jamf

Défense en profondeur

Combler les lacunes de sécurité par l'intégration et la superposition de solutions

La cybersécurité n'est pas seulement importante.

Elle est absolument **cruciale** pour défendre votre organisation contre l'évolution des menaces et des attaques ciblant vos appareils, vos utilisateurs, vos données et vos ressources.

Auparavant, la sécurité de l'information se résumait à une solution antivirus installée sur chaque ordinateur et à un client VPN pour les quelques employés, comme les équipes de vente itinérantes, qui travaillaient en dehors du bureau.

Mais les temps ont changé et la manière dont nous gérons la cybersécurité a évolué également.

Dans ce livre blanc, nous abordons :

- L'évolution du paysage des menaces
- La nécessité absolue de protéger tous les types d'appareils et tous les OS
- Les clés de la sécurité au-delà de la protection des ressources
- L'importance de la mise en œuvre d'une stratégie de défense en profondeur
- L'importance d'une approche intégrée de la sécurité en entreprise

L’évolution du paysage des menaces

Notre secteur a parcouru un long chemin et les progrès de la technologie mobile ont encouragé les utilisateurs et les organisations à changer leurs méthodes de travail. Mais cette évolution a dépassé les frontières de notre industrie. Les pirates ont, eux aussi, transformé leurs tactiques pour s’adapter à ces changements. Leurs attaques sont devenues beaucoup plus sophistiquées, et donc plus difficiles à repérer pour les utilisateurs finaux et à arrêter pour les professionnels de la sécurité.

Une chose est claire : aujourd’hui, les menaces viennent de toutes parts. Elles ciblent tous les types d’appareils et tous les systèmes d’exploitation, et se déploient via n’importe quelle connexion réseau.

Pourquoi, demanderez-vous ? Parce que la « stratégie de solution unique » basée sur le périmètre, autrefois performante pour assurer la sécurité des données et des terminaux, a perdu son efficacité. Le périmètre du réseau a en effet été érodé par :

- L’adoption de services et d’applications basés sur le Cloud
- Le passage au télétravail et aux environnements de travail hybrides
- L’intégration des appareils personnels au travail
- Le recours à des connexions réseau non fiables pour la communication
- L’utilisation d’outils de collaboration partagés

Toutes ces nouveautés ont clairement donné aux utilisateurs la possibilité de travailler partout, à tout moment, sur tout type d’appareil et via n’importe quelle connectivité réseau. Mais elles ont aussi multiplié les vecteurs d’attaque potentiels en élargissant la surface d’attaque des appareils.

Passons en revue quelques évolutions du paysage des menaces qui ont accompagné l’essor des technologies mobiles et de la dispersion des équipes.

APT, convergence des menaces et complexité croissante des attaques

Le paysage des menaces a évolué. Tout professionnel de la sécurité digne de ce nom le sait. Mais nous allons ici nous demander comment le paysage a changé. Dissimulé au cœur d’une fausse application ou exécuté via un site web compromis, du code malveillant reste du code malveillant et son objectif est toujours le même : infecter votre appareil et lui faire exécuter les attaques voulues par le pirate.

Comme on peut l'observer, les formules classiques sont progressivement abandonnées. Les attaques gagnent en complexité. Elles sont souvent combinées à d'autres menaces ou déployées par des moyens détournés, par exemple en compromettant un partenaire de confiance de la cible pour accéder à ses ressources. Voici quelques exemples de ces attaques sophistiquées survenues au cours de ces trois dernières années :

- Deux attaques en deux ans ont affecté plus de **100 millions** de clients en compromettant leurs IPT.

Les attaques de la chaîne d'approvisionnement ont triplé en 2023 : on a recensé **2,1 milliards de téléchargements** de logiciels présentant des vulnérabilités (alors que des versions corrigées étaient disponibles).

- Des casinos et des hôtels ont subi une attaque de ransomware doublée d'une campagne d'ingénierie sociale qui a impacté les opérations, compromis les données des clients et entraîné des pertes financières.
- Les données de **5,4 millions d'utilisateurs** ont été exposées, et les données publiques et privées de **400 millions d'utilisateurs** ont été vendues sur le dark web suite à la compromission de l'API d'une plateforme de réseau social.
- Les personnes à haut risque sont continuellement ciblées par des États-voyous qui utilisent le logiciel espion Pegasus pour surveiller leur appareil mobile à leur insu.

Convergence des menaces

Également appelée convergence cyber-physique, elle décrit l'imbrication croissante des espaces numériques et physiques. La ligne de démarcation entre ces deux sphères s'estompe progressivement, et ce qui survient dans un domaine (cyber) a des effets très concrets sur l'autre (physique). Au-delà des perturbations physiques des systèmes, des processus et des es ressources, les cybermenaces étendent la portée des attaques et amplifient leur impact par de multiples moyens :

- Implantation persistante
- Élévation de privilèges
- Déplacements latéraux
- Déploiement de logiciels malveillants
- Exfiltration de données

Nous observons ce phénomène dans des entreprises de tous les secteurs. En effet, la continuité des activités dépend lourdement de la technologie, si bien qu'une cyberattaque qui, par exemple, empêcherait les utilisateurs d'accéder à leurs e-mails, peut quasiment interrompre toute activité jusqu'à ce que l'accès soit rétabli. Si elle persiste, l'impact sur les opérations peut devenir considérable : perte de production et de revenus, voire la fermeture définitive des business concernés.

