Tendance 4 : La conformité aux réglementations fait partie de la pile de sécurité

Parallèlement à la sécurité des données de l'entreprise, la protection de la confidentialité des utilisateurs gagne en importance. C'est surtout dans le domaine de la conformité que ce problème se pose, en particulier vis-à-vis des réglementations nationales, fédérales et régionales. Pensez au règlement général sur la protection des données (RGPD) et à la loi californienne sur la protection de la vie privée des consommateurs (CCPA), qui renforcent considérablement les droits des utilisateurs à la confidentialité. Pensez également aux multiples aspects de gouvernance auxquels est soumise la fintech, qui figure parmi les secteurs les plus réglementés au monde.

Voici quelques exemples de réglementations qui, de manière autonome ou en conjonction avec d'autres, encadrent la conformité réglementaire de certains secteurs :

Loi Sarbanes-Oxley de 2002 (SOX) : dicte les pratiques comptables.

Gramm-Leach-Bliley Act (GLB) : établit les niveaux minimaux de protection de cybersécurité requis pour maintenir la sécurité de l'information.

Financial Industry Regulatory Authority (FINRA) : détaille explicitement le lien entre les processus métier et la protection des investisseurs en prescrivant des opérations équitables et honnêtes dans le secteur des titres et actions.

Les réglementations affectent les entreprises de certains secteurs et certaines ont une portée mondiale, obligeant les organisations concernées à se conformer à des lois qui peuvent se situer bien au-delà de leur juridiction. Elles se retrouvent alors dans l'obligation d'exercer un plus grand contrôle sur leurs workflows afin de préserver la confidentialité et la bonne gestion des types de données protégées. Informations d'identification personnelle (IIP), informations de santé protégées (ISP) et informations de business intelligence (IBI) doivent en effet être collectées, traitées, stockées, modifiées, partagées et détruites conformément aux souhaits des personnes concernées et/ou les réglementations en vigueur.

La mise en conformité est une tâche difficile qui nécessite une grande réflexion, une bonne gestion et un appui solide, même si vos appareils et vos données sont gérés par l'organisation. Mais comment garantir cette conformité quand les équipes sont décentralisées et doivent pouvoir accéder aux ressources de l'organisation partout, à tout moment et sur n'importe quel appareil ? Les complications créées par le télétravail peuvent être un véritable défi pour les organisations soumises à des exigences de conformité et confrontées au paysage moderne des menaces.

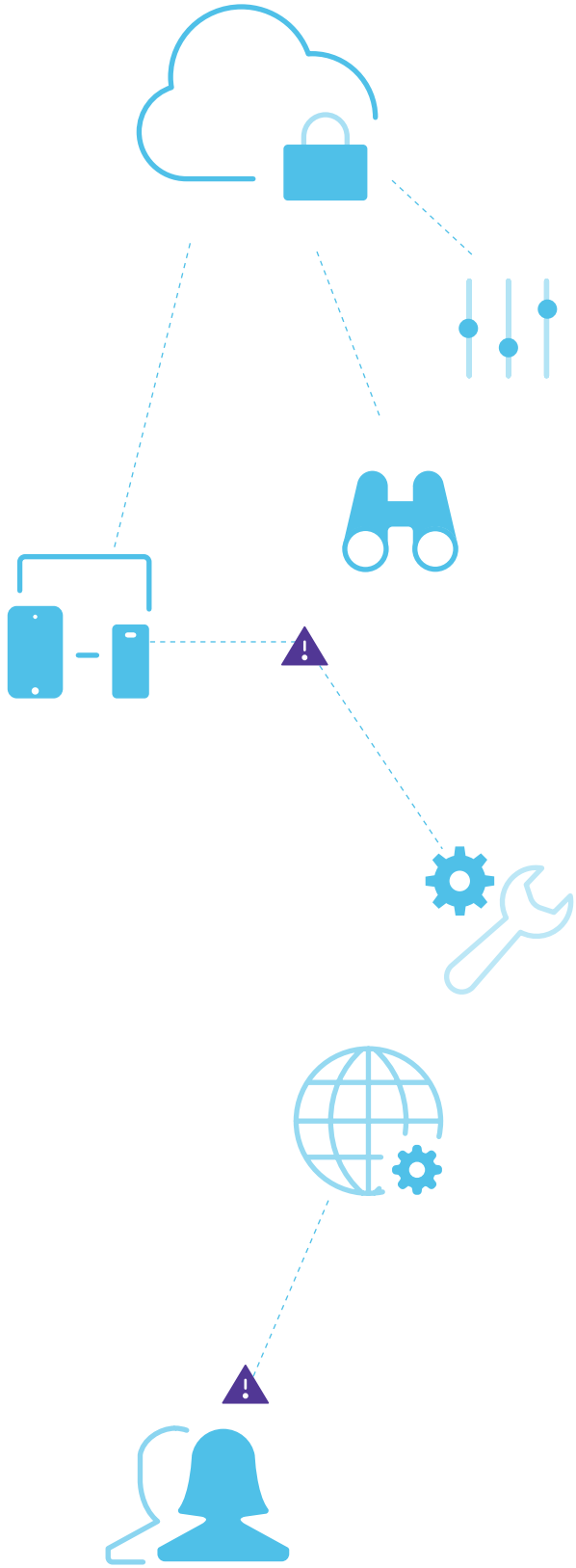
« En **2022, 21 %** des employés utilisaient des appareils **mal configurés** et donc à **risque**. »

