jamf

Évaluer les besoins de sécurité de votre organisation

Une démarche essentielle pour votre posture de sécurité globale

Comprendre les besoins uniques de votre organisation en matière de sécurité est un art qui relève à la fois de la théorie et de la pratique. Malgré cette dualité, il reste fermement ancré dans la logique. Il s'appuie en effet sur les données de vulnérabilité recueillies lors des évaluations des risques, ainsi que sur la télémétrie des terminaux collectée par le biais de la visibilité et de la surveillance. Il repose enfin sur une excellente connaissance des exigences réglementaires en vigueur. Tous ces éléments, lorsqu'ils sont combinés, orientent l'acquisition d'outils de sécurité et aident les organisations à atteindre (et préserver) leurs objectifs de conformité.

Pour assurer le succès de votre organisation à long terme, vous devez prendre son pouls en permanence. Demandez à n'importe quel dirigeant d'entreprise comment rester performant, et il vous répondra certainement que vous devez comprendre les besoins de votre organisation et exploiter ces informations à bon escient, de manière à minimiser les risques tout en maximisant les opportunités de progrès. C'est particulièrement vrai pour ceux qui ont réussi à maintenir leurs activités malgré les ralentissements économiques et les crises sanitaires, parfois sur plusieurs décennies.

Dans ce document, nous abordons plusieurs thèmes clés :

- Ce qu'est le risque, et comment les données télémétriques collectées apportent une visibilité sur l'état des appareils et la posture de sécurité globale
- Pourquoi l'évaluation des risques doit être une démarche récurrente et itérative, intégrée à la gestion de la pile de sécurité
- Comment ces données aident votre organisation non seulement à déterminer ses besoins de sécurité, mais peuvent aussi la protéger contre les risques actuels et futurs
- Pourquoi l'intégration des données de risque aux solutions de sécurité des terminaux permet de maintenir une posture de sécurité forte tout en respectant les objectifs de conformité de l'organisation

Cette conviction est valable quel que soit le type d'entreprise que vous dirigez. Prenez les films et la musique, par exemple. Le divertissement existe depuis des siècles. À des degrés divers, elle a résisté à l'épreuve du temps en comprenant les attentes de son public cible et en transformant son offre pour mieux y répondre.

C'est un processus continu et évolutif.

Et la cybersécurité fonctionne à peu près de la même manière. Mais plutôt que d'évaluer les exigences de leurs clients, ce sont leurs propres opérations que les organisations doivent examiner, afin de déterminer ce qui est nécessaire au maintien de la continuité et de la sécurité de leurs activités commerciales. L'évaluation des risques porte sur tous les actifs, des appareils aux données en passant par l'infrastructure et les logiciels, et englobe les processus et les règles de votre organisation. Ce sont en effet toutes les pièces du puzzle de la posture de sécurité.

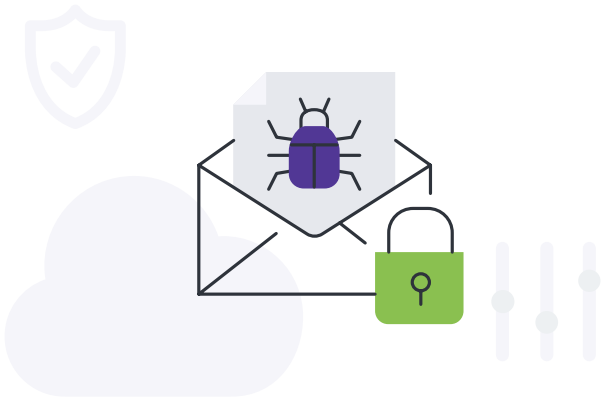
Fortes de ces informations, les organisations vont évaluer les risques et les vulnérabilités de leur stratégie de cybersécurité actuelle. Elles pourront ensuite passer à l'action pour les corriger et atténuer les menaces.

L'évaluation des risques n'est pas un processus isolé. Les bonnes pratiques recommandent de la renouveler à intervalles réguliers La technologie est dynamique par nature, et tout état est nécessairement transitoire. Cette situation est lourde de conséquence sur le plan de la sécurité : les bogues, aussi inévitables que récurrents, créent des vulnérabilités qui abaissent la posture de sécurité. En bout de ligne, ce sont les appareils, les utilisateurs et les données qui sont exposés.