Ce fut le cas lorsque le plus grand oléoduc de produits pétroliers raffinés des États-Unis. Capable de transporter 3 millions de barils de carburant par jour, il a été contraint de fermer pendant cinq jours après avoir été victime d'une attaque par ransomware en 2021. L'impact sur cette infrastructure critique ? La plus médiatisée est sans aucun doute la rançon de 5 millions versée aux pirates pour rétablir l'accès aux données et aux systèmes chiffrés. Au cours des années qui ont suivi, plusieurs changements ont été mis en œuvre. Le ministère de la Justice a notamment adopté une approche plus agressive pour démanteler les infrastructures et les réseaux criminels à l'origine des attaques par ransomware. Mais les pirates ont également fait évoluer leurs tactiques, puisque « plus de 90 % des attaques ne chiffrent plus l'appareil de la victime, mais se contentent d'exfiltrer les données pour la faire chanter. »

Ingénierie sociale

Les menaces basées sur l'ingénierie sociale ne semblent pas avoir de fin dans l'environnement d'aujourd'hui. Il fut un temps où les sources d'inquiétude étaient limitées : un usurpateur pouvait tenter de se faire passer pour l'employé d'une entreprise, ou bien vous pouviez recevoir un e-mail d'un prince généreux, mais inquiet, et qui avait désespérément besoin de votre compte en banque pour entreposer ses millions.

Les temps ont bien changé.

L'ingénierie sociale désigne aujourd'hui un organigramme complexe et ramifié d'attaques trop diverses pour être toutes énumérées. Dans ce système, chaque nouvelle technologie s'accompagne de l'apparition de nouvelles formes d'attaques. Une chose est claire : « l'anneau qui les gouverne tous » est le phishing, avec toutes ses variantes.

Chaque nouvelle itération, comme le phishing par code QR, ou « quishing » comme on le surnomme affectueusement, se fait une place dans notre jargon de sécurité. Mais l'ingénierie sociale évolue en réalité sur deux niveaux : à la surface et en dessous. La première évolution est facile à repérer. Il s'agit des cinq grandes attaques d'usurpation d'identité, fruits de l'adaptation du phishing à nos méthodes de travail :

1. Phishing par e-mail
2. Phishing ciblé
3. Whaling
4. Smishing et vishing
5. Phishing du pêcheur à la mouche

Le deuxième niveau d'évolution, quant à lui, ne porte pas de surnom pratique. Ces nouvelles menaces sont donc d'autant plus dangereuses et difficiles à détecter par les utilisateurs finaux, les équipes informatiques et les équipes de sécurité.

Le Jamf Threat Labs a récemment mis au jour deux techniques de sabotage de ce type. Les preuves de concept (PoC) élaborées par l'équipe ont de lourdes implications pour la sécurité sur mobile, aujourd'hui et demain :

Faux mode avion

Cette technique de persistance post-exploit affiche un faux « mode avion ». En regardant sous la surface, vous découvrirez qu'après avoir exploité l'appareil, les fichiers système contrôlant l'interface utilisateur ont été modifiés de façon à afficher les icônes du mode avion et à désactiver l'accès à Internet de toutes les applications, à l'exception de celle qui doit servir au pirate. De cette manière, le pirate conserve l'accès à l'appareil (persistance) même lorsque l'utilisateur pense l'avoir mis hors ligne.

Faux mode verrouillage

Nous avons déjà évoqué le logiciel espion Pegasus et la manière dont des États-voyous l'utilisent pour surveiller des personnes d'intérêt à leur insu. Nous allons aborder les menaces parrainées par des États dans la section suivante, et le mode verrouillage d'Apple constitue un outil important pour réduire la surface d'attaque.

Imaginez la situation : pendant que votre appareil mobile a été compromis, vous activez le mode verrouillage pour vous protéger contre toute exposition supplémentaire. Mais en réalité, votre appareil est toujours aussi vulnérable : les pirates ont contourné cette protection de dernier recours.

C'est un exemple typique d'ingénierie sociale : les utilisateurs pensent qu'ils sont protégés, mais il s'agit d'un faux sentiment de sécurité. Pendant ce temps, les pirates conservent l'accès et le contrôle sur leur appareil mobile.

Attaques ciblées et parrainées par des États-voyous

À l'ère numérique, on peut comprendre les sentiments de paranoïa associés aux moindres gestes, paroles et messages, que ce soit en public, au bureau ou même à la maison, compte tenu de l'omniprésence de la technologie dans toutes les facettes de notre existence.

Même si, comme Christopher Walken, vous avez choisi de renoncer à l'ordinateur et au smartphone, vous risquez toujours de voir votre vie privée exposée par ceux qui utilisent des appareils autour de vous.

Les groupes de cybercriminels parrainés par des États et les menaces persistantes avancées (APT) ne menacent pas seulement les entreprises de certains secteurs. Aujourd'hui, les APT étendent leur champ d'attaque au-delà des infrastructures critiques et n'hésitent pas à cibler toutes les personnes, organisations et régions qui présentent un intérêt pour l'État qui les dirige.

Voici quelques chiffres à ce sujet :

90 % des alertes de sécurité proviennent de secteurs extérieurs aux infrastructures critiques

Les trois secteurs les plus ciblés au niveau mondial sont :

L'éducation **16%**

L'administration **12 %**

Les think tanks/ONG et le secteur de l'informatique, à égalité à **11 %**

9 organisations sur 10 pensent avoir été ciblées par des acteurs malveillants affiliés à des États.

Le coût pour les organisations s'élève en moyenne à **1,6 million de dollars par incident**.

5 groupes APT (jusqu'à présent) ont commencé à utiliser l'IA pour améliorer les performances de leurs attaques.

Si le gain financier figure indéniablement parmi les principales motivations des groupes cybercriminels, le vol de données est l'objectif premier des États-voyous. Cela ne veut pas dire que l'espionnage et la perturbation des systèmes, des services et des réseaux sont relégués au second plan. Dans le contexte actuel, les APT se concentrent davantage sur l'exfiltration de données sensibles et confidentielles, dans le but de recueillir des renseignements, de mener d'autres attaques et d'influer sur les activités sociales et politiques.

Sur ce dernier point, la prolifération des logiciels malveillants mobiles utilisés pour espionner les personnalités importantes est à rapprocher des inquiétudes que suscite la myriade de capteurs intégrés aux appareils mobiles en matière surveillance non autorisée et d'infraction à la vue privée. Et cela ne s'arrête pas là : les États-voyous utilisent les données recueillies pour mieux cibler leurs victimes – journalistes, personnalités politiques, cadres dirigeants – et les espionner à leur insu. Extrêmement discrets, ces logiciels espions sont conçus pour être déployés à distance et extraire tout type de données de l'appareil mobile de la victime. Ils s'appuient le plus souvent sur une installation « zéro clic » et des exploits « zero-day » pour infecter les appareils mobiles cibles.