Et le ciel de la conformité s'assombrit encore lorsqu'on intègre les appareils personnels aux impératifs de gestion. En 2022, 21 % des employés utilisaient des appareils mal configurés et donc à risque. Plus précisément, lorsque des données sensibles, confidentielles ou stratégiques – et potentiellement réglementées – ne sont pas à l'abri, c'est l'organisation elle-même (et éventuellement l'utilisateur) qui s'expose à des poursuites civiles et/ou pénales si une faille entraîne une infraction aux lois de réglementation.

De nombreuses entreprises ont opté pour le BYOD ou laissent à leurs employés le choix de leur appareil et de leur système d'exploitation, dans un souci de confort et de productivité. Dans ce contexte, une gestion efficace de la conformité ne peut pas se contenter de bloquer l'accès de tous les appareils à l'exception de ceux qui sont gérés. **Nous avons vu que 8 % des utilisateurs et 21 % des organisations étaient touchés par des vulnérabilités de configuration**. Autrement dit, même les appareils qui appartiennent à l'entreprise qu'elle gère peuvent être concernés. Les solutions doivent prendre davantage de paramètres en considération pour aborder les problèmes de sécurité sans s'arrêter à la gestion des appareils.

Le fait est que n'importe quel terminal, à tout moment, peut être à risque : correctif oublié, fuite de données causée par une vulnérabilité courante, perte et vol, tout simplement. Dans chaque scénario, l'atténuation du risque réclame une action différente. Certains cas peuvent être traités par des workflows de réponse et de correction automatisés, mais dans d'autres, la correction manuelle sera toujours de mise.

Comme bien souvent lorsqu'on parle de sécurité, il n'existe pas de solution miracle ou universelle, capable d'assurer tous les fondamentaux et de garantir la conformité permanente de votre infrastructure. Nous recommandons de mettre en œuvre d'une stratégie de sécurité de type « défense en profondeur », qui fait converger plusieurs solutions pour répondre à vos exigences de sécurité uniques sous plusieurs angles.



Tendance 5 : Sécuriser les données reste un défi dans les environnements distants

Le passage au télétravail a entraîné des bouleversements en matière de sécurité des utilisateurs, des données et des appareils. Le périmètre du réseau s'est effectivement érodé, et les solutions sur site ont été remplacées par des alternatives basées sur le cloud afin de rapprocher les services de sécurité d'utilisateurs dispersés, travaillant sur tout type d'appareil. Le résultat : une solution de sécurité des terminaux plus puissante et autonome, une résilience accrue et une sécurité robuste pour les applications.

Et pourtant, malgré ces avantages incontestables, les organisations ont toujours des difficultés à sécuriser les données dans les environnements de travail à distance, plusieurs années après la migration. Malheureusement, aucun problème clair ne permet de désigner le coupable. C'est une pluralité de facteurs qui empêche de sécuriser les données comme il le faudrait. On peut toutefois identifier des lacunes dans plusieurs domaines :

- Visibilité en temps réel de la santé des terminaux
- Intégration entre les outils de gestion et de sécurité
- Automatisation des processus et des workflows
- Journalisation décentralisée et renseignements sur les menaces
- Respect des règles et de la conformité
- Formation des utilisateurs finaux à la sécurité
- Solutions spécialisées
- Pratiques d'évaluation des risques pour identifier les actifs et les menaces

Par exemple, nous avons constaté que **64 % des appareils vulnérables avaient accès à des outils de collaboration, et que 34 % pouvaient utiliser la messagerie de l'entreprise**. Certes, les indicateurs de risque et de compromission sont subjectifs et varient d'une entreprise à l'autre. Mais cela révèle nettement que les tâches de routine – gestion des correctifs en tête – ne sont pas correctement effectuées sur tous les appareils. Les appareils eux-mêmes sont exposés, et mettent les ressources de l'organisation en danger.
Et le problème dépasse le cadre des applications et des configurations. Jamf Threat Labs a constaté qu'**un appareil sur cinq utilisait un système d'exploitation qui n'était pas à jour.** Il est essentiel que la sécurité soit présente à tous les niveaux d'une stratégie de défense en profondeur, en commençant par l'OS, pour protéger les utilisateurs et les organisations.