Et c'est sans compter les acteurs malveillants qui sondent et testent activement les défenses de votre réseau à la recherche de signes de faiblesse et de vecteurs d'attaque à exploiter.

En d'autres termes, l'évaluation des risques doit être effectuée régulièrement et s'inscrire dans le cadre d'une stratégie globale de cybersécurité. Les données d'évaluation obtenues ne doivent pas seulement être utilisées pour connaître l'état actuel de la sécurité ; elles doivent aussi informer de manière itérative le plan holistique de défense en profondeur de l'organisation, qui vise à :

- Établir les étapes du cycle de vie des appareils et des applications
- Fournir, configurer et déployer des contrôles de sécurité
- Atteindre les objectifs réglementaires et assurer la conformité
- Identifier les menaces existantes et émergentes, et leur attribuer des niveaux de criticité et de gravité
- Maintenir l'alignement entre la tolérance au risque et les stratégies d'atténuation
- Réviser et mettre en œuvre des procédures de réponse aux incidents
- Mettre à jour et instituer des stratégies de prévention des menaces, telles que la formation des utilisateurs finaux.



Évaluation des risques

Nous avons compris l'importance de l'évaluation des risques, mais en quoi consiste-t-elle exactement ? Quels actifs sont réellement en danger ? Si les détails varient selon l'organisation et son secteur, il s'agit essentiellement de comprendre :

- Le paysage des menaces
- Les vulnérabilités de votre organisation
- La probabilité d'une attaque
- L'impact d'une attaque sur votre organisation
- La rapidité avec laquelle votre organisation peut se remettre d'une attaque grave

> *« Pour connaître son ennemi, vous devez devenir votre ennemi. »* **– Sun Tzu**

Voyons à quelles questions une évaluation des risques doit répondre.

Quelles sont les zones de vulnérabilité de mon organisation ?

Matériel, logiciels, interfaces et interactions des fournisseurs avec votre infrastructure réseau… un attaquant peut utiliser de nombreux points d'entrée pour exploiter votre système. Il peut également cibler tout utilisateur qui a accès à ces composants. Les vulnérabilités peuvent également se trouver dans les processus et les règles de votre entreprise.

Vous devez inventorier et classer tous ces composants pour avoir une bonne compréhension de votre infrastructure. Vous avez besoin de savoir :

- Quels appareils accèdent à votre réseau
- Qui a accès à vos données
- Si vous appliquez les bonnes pratiques de sécurité (principe du moindre privilège, obligation de mot de passe fort, etc.)
- Si vos fournisseurs introduisent des vulnérabilités dans vos systèmes
- Si les utilisateurs sont formés à reconnaître les menaces potentielles et à pratiquer une bonne hygiène de sécurité

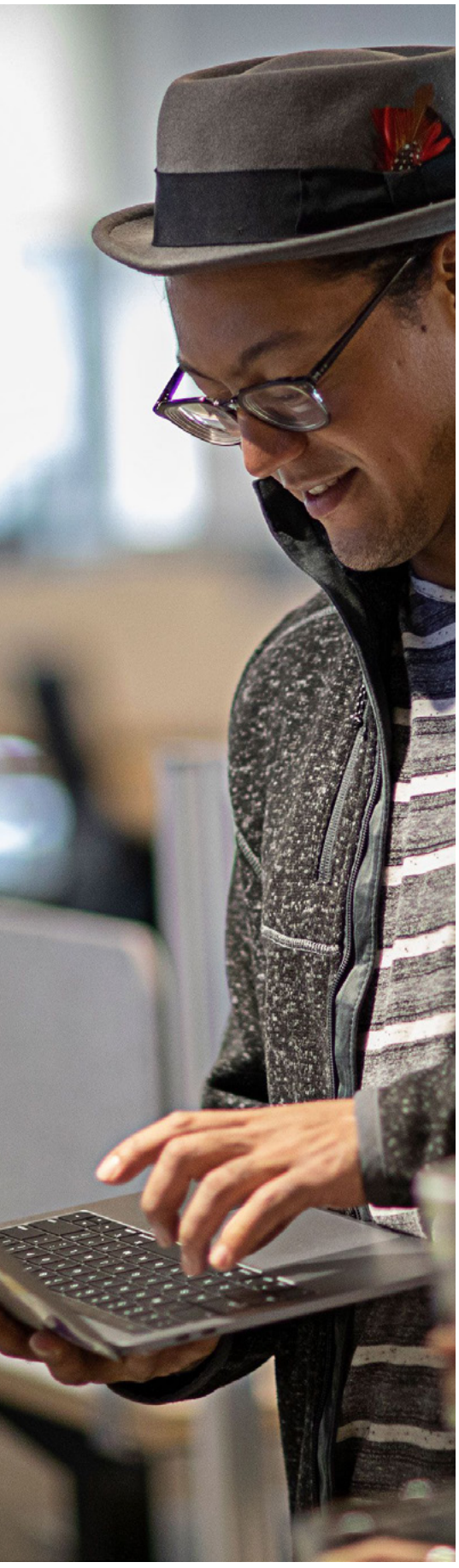
Quelles sont les menaces ?