Il n'y a pas de solution générique

Comme nous l'avons vu, les cybermenaces évoluent constamment, et la combinaison des facteurs que nous avons recensés nous amène à la situation actuelle. Nous sommes à un point de bascule, car les solutions, les procédures et les workflows actuels sont conçus pour protéger :

- Un ordinateur de bureau appartenant à l'entreprise
- Exécutant un seul OS pris en charge

Et verrouillé par le service informatique de manière à :

- N'utiliser qu'une sélection d'applications
- Empêcher l'exécution de toute tâche sortant du cadre professionnel
- Rester dans la sécurité relative du périmètre du réseau de l'entreprise.
- Acheminer le trafic réseau à travers le pare-feu de l'entreprise
- Protéger les données grâce à des solutions antimalware
- Et sécuriser l'accès à distance à l'aide d'un VPN

Les solutions développées pour sécuriser les terminaux statiques ne suffisent pas à garantir la posture de sécurité d'un ordinateur dans le paysage actuel des menaces. La situation est plus criante encore dans les grandes entreprises modernes où convergent toutes les grandes transformations des environnements de travail dynamiques.

Les stratégies de sécurité modernes gagnent à être à la fois solides et flexibles. Il ne suffit plus d'invoquer une règle interdisant l'utilisation des appareils mobiles, d'un type d'OS particulier ou des appareils personnels pour atténuer les risques associés. Cette règle n'empêchera pas les utilisateurs d'essayer d'accéder aux ressources professionnelles à partir de « terminaux interdits ». Il est tout à fait possible qu'ils introduisent des risques dans votre réseau. Pire encore, les administrateurs ne s'en rendront sans doute compte qu'après un incident.

Quelle est la meilleure approche ?

C'est quand elles s'appuient sur les solutions les plus performantes que les équipes informatiques et de sécurité gèrent au mieux les terminaux et leur sécurité. Il leur faut des solutions de gestion et de sécurité conçues pour prendre en charge nativement les types d'appareils et les OS qu'elles supervisent. Cette approche ne garantit pas seulement le plus haut niveau de compatibilité avec le matériel et les logiciels : elle fournit aux équipes informatiques et de sécurité tous les outils nécessaires pour gérer et sécuriser les terminaux de leur infrastructure de façon optimale.

macOS en entreprise

Réfléchissez à l'environnement de votre entreprise. Vous gérez très certainement des appareils Windows, mais quelle est votre position à l'égard des appareils macOS ? Selon une récente enquête menée auprès de PME, « **55 %** des entreprises utilisent directement des appareils Mac ou approuvent explicitement leur utilisation au travail, » et ce dans tous les secteurs d'activité.

Avant de poursuivre, examinons les parts de marché de macOS (en février 2024) :

Au niveau mondial :	États-Unis :
15,46 %	**25,02 %**

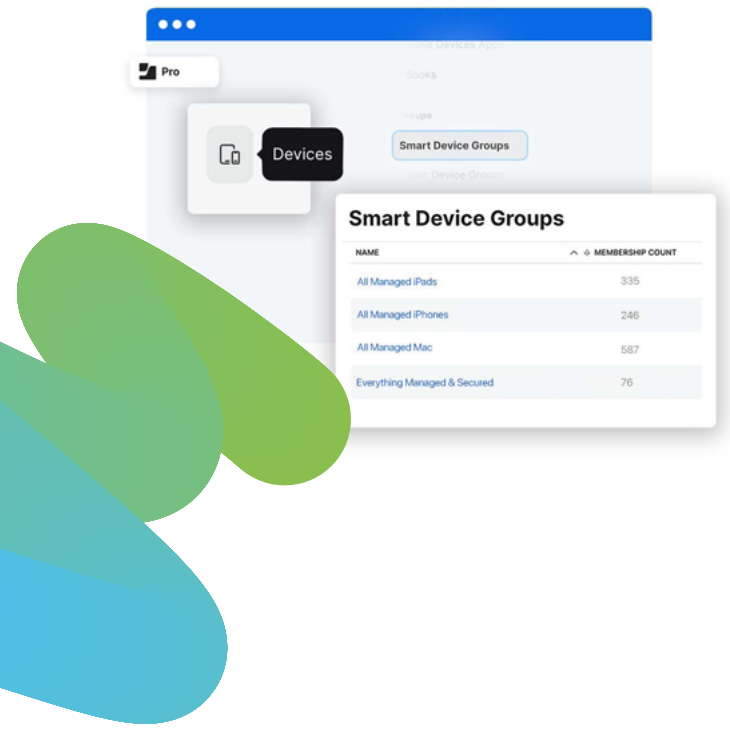
Aux États-Unis, macOS représente un quart du marché, et un peu plus de la moitié des machines sont utilisées en entreprise. La question n'est donc pas de savoir si, mais quand macOS fera son entrée dans votre entreprise, et comment vous les sécuriserez à ce moment-là. Que vous le vouliez ou non, macOS est sans doute utilisé à un degré ou à un autre par vos employés pour effectuer des tâches liées à leur travail. Cet appareil peut avoir été fourni ou autorisé par l'entreprise, dans le cadre d'un programme de choix des employés ou d'une initiative BYOD/COPE. Mais il peut aussi s'agir d'un appareil personnel utilisé hors de tout cadre d'autorisation.

La croissance du Mac accélère, en particulier dans le monde du travail, ce qui a des conséquences critiques sur la sécurité de l'entreprise si les équipes informatiques et de sécurité n'utilisent pas des outils de gestion et de sécurité adaptés aux besoins uniques des Mac. C'est déjà le cas pour les appareils sur Windows, comme avec n'importe quel matériel ou logiciel.

Appareils mobiles : un risque non maîtrisé

L'utilisateur moyen dispose d'un seul ordinateur, mais il utilise souvent plusieurs types d'appareils mobiles : smartphone, tablette, montre connectée, etc. En effet, selon une enquête de Statista, le nombre moyen d'appareils par utilisateur dans le monde est passé à 3,6 en 2023.