C'est un argument de plus en faveur d'une visibilité totale sur votre flotte d'appareils et leurs interactions avec l'infrastructure de votre organisation, surtout si votre secteur est réglementé. Cette exigence est d'autant plus forte que la plupart des administrations demandent aux organisations de prouver leur conformité par le biais d'audits réguliers. Ces contrôles visent à vérifier que les données protégées et les terminaux qui les exploitent sont sécurisés conformément aux réglementations.

Mais en évaluant vos actifs et les menaces qui pèsent sur votre organisation, et recueillant des données de télémétrie pour identifier les terminaux touchés, vous n'obtenez qu'une solution partielle. Pour atténuer les risques et prendre des décisions d'accès en temps réel, il faut des solutions modernes. Quand il s'agit de sécuriser les connexions à distance, les technologies traditionnelles comme le VPN ne peuvent certainement pas rivaliser avec les nouvelles approches pensées pour le télétravail et adaptées au paysage actuel des menaces. Le ZTNA n'accorde l'accès aux applications et aux services qu'après avoir vérifié que l'utilisateur possède les autorisations requises et que son appareil remplit des critères minimum de santé.

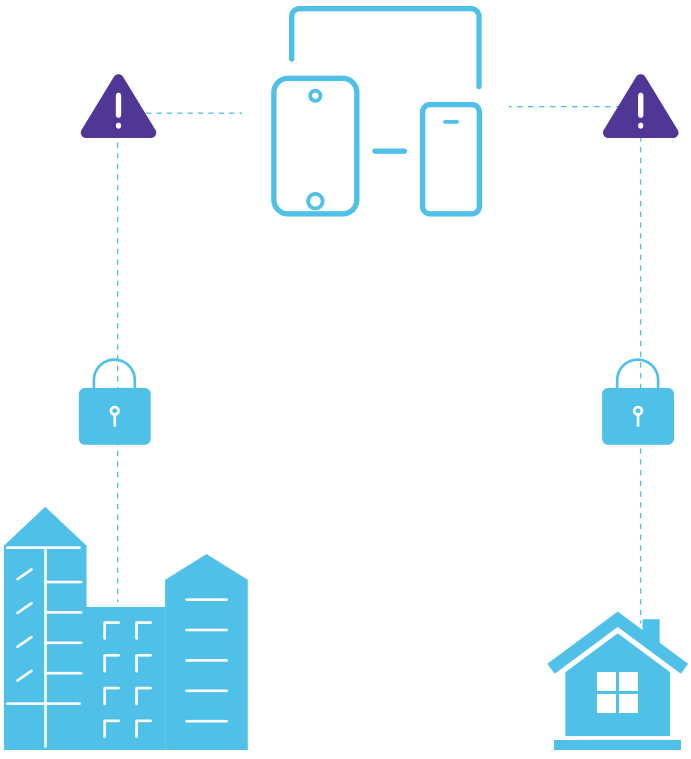
Conçues pour les réseaux et les workflows modernes, les solutions ZTNA atténuent les risques et protègent les données. Flexibles, elles permettent également de préserver la confidentialité des applications et données personnelles. Au-delà, l'accès des utilisateurs est déterminé selon le principe du moindre privilège. Le trafic professionnel est acheminé via des microtunnels qui l'isolent : si un adversaire compromet l'appareil d'un utilisateur, il ne pourra pas accéder à toutes les applications auxquelles il a normalement droit. Cette segmentation intégrée du trafic empêche les attaquants d'effectuer de mouvements latéraux sur le réseau, mettant un frein efficace aux menaces.

Autre élément clé, les solutions sont intégrées de façon sécurisée au moyen d'API qui assurent le partage des données critiques de télémétrie et de santé des terminaux. Elles peuvent ainsi activement réduire le taux de réussite des menaces ciblant les appareils, les utilisateurs et les données sensibles. Le contraste est saisissant avec les solutions de sécurité monobloc et autonomes qui n'offrent pas les possibilités d'intégration nécessaires à la création d'une approche holistique de défense en profondeur.