L'évaluation des risques implique également de connaître les menaces existantes et l'impact qu'elles peuvent avoir sur votre système. Vos équipes informatiques et de sécurité pourront alors identifier la partie la plus vulnérable de votre organisation, la probabilité d'une attaque et ses conséquences potentielles.

EXEMPLE

Le cadre MITRE ATT&CK aide les équipes de sécurité à mieux comprendre de quelle façon des pirates pourraient attaquer votre système. Et pour faire face aux menaces inconnues, elles peuvent se tourner vers la recherche des menaces et l'utilisation de logiciels d'IA et de machine learning (ML), conçus pour identifier les comportements suspects ou malveillants. L'IA et le ML travaillent sans relâche en coulisses pour identifier toute anomalie par rapport au comportement de référence de votre réseau. Capables de traiter de vastes ensembles de données de renseignement sur les menaces et de reconnaissance de schémas, ces outils doivent occuper une place de choix dans votre arsenal de cybersécurité. De plus, les données qu'ils collectent peuvent être partagées avec l'ensemble de la communauté de la sécurité, afin d'enrichir la base de connaissances sur les menaces à l'échelle mondiale.

Si vous connaissez les vecteurs de menaces les plus courants, vous pourrez traiter en priorité les parties de votre organisation qui ont le plus besoin d'être défendues. Les menaces prennent de nombreuses formes. Selon le **Rapport 2023 de Verizon sur les enquêtes sur les violations de données**, les attaquants s'infiltrent dans les organisations en volant des identifiants, en recourant au phishing et en exploitant des vulnérabilités. En général, les violations de données proviennent de sources totalement externes, mais une part non négligeable (jusqu'à 40 %) des failles s'appuie sur l'exploitation de logiciels de partenaires. Pour se défendre contre ces menaces, il faut procéder à une analyse approfondie des configurations et des règles en vigueur. Nous y reviendrons plus tard.



Quel serait l'impact d'une cyberattaque sur mon organisation ?

Comprendre la probabilité d'une menace permet d'établir des priorités dans votre stratégie de défense. Mais vous devez également évaluer l'impact d'une menace sur la mission de votre organisation, en particulier sur le plan financier : en moyenne, le coût total d'une violation de données s'élevait à 4,35 millions de dollars en 2022, selon le **rapport d'IBM sur le coût d'une violation de données**. Pensez également au temps perdu, car il faut en moyenne 277 jours pour identifier et contenir une violation. N'oubliez pas non plus les conséquences sur vos relations avec les clients. La réputation n'est pas le seul enjeu : 60 % des organisations touchées par une violation en 2022 ont dû augmenter leurs prix. Il faut enfin tenir compte des éventuelles amendes infligées par les autorités de régulation en cas de défaut de conformité.

Quelle est l'étape suivante ?

Naturellement, plus l'impact d'une attaque est important, plus la défense des systèmes concernés devient prioritaire. Il en va de même pour les attaques dont la probabilité est plus élevée. La combinaison de ces deux paramètres – l'impact et la probabilité – permet de quantifier le risque que certaines menaces représentent pour votre organisation. Armé d'une bonne compréhension du risque, vous saurez établir des priorités et identifier plusieurs éléments clés :

- Quels systèmes critiques ont le plus besoin d'être protégés (ceux dont la défaillance entraînerait la plus grande perte de fonctionnalités stratégiques)
- Quels contrôles mettre en place pour une stratégie de défense optimale
- Quels outils logiciels peuvent améliorer votre posture de sécurité
- Le niveau de risque que vous pouvez supporter (votre tolérance au risque)

Il est maintenant temps de mettre en œuvre les enseignements tirés de votre évaluation des risques. Dans les prochaines sections, nous aborderons la télémétrie de votre réseau et de vos appareils, ainsi que les directives à suivre pour élaborer et revoir vos règles de sécurité.