C'est presque quatre vecteurs d'attaques par utilisateur. Les entreprises savent parfaitement qu'elles doivent sécuriser les appareils de bureau. Mais si elles ne contrôlent pas les appareils mobiles, cela signifie qu'ils sont probablement autorisés à se connecter sans protection aux réseaux, aux données et aux ressources professionnels.



Quels sont les types de menaces liées à la mobilité ?

Ce sont souvent les mêmes que celles qui pèsent sur les ordinateurs de bureau, mais sans logiciel de sécurité spécialisé pour offrir une visibilité sur les systèmes de fichiers des appareils mobiles.

Voici les principaux risques associés à la mobilité en entreprise :

- **Accès non autorisé :** les pirates mènent des campagnes d'ingénierie sociale par le biais de SMS et de messages sur les réseaux sociaux pour recueillir les identifiants des victimes et accéder aux services de l'entreprise.
- **Introduction de logiciels malveillants :** les applications téléchargées à partir de boutiques non officielles ou par sideloading peuvent exécuter du code malveillant ciblant les données professionnelles et personnelles.
- **Non-conformité :** quand les règles internes ne sont pas appliquées, la conformité des appareils devient précaire, ce qui peut avoir de lourdes conséquences dans les secteurs réglementés.
- **Exfiltration de données :** le vol de données commerciales, personnelles et confidentielles peut être très lucratif pour des acteurs malveillants.
- **Mouvement latéral :** les attaques basées sur le réseau utilisent des identifiants compromis pour se propager à l'ensemble de l'infrastructure et accroître l'ampleur des violations de données.
- **Contournement des protections :** les réglages de sécurité défaillants et les applications mal configurées agrandissent la surface d'attaque et facilitent l'exécution de charges utiles sur les appareils.
- **Élévation de privilèges :** les pirates peuvent exploiter les vulnérabilités présentes dans les logiciels obsolètes pour s'introduire dans les appareils et, par extension, dans votre réseau.

Au-delà de la protection des ressources

Pour combler les lacunes de la couverture de sécurité, les professionnels envisagent une succession de moyens d'atténuation. Ils cherchent notamment à améliorer les processus de gestion des correctifs pour que les logiciels et les systèmes d'exploitation restent à jour et soient mieux protégés contre les menaces. Il est également intéressant d'ajouter les nouvelles technologies d'intelligence artificielle (IA) et de machine learning (ML) à votre pile de sécurité afin de répondre plus rapidement aux incidents ou de systématiser la recherche des menaces.

Ce sont d'excellents moyens de combler les lacunes de sécurité, mais d'autres éléments vont au-delà de ces contrôles pour mieux sécuriser les appareils, les utilisateurs et les données. Ces mesures sous-jacentes, moins visibles que les contrôles techniques et logiques, apportent une valeur ajoutée à votre organisation en uniformisant, en automatisant et en consolidant les procédures, les processus, les outils et les workflows de votre stratégie de sécurité globale. Elles permettent également de centraliser les outils des équipes informatiques et de sécurité chargées de veiller à la conformité des appareils, des utilisateurs et des données, pour un fonctionnement optimal.

Dans cette section, nous détaillons ces mesures que nous appelons « les quatre C » et qui s'articulent pour un maximum d'efficacité. Leur objectif est de minimiser les défis dans la posture de sécurité globale de votre organisation.

Cohérence

En matière de sécurité, les organisations doivent traiter tous les types d'appareils professionnels connectés aux ressources de l'entreprise de la même manière, OS inclus. Une entreprise qui fournit des ordinateurs Windows à ses employés et déploie des contrôles de sécurité des terminaux pour les gérer et les sécuriser. Mais ces mêmes employés peuvent aussi utiliser des appareils mobiles non contrôlés, et si elle ne met pas aussi en place une solution de défense contre les menaces mobiles pour protéger les données auxquelles ils accèdent, le risque de violation devient très élevé.

On le sait, les appareils Apple sont sécurisés dès la conception et le constructeur fait de la sécurité et du respect de la vie privée une priorité. Pourtant, les pirates ciblent régulièrement les appareils macOS, iOS et iPadOS, comme ils le font pour les appareils Windows ou Android. Pour parvenir à la cohérence, l'idée n'est pas de se focaliser sur ce qui distingue les différents OS, mais plutôt sur leurs points communs. Les ordinateurs de bureau, les ordinateurs portables, les tablettes et les smartphones ont bien plus en commun que leur aspect ne le laisse penser.

L'objet de la cohérence est précisément de traiter de la même manière tous les terminaux qui accèdent aux ressources de l'entreprise, quels que soient :

- Le type d'appareil
- Son format
- Son système d'exploitation
- Les applications et les services

Conformité

La conformité désigne ce qui est conforme à un désir, une demande, une proposition, un régime ou la coercition

La conformité peut revêtir une signification différente selon le secteur d'activité de votre entreprise. Dans les secteurs réglementés, des lois spécifiques régissent la manière dont les données, les processus et les workflows doivent être sécurisés pour éviter toute fuite de données appartenant à des catégories protégées. Mais les entreprises des autres secteurs peuvent, elles aussi, définir un certain nombre de standards de conformité. Elles établissent des règlements internes, par exemple, ou alignent leurs activités sur standards ou des cadres industriels.

Parler de conformité pour combler les lacunes de sécurité, c'est aborder deux points importants :

Utiliser des profils de référence

Première chose, les profils de référence, ou lignes de base. Définir ces profils permet de fixer les limites de ce qui est considéré comme un fonctionnement normal au sein de votre infrastructure. Mais ces lignes de base ont un autre intérêt : elles servent d'étalon administrateurs, qui peuvent être alertés quand les terminaux s'écartent des paramètres acceptables et ne sont plus conformes.