Les outils des acteurs malveillants évoluent, et les organisations doivent consolider leurs solutions pour prévenir les attaques connues tout en atténuant les risques liés aux menaces émergentes. Dans ce contexte, la recherche des menaces gagne en importance dans l'entreprise. Elle aide les équipes informatiques et de sécurité à identifier, atténuer et corriger les menaces inconnues avant qu'elles n'entraînent des violations. Les technologies d'intelligence artificielle (IA) et de machine learning (ML) ont montré leur efficacité dans plusieurs secteurs, dont la cybersécurité. Les solutions s'appuient de plus en plus sur leur puissance de traitement leurs capacités d'analyse comportementale pour comprendre les menaces, les prédire et les contrer, à des vitesses hors de portée des administrateurs humains.

Axez votre stratégie sur la gestion des appareils mobiles (MDM) afin de sécuriser et tenir à jour les appareils appartenant à l'entreprise comme aux employés. Déployez une solution de sécurité des terminaux pour arrêter les logiciels malveillants et recueillir des données de télémétrie riches grâce à une surveillance active des appareils. Et misez sur une API pour permettre à ces deux solutions de partager des renseignements sur les menaces en toute sécurité et pour faire respecter les règles de conformité. Enfin, une solution de gestion des identités et des accès va centraliser la gestion des identifiants et l'octroi des autorisations sur les ressources de l'organisation, dont l'accès sera sécurisé par l'authentification multifacteur (MFA).

Ces aspects s'intègrent aux approches de sécurité modernes comme le ZTNA pour sécuriser les connexions sur n'importe quel réseau, détecter les nouvelles menaces grâce au ML, arrêter les attaques dans l'œuf et atténuer les menaces basées sur le réseau en remplaçant les VPN classiques par des solutions capables de segmenter les demandes d'accès. Une solution de ce type va enfin collecter en temps réel des données sur les menaces et la santé des terminaux pour automatiser de manière globale la gestion du cycle de vie des appareils.



Recommandations

Cela va faire trois ans que la pandémie a amorcé un bouleversement des environnements de travail à grande échelle. Aujourd'hui, la question n'est plus **« comment poursuivre nos activités ? »** mais bien **« comment assurer en permanence la protection des utilisateurs distants et des ressources de l'entreprise ? »**

Ce changement d'état d'esprit a une raison majeure. Certes, le télétravail se pratique depuis plusieurs années déjà, mais le nombre d'utilisateurs distants pris en charge par les équipes informatiques et de sécurité a plus que doublé. Ils sont désormais 46 %, contre 21 % avant la pandémie, selon le rapport **État de la cybersécurité 2022** de Splunk. Selon les conclusions de l'enquête mondiale de Splunk, « non seulement les attaques se multiplient, mais les violations également. »

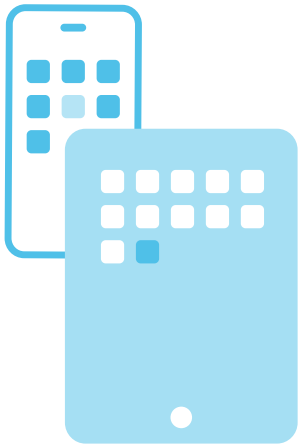
L'augmentation du nombre d'attaques, l'évolution du paysage des menaces et la nécessité de sécuriser les ressources utilisées à distance confirment les conclusions du rapport Security 360 de l'année dernière :

> Les solutions d'accès à distance sécurisé doivent être suffisamment souples et agiles pour permettre, et non empêcher, la productivité.

Ce à quoi nous ajouterons cette année :

> La sécurité des terminaux doit assurer la convergence des solutions de sécurité, en s'appuyant sur une base solide, une visibilité granulaire et des technologies avancées comme le ML. L'objectif doit être de développer des workflows sécurisés automatisés, alignés sur les règles de l'organisation et les réglementations du secteur.

Les organisations doivent, à terme, élaborer une stratégie de sécurité moderne de défense en profondeur reposant sur le cloud, pour répondre à leurs besoins actuels et disposer de l'évolutivité nécessaire pour faire face à ceux de demain.



À propos de cette recherche

Nous cherchons à identifier les grandes tendances technologiques qui émergent dans le monde du travail hybride. Les informations et les statistiques présentées dans ce document sont les résultats de notre analyse des tendances de sécurité. Elle porte sur un échantillon de 500 000 appareils (iOS, macOS, iPadOS, Android et Windows) protégés par Jamf, dans 90 pays, sur une période de 12 mois. Cette analyse a été réalisée au quatrième trimestre de 2022. Les métadonnées analysées dans cette recherche proviennent de journaux agrégés dépourvus d'informations permettant d'identifier les personnes ou les organisations. L'objectif de cette analyse n'est pas de vous effrayer, mais bien de vous informer, vos utilisateurs et vous, sur les options qui s'offrent à vous. Apprenez à sécuriser au mieux tous les aspects des appareils, ainsi que les données des utilisateurs et de l'entreprise.