Visibilité et suivi

Vous avez évalué les risques, vous les avez identifiés et vous avez établi votre degré de tolérance. Vous avez également fait quelques changements pour mettre en place et configurer des contrôles de sécurité, afin d'atténuer les risques identifiés. Votre posture de sécurité est solide. Les membres de l'organisation ont reçu la formation nécessaire pour identifier les menaces actuelles. Ils savent qu'elles doivent systématiquement être signalées et prises en charge. Les terminaux sont protégés contre les menaces, les objectifs de conformité sont atteints, tous les appareils sont conformes. Et maintenant ?

Peut-on dire que les équipes informatiques et de sécurité ont terminé leur travail et qu'elles peuvent prendre des vacances bien méritées ? Malheureusement, non.

La technologie reste profondément dynamique et, dans notre contexte, cela veut dire une chose : ce qui est sécurisé aujourd'hui ne le sera pas nécessairement demain. Pour protéger vos appareils, votre infrastructure et votre organisation des menaces de sécurité omniprésentes, vous devez connaître l'état des terminaux à tout moment.

> *« On ne peut conduire une armée en marche sans connaître pas la physionomie du pays… »*
> **– Sun Tzu, L'art de la guerre**

Les données télémétriques enregistrées par la surveillance active de l'état des appareils contiennent une mine d'informations utiles pour préserver la posture de sécurité des appareils et de l'organisation. D'ailleurs, puisque nous abordons la question de la conformité, sachez que les données télémétriques sont essentielles pour s'assurer que les terminaux sont configurés conformément aux exigences réglementaires – et apporter la preuve de leur conformité à tout moment. C'est crucial pour obtenir une certification réglementaire, comme **PCI-DSS** pour les organisations qui souhaitent accepter et traiter des paiements par carte en toute sécurité.

De plus, la visibilité obtenue grâce à la surveillance permet de prendre des décisions éclairées tout au long du cycle de vie des appareils et des applications. Le processus de surveillance apporte aux équipes informatiques ou de sécurité des informations actualisées sur l'état de leurs appareils, les logiciels qui s'y exécutent et certaines activités des utilisateurs finaux. Mais il offre aussi aux administrateurs et à la gestion de riches données de télémétrie, très utiles pour prendre des décisions visant à garantir la conformité des appareils et la sécurité des utilisateurs et des données.

Quel type de données la surveillance permet-elle de collecter ?

Avant d'examiner les données télémétriques recueillies, rappelons qu'il existe deux types de surveillance :

- **Passive :** les données de santé sont collectées lentement, généralement sur une période définie pour minimiser l'impact sur l'utilisateur final ou les performances de l'appareil. Parce que la capture des données est intermittente, la collecte de la télémétrie peut être lente et retarder la création d'un profil de référence complet. En outre, tout retard peut avoir une incidence directe sur l'exactitude ou l'actualité des données, en particulier si des jours ou des mois s'écoulent entre les captures.
- **Active :** les données de santé sont régulièrement communiquées par les terminaux. Les terminaux sont sondés à intervalle régulier et les informations sont transmises à un référentiel centralisé, souvent en temps réel.

Dans les deux cas, les données capturées sont identiques ou presque. Pourtant, les deux approches présentent des différences majeures à plusieurs égards :

- **Méthode** de capture des données télémétriques
- **Temps** nécessaire à l'établissement d'un profil de référence
- **Exactitude** des informations
- **Fréquence de mise à jour** des données de télémétrie

Certes, les deux types de surveillance ont chacun leurs avantages et leurs inconvénients. Mais une chose est claire : face à un paysage des menaces immense et en évolution rapide, seule une surveillance active s'avère efficace pour recueillir les données les plus récentes sur la santé des appareils. Une fois converties en informations exploitables, ces données permettent de combler les lacunes de votre plan de sécurité. Rappelez-vous l'axiome de la sécurité : « Vous ne pouvez pas protéger ce que vous ne voyez pas », cité dans l'article de SecurityWeek **Surveillance active ou passive : vous n'avez plus le choix.**