Fournir des preuves aux auditeurs

Que votre entreprise organise des contrôles internes ou qu'elle soit soumise à des audits indépendants dans le cadre de ses obligations réglementaires, elle doit pouvoir produire des preuves pour démontrer que la conformité a été maintenue. Pour les auditeurs chargés de vérifier la conformité des terminaux, les choses sont simples : « Si ce n'est pas documenté, ça n'existe pas. »

La clé de la gestion des profils de référence et de la collecte de preuves réside dans les données de télémétrie. Elles donnent aux administrateurs de la visibilité sur la santé des terminaux. Ils peuvent savoir à tout moment si les appareils utilisés pour consulter, traiter, stocker, modifier, diffuser ou partager les données de l'entreprise sont conformes aux directives ou aux exigences définies par votre plan de sécurité ou votre administration.

Consolidation

Le troisième « C » est aussi l'un des plus mal compris, car on le confond souvent avec la consolidation des outils.

> « La cybersécurité est bien plus qu'une question d'informatique. »
>
> — Stephane Nappo

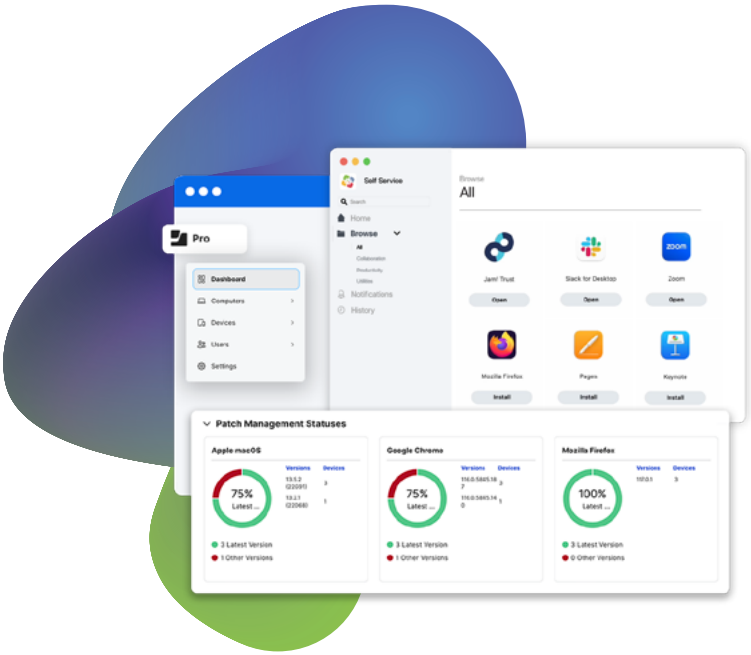
Ici, la consolidation consiste à réunir les professionnels de l'informatique et de la sécurité en une seule équipe – un vrai changement par rapport au modèle traditionnel à deux équipes. Si les deux domaines appartiennent à la grande catégorie des technologies de l'information, les organisations choisissent généralement de séparer les activités de ces départements pour un certain nombre de raisons métier.

Mais face au paysage moderne des menaces, ce mode de fonctionnement présente un défaut majeur : chaque service gère son propre ensemble de logiciels, de fournisseurs, de processus, de règles et de workflows. En théorie, la différence des approches vise à renforcer la posture de sécurité des appareils et de l'organisation dans son ensemble. Mais en réalité, ce type de structure produit souvent l'effet inverse.

Une consolidation efficace nécessite de moderniser et d'intégrer les architectures et les processus de cybersécurité pour :

- Centraliser les solutions les plus performantes pour gérer les différentes plateformes de manière native
- Réduire le nombre de fournisseurs et de partenariats
- Casser les silos et faciliter le partage d'informations
- Éliminer le problème des « domaines réservés » en mettant en place des pratiques de gestion des connaissances
- Intégrer l'approche de la gestion et de la sécurité
- Unifier la prévention des menaces et accélérer la réponse aux incidents
- Étendre les protections à l'ensemble de l'infrastructure

En adoptant une approche intégrée de la sécurité et de la gestion, les administrateurs ont toutes les cartes en main pour protéger les appareils et les utilisateurs par des mesures de sécurité complètes lorsqu'ils utilisent des données commerciales sensibles. Et ces mesures peuvent être étendues de manière holistique à l'ensemble des ressources de l'entreprise.



Réduction des coûts

Parallèlement à la consolidation de l'administration informatique et de la sécurité, il faut accorder au retour sur investissement (ROI) l'importance qu'il mérite. Le retour sur investissement doit permettre de réaliser des économies en choisissant des solutions en phase avec les besoins spécifiques et les efforts de conformité des entreprises. Pour cela, il faut non seulement de comprendre la valeur des solutions par rapport à leur coût, mais aussi soupeser les autres facteurs qui influent directement et indirectement sur la rentabilité de votre stratégie de défense en profondeur.

Voici quelques facteurs directs et indirects qui améliorent le ROI d'une stratégie de renforcement de la sécurité :

- Choisir des outils qui prennent en charge nativement les appareils et les OS de votre organisation, mais qui soient également capables de s'intégrer pour former une solution holistique
- Automatiser les tâches manuelles et fastidieuses pour gagner en efficacité et permettre aux administrateurs de se concentrer sur des projets à valeur ajoutée
- Uniformiser les processus et les workflows de sécurité, les étendre à l'ensemble de l'infrastructure et les optimiser pour prendre en charge les terminaux et les applications à grande échelle
- Minimiser la complexité des solutions et de la réponse aux incidents pour réduire les délais de découverte et de correction des incidents de sécurité. Le résultat : moins de temps d'arrêt et plus de productivité.
- Exploiter les données télémétriques riches produites en temps réel par la surveillance active et les rapports, afin de détecter et corriger de manière proactive les vecteurs de risque avant que la conformité ne soit affectée

Autre facteur important sur le plan économique comme dans le contexte du paysage moderne des menaces : l'utilisation d'appareils personnels au travail. De nombreuses organisations ont mis en place un programme BYOD, en particulier dans les environnements où le télétravail est fréquent, pour que les membres de l'équipe restent connectés et collaborent efficacement. Et il ne fait aucun doute que le BYOD présente des avantages pour les employeurs : Zippia a d'ailleurs récemment rapporté que près de **70 %** des décideurs informatiques aux États-Unis approuvent les programmes BYOD .

96 % des appareils mobiles qui se connectent aux réseaux d'entreprise appartiennent à leur utilisateur

80 % des cadres dirigeants estiment que les appareils mobiles sont essentiels pour que les employés puissent faire leur travail

Le nombre d'employés équipés de technologies portables devrait augmenter de **30 %**

D'autres organisations ont mis en place des programmes de choix et permettent à leurs employés d'utiliser le matériel et les logiciels qu'ils jugent les plus performants. Elles s'épargnent ainsi l'impact financier de l'achat et de l'entretien de centaines ou de milliers d'appareils mobiles, en plus des ordinateurs. Les avantages et les économies sont considérables.

Défense en profondeur : une sécurité multicouches efficace

Selon la définition du National Institute of Standards and Technology (NIST), la défense en profondeur (DeP) est une *« stratégie de sécurité de l'information intégrant les capacités humaines, technologiques et opérationnelles afin de mettre en place des barrières variables à travers les multiples couches et missions de l'organisation ».*

En adaptant ce principe à votre plan de cybersécurité, vous obtiendrez des protections supplémentaires qui renforceront votre posture de sécurité. Cette approche consistant à superposer les contrôles crée un filet de sécurité pour les organisations. Ses mesures d'étanchéité visent à empêcher les menaces de compromettre les ressources de l'entreprise. Si une menace parvient à contourner un niveau de contrôle, le suivant va intercepter et atténuer la menace avant qu'elle ne se transforme en un incident et n'impacte la conformité.

Cette section aborde plusieurs questions clés :

- Quelle est l'incidence globale de l'intégration sur le plan de cybersécurité de votre entreprise ?
- Quels types de contrôles de sécurité globaux pouvez-vous mettre en œuvre pour parvenir à la défense en profondeur ?
- Quel est l'impact de votre plan de cybersécurité orienté DeP sur le respect des exigences de conformité ?

Gestion + Identité + Sécurité

Vous connaissez sans doute les grands concepts de la gestion des appareils : gestion, identité et sécurité. Chacun d'eux représente un élément fondamental et s'accompagne d'un ensemble de technologies et de bonnes pratiques :

- **Gestion des appareils :** administration des ordinateurs et des appareils mobiles, qui comprend la gestion des réglages, le déploiement de configurations sécurisées, l'installation de logiciels et l'application des règles.
- **Identités et accès :** cadre de règles et de technologies garantissant que les utilisateurs authentifiés et/ou les appareils autorisés obtiennent l'accès aux ressources protégées en fonction des permissions qui leur ont été attribuées.
- **Sécurité des terminaux :** technologies logicielles conçues pour minimiser les risques, protéger les appareils et les utilisateurs contre les menaces et les attaques, et sauvegarder les ressources protégées.

L'intégration de ces trois éléments fondamentaux est à la base d'un plan de défense en profondeur de cybersécurité. Son objectif est de garantir la protection des ressources professionnelles contre les accès non autorisés, de minimiser les vecteurs de risque liés aux terminaux et de préserver la sécurité et la productivité des utilisateurs.

Dans les sections suivantes, nous abordons des technologies rendues possibles par cette intégration, en mettant en évidence comment leur coordination minimise les risques, prévient les logiciels malveillants, et détecte et atténue les menaces avancées :

- Déploiement Zero-Touch
- Recherche des menaces
- Accès réseau zero-trust (ZTNA)
- Réponse aux menaces avancées

Déploiement zero-touch : la sécurité dès le départ

La sécurité est souvent un processus réactif. Le terme « réponse aux incidents » fait justement référence à cette approche qui consiste à attendre que les menaces se manifestent pour les prendre en charge, dans un lien de cause à effet.

Les administrateurs ne peuvent pas transformer la nature de ce lien, mais il est possible de réduire la surface d'attaque – autrement dit, « où » et « comment » une menace peut s'exercer sur un appareil.

Et le meilleur moment pour commencer, c'est la première fois qu'on allume un appareil. Toute la magie de l'approvisionnement et du déploiement zero-touch est là. Et avec des appareils Apple, c'est particulièrement facile à mettre en place.

En effet, les déploiements zero-touch en entreprise s'appuient sur des paramètres de gestion, d'identité et d'accès fournis aux appareils dès la configuration initiale. Plus précisément, dès que l'utilisateur s'est authentifié à l'aide de ses identifiants d'entreprise, qu'il a fini d'inscrire son appareil et qu'il a installé le profil de gestion. La solution MDM commence immédiatement à déployer tout ce dont l'utilisateur a besoin pour travailler et configure l'appareil selon les normes de l'organisation.

Que peut-on déployer pendant la phase d'approvisionnement du déploiement zero-touch ?

- Renforcement de la sécurité des appareils
- Installation d'applications gérées
- Configuration des réglages des applications
- Attribution de comptes utilisateurs
- Sélection d'options Self Service
- Correctifs système
- Logiciels de sécurité
- Application des règlements internes

Vous me répondrez peut-être que c'est idéal pour les appareils d'entreprise, mais que fait-on du BYOD ?

Les workflows zero-touch s'étendent à tous les modèles de propriété, y compris aux appareils personnels. Pour ces cas, Apple a mis au point l'inscription par l'utilisateur, qui protège la vie privée de l'employé sans sacrifier les protections de sécurité de l'entreprise.

L'inscription des appareils personnels dans la solution MDM de l'entreprise présente de nombreux avantages :

- Accès sécurisé aux ressources institutionnelles : e-mails, contacts, calendriers, Wi-Fi et connexions réseau chiffrées
- Les données professionnelles sont stockées dans un volume séparé et chiffré sur l'appareil, tandis que les données personnelles restent intactes.
- Il est possible d'utiliser deux identifiants Apple conjointement : un identifiant personnel pour l'activité et les données privées, et un identifiant géré pour les données professionnelles
- Sur un appareil en BYOD, les administrateurs ne peuvent voir et supprimer que des données institutionnelles ; les données personnelles et privées restent inaccessibles.
- Normalisation de la sécurité à l'échelle de l'entreprise, pour que tous les appareils possèdent le même niveau de protection, quel que soit leur propriétaire

Recherche des menaces : mieux vaut prévenir que guérir

Parmi les tâches les plus spécialisées qui incombent aux équipes administratives, la réponse aux incidents est un enjeu majeur. La détection et le tri des problèmes potentiels commencent dès qu'elles reçoivent une alerte de leur logiciel de sécurité des terminaux, signalant un comportement malveillant ou la présence d'une menace. Des équipes d'intervention doivent alors confirmer, contenir et corriger le problème.

S'il est normal que les intervenants s'attaquent aux problèmes connus, il est possible de transformer un processus largement réactif en approche proactive. Comment ? En intégrant les solutions de gestion et de sécurité pour enrichir les workflows et les processus.

Mettre en place des fondamentaux de sécurité

Dans le domaine de la cybersécurité, les lignes de base décrivent le fonctionnement normal des terminaux. Une base de référence ne se limite pas à des indicateurs de performance : elle implique des configurations, des réglages, des logiciels de sécurité des terminaux, des applications et des services – bref, tout l'arsenal nécessaire pour que les utilisateurs puissent travailler en toute sécurité. Elle implique également le respect des exigences de conformité et des règles de l'entreprise.

Prévention des menaces connues

En définissant et en enregistrant les paramètres nécessaires sous la forme de profils de référence, les administrateurs sont mieux armés pour déterminer si la santé des terminaux se situe dans des limites acceptables. Dans le cas contraire, la journalisation des terminaux avertira les administrateurs de la moindre anomalie et leur donnera la possibilité d'intervenir pour la corriger. Mais si elle est intégrée à votre solution de gestion, le partage des données de télémétrie déclenchera l'exécution de workflows de correction automatisés.

Détection des menaces inconnues

La dualité proaction/réaction est au cœur de la technologie, et c'est un concept essentiel pour assurer la gestion et la sécurité des terminaux face à la convergence et à l'évolution des menaces. La recherche des menaces vise précisément à se tenir à la pointe de la proaction.

Pour mener à bien cette tâche, il faut :

- Des données riches sur votre environnement
- De solides compétences en matière d'analyse des données et de reconnaissance des modèles
- Une connaissance approfondie du matériel et des logiciels
- Des outils de sécurité puissants et maîtrisés
- Du temps, de la patience et de la diligence pour enquêter sur l'inconnu

ZTNA : Ne jamais faire confiance, vérifier systématiquement

Au fil du temps, les technologies qui étaient à la pointe du progrès deviennent obsolètes avant d'être complètement abandonnées au profit d'une approche généralement plus rapide, plus performante et plus robuste. Le Zero Trust est un modèle de sécurité qui relève les défis posés par les menaces modernes d'une manière qui dépassent entièrement les capacités des technologies traditionnelles comme le VPN.

Le ZTNA intègre la technologie, l'identité et la gestion pour établir un nouveau paradigme en matière de cybersécurité.

Arrêter les menaces basées sur le réseau

En tant que technologue, vous avez l'habitude de travailler avec des pare-feux. Vous connaissez leurs fonctions et leurs possibilités. Ces appareils puissants protègent le périmètre du réseau contre les attaques. Mais avec l'adoption croissante des pratiques de télétravail et l'utilisation courante d'appareils personnels au travail, ils perdent de leur efficacité, car ils ne couvrent pas les employés qui travaillent à distance sur un appareil personnel non géré. Le ZTNA fournit une protection contre les menaces et les attaques à la fois sur l'appareil et sur le réseau. Surtout, il étend cette protection à plusieurs plateformes pour sécuriser de façon uniforme les ordinateurs comme les appareils mobiles, qu'ils fonctionnent sous macOS, iOS, iPadOS, Windows ou Android.

Isoler et chiffrer les connexions

Le ZTNA crée des tunnels chiffrés sur n'importe quelle connectivité réseau et reste constamment actif pour un maximum de sécurité. Il peut même se rétablir automatiquement s'il est désactivé par un utilisateur ou un logiciel malveillant. Le ZTNA apporte également une couche de protection supplémentaire grâce à son intégration avec la gestion des identités et des accès : à chaque fois qu'une connexion à une ressource protégée est établie, ZTNA génère un microtunnel unique, propre à l'application ou au service. C'est d'abord une excellente protection contre les attaques de type « Homme du milieu » (MitM), fréquentes sur les points d'accès publics, mais cela empêche également les mouvements latéraux sur le réseau en cas de compromission, car les microtunnels sont isolés les uns des autres. Le ZTNA applique enfin le principe de moindre privilège : une fois authentifiés, les utilisateurs ne reçoivent un accès explicite qu'aux ressources qui leur sont attribuées. Toutes les autres parties de l'infrastructure réseau restent fermées par défaut, contrairement au VPN classique qui accorde l'accès à l'ensemble du réseau une fois l'étape d'authentification franchie.

Vérifier la santé des terminaux et les demandes d'accès.

Au lieu de « faire confiance » aux appareils de manière implicite, les modèles zero-trust vérifient la santé des terminaux et des identifiants à chaque demande. Ils comparent l'état actuel du terminal aux normes de tolérance de votre organisation. C'est seulement après avoir franchi ces deux points de contrôle que l'accès à la ressource demandée est accordé. En cas d'échec de l'authentification ou du contrôle de la santé de l'appareil, l'accès reste coupé (comportement par défaut) et des workflows de correction sont déployés pour remédier aux anomalies. Une fois la correction effectuée, la demande doit à nouveau passer par les points de contrôle. Le ZTNA n'accorde l'accès à la ressource demandée qu'après avoir vérifié l'appareil et les identifiants.

Le ZTNA ne tient pas compte du fait que l'appareil mobile :

- appartient à l'entreprise ou à l'utilisateur
- se connecte au réseau de l'entreprise ou à un point d'accès public
- réussit les contrôles de santé s'il échoue au contrôle des identifiants

Il n'est pas non plus important que le compte de l'utilisateur :

- soit associé à un rôle particulier, comme celui de cadre ou de dirigeant
- se soit bien authentifié une heure – ou même cinq minutes – avant
- passe le contrôle des identifiants s'il échoue aux contrôles de santé

Le principe « ne jamais faire confiance, vérifier systématiquement » signifie que l'accès est désactivé par défaut. Les appareils et les identifiants doivent être vérifiés systématiquement, à chaque demande.

Réponse aux menaces avancées : protection des cadres

Les menaces persistantes avancées, ou APT, prolifèrent et cible des entreprise de tous les secteurs à l'échelle mondiale.

Dans cette section, nous abordons les mesures de défense à la disposition des administrateurs lors de l'intégration des solutions de sécurité et de gestion. Grâce aux renseignements sur les menaces recueillis et partagés entre les deux outils, on obtient une solution plus complète et robuste, capable de faire face aux menaces avancées qui ciblent de plus en plus les personnes occupant des postes clés, comme les dirigeants d'entreprise.

L'intégration de la sécurité et de la gestion présente plusieurs avantages majeurs pour l'atténuation des risques liés aux menaces avancées :

Acquérir une visibilité sur les attaques mobiles

Les menaces mobiles sont de plus en plus nombreuses. Le paysage des menaces ne cesse d'évoluer et les attaques visant directement les appareils mobiles et leurs utilisateurs se multiplient d'une année sur l'autre.

Pour vous en convaincre, voici quelques chiffres clés :

- **43 %** des appareils compromis étaient entièrement exploités (et non jailbreakés ou rootés), soit une augmentation de **187 %** d'une année sur l'autre.
- **80 %** des sites de phishing ciblent spécifiquement les appareils mobiles ou sont conçus pour fonctionner à la fois sur ordinateur de bureau et sur mobile.
- Le nombre de vulnérabilités Android critiques a augmenté de **138 %** en 2022, et les appareils Apple iOS représentaient **80 %** des vulnérabilités zero-day activement exploitées
- Les mauvaises configurations de stockage cloud dans les applications mobiles constituent une surface d'attaque de premier plan. **± 2 %** des applications iOS et **± 10 %** des applications Android ont accédé à des instances de cloud non sécurisées.
- Le nombre total d'exemplaires uniques de logiciels malveillants mobiles a augmenté de **51 %**, avec plus de **920 000** échantillons détectés

La surveillance active et la visibilité sont essentielles pour obtenir des informations sur les attaques mobiles. Il ne s'agit pas seulement d'identifier les menaces, mais aussi de connaître l'état de santé des terminaux qui accèdent aux ressources de l'entreprise. L'objectif : minimiser les facteurs de risque avant qu'ils ne puissent être exploités par des acteurs malveillants.

Une fois l'opération accomplie, la solution de sécurité des terminaux analyse à nouveau l'appareil pour confirmer que le risque a été atténué. Si c'est bien le cas, il reçoit l'accès aux ressources. Autrement, la demande est à nouveau déclinée et d'autres mesures de correction sont envisagées.

Éliminer les menaces avancées et persistantes

> *« Une once de prévention vaut une livre de guérison. »*
> – Benjamin Franklin

Comprendre le paysage des menaces, c'est, bien sûr, comprendre que la prévention est de loin supérieure à la réaction. Mais c'est aussi reconnaître qu'une menace peut inévitablement passer entre les mailles du filet et infecter votre réseau. Et face au niveau de sophistication des APT, la question n'est pas de savoir « si » les terminaux seront touchés, mais « quand ». Pour pivoter rapidement, la clé réside dans le degré de préparation de votre équipe. Son aptitude à faire face aux APT va dépendre des outils qu'elle utilise et de la qualité des données dont elle dispose pour corriger les menaces avancées.

Là encore, sécurité et gestion convergent pour créer des procédures et des workflows avancés capables de :

- Détecter les comportements suspects
- Alerter les administrateurs en cas d'incident
- Évaluer les menaces en recherchant les indicateurs de compromission (IoC) et d'attaque (IoA)
- Analyser les résultats obtenus à partir de multiples sources de renseignements sur les menaces
- Vérifier qu'une menace est bien réelle en éliminant les faux positifs
- Déployer des stratégies d'atténuation
- Effectuer des tâches de correction, si nécessaire
- Scanner l'appareil pour en vérifier la conformité

Selon le degré de gravité de la menace, l'intégration entre la sécurité et la gestion peut enrichir les processus manuels de réponse aux incidents ou exécuter automatiquement des actions de correction.

Réduire les délais d'enquête de plusieurs semaines à quelques minutes

Toutes les menaces ne se valent pas. Face au degré de sophistication atteint par certaines menaces et « preuve de concept » (PoC) récentes, les équipes d'intervention et de recherche des menaces doivent mener des investigations approfondies pour découvrir l'impact réel des menaces inconnues. Par le passé, les enquêtes pouvaient prendre des semaines, selon la gravité de la menace et sa complexité.

Pour détecter les incidents et les attaques liés à des menaces avancées sur les appareils mobiles et y répondre efficacement, il faut des outils particulièrement perfectionnés. Et comme il s'agit de terminaux mobiles, la détection des attaques et la réponse aux incidents doivent pouvoir se faire à distance. Et c'est précisément ce que permet la convergence de la sécurité des terminaux de bureau et mobiles qui :

- Effectue des analyses approfondies pour identifier les indicateurs de compromission
- Établit la chronologie des événements suspects pour montrer quand et comment les appareils ont été compromis.
- Présente des résumés d'incidents clairs et lisibles, qui mettent en évidence les attaques sophistiquées de type « zero-day », autrement invisibles
- Élimine les APT grâce à des outils intégrés tandis que la surveillance continue garantit la neutralisation des menaces.

Résumé

Pour combler les lacunes de sécurité, il faut adopter une approche moderne de la cybersécurité. Une superposition de protections complètes, pour étendre la sécurité et la protection de la vie privée à l'ensemble des appareils, des utilisateurs et des données de votre infrastructure. Une solution unique et puissante de défense en profondeur, qui intègre la gestion, l'identité et la sécurité.

© 2024 Jamf, LLC. Tous droits réservés.