Les types de données télémétriques collectées et leur intérêt pour votre posture de sécurité :

- **Mises à jour des OS :** identifiez la version du système d'exploitation (OS) pour savoir si les appareils possèdent les fonctionnalités et les protections les plus récentes afin de minimiser les vulnérabilités.
- **Correctifs des applications :** tout comme l'OS, les applications doivent recevoir des correctifs, qui rectifient des bugs et atténuent des vulnérabilités.
- **Paramètres de configuration :** le renforcement des appareils est essentiel à la posture de sécurité. L'objectif n'est pas seulement de les configurer pour une sécurité maximale : cela permet également de minimiser le risque de mauvaise configuration, **responsable de 21 % des failles de données causées par des erreurs (Rapport 2023 sur les enquêtes sur les violations de données, Verizon).**
- **Activité du réseau :** avec quel contenu web les appareils communiquent-ils ? Les connexions non fiables sont-elles sécurisées ? Sur quels ports voit-on des données circuler ? Les réponses à ces questions et à d'autres, essentielles, concernant l'utilisation du réseau, permettent de déterminer la posture de sécurité de vos appareils.
- **Analyse comportementale :** si les utilisateurs sont considérés comme le maillon faible de la chaîne de sécurité, c'est pour une excellente raison. Ce sont en effet les disparités dans leur connaissance du sujet qui expliquent le succès des attaques d'ingénierie sociale. Avec une meilleure visibilité sur le comportement des utilisateurs, les administrateurs ont une idée plus précise de la manière dont ils peuvent introduire des risques introduits – et ainsi s'en protéger.
- **Audit d'authentification :** les protocoles d'authentification et la gestion des mots de passe protègent les appareils et leurs données sensibles. Mais aussi robuste et complexe soit-il, un verrou ou un mot de passe complexe ne vous dit pas si les utilisateurs partagent leurs identifiants ou si leurs comptes ont été compromis. Et l'enjeu est encore plus grand dans les environnements de travail hybrides où une gestion basée sur des règles doit assurer la sécurité des terminaux distants.
- **Code malveillant :** le code malveillant peut se manifester sous différentes formes. Un cheval de Troie déguisé en application légitime, un programme installé par sideloading, la visite involontaire d'un site web compromis, une menace fonctionnant silencieusement en arrière-plan… Toutes ces nuisances peuvent compromettre la conformité d'un appareil, en particulier dans le contexte de la multiplication des attaques visant les mobiles, devenus omniprésents.
- **Enregistrement des erreurs :** les appareils enregistrent tout. Plus le parc à surveiller est vaste, plus il est difficile pour les administrateurs de traiter chaque problème signalé. Ce qui arrange bien les pirates. Mais cette situation est loin d'être inévitable. Avec une bonne gestion et l'appui d'une solution de gestion des informations et des événements de sécurité (SIEM) pour trier et interpréter ce grand flux de télémétrie, l'enregistrement des erreurs et la détection des menaces peuvent devenir extrêmement efficaces.
- **Processus système :** les administrateurs ont besoin de savoir quelles applications s'exécutent sur les appareils qu'ils supervisent. Toujours grâce au contrôle du profil de référence, ils sont avertis en cas d'utilisation d'outils non validés (Shadow IT) ou interdits, susceptibles de dégrader la sécurité, de faciliter les fuites de données ou **de mettre à mal la confidentialité des utilisateurs.**
- **Conformité aux audits :** la visibilité de la santé des terminaux concerne autant sur ce qu'on connaît que ce que l'on ignore. Dans les secteurs réglementés, les organisations qui veulent connaître leur posture de conformité doivent à la fois savoir comment atteindre leurs objectifs et collecter des preuves de leurs démarches.

Mais peut-on utiliser les données de télémétrie pour atténuer automatiquement les risques ?

Parfaitement, c'est possible. En effet, plusieurs facteurs rendent la gestion des risques beaucoup plus difficile :

- Acquisition de grandes quantités d'appareils de différents types
- Nécessité d'assurer la sécurité d'une flotte composée d'appareils d'entreprise et d'appareils personnels
- Prise en charge des employés en télétravail
- Convergence de deux types de menaces ou plus dans le cadre d'attaques complexes sur plusieurs fronts
- Application de réglages de sécurité pour maintenir la conformité des terminaux

Il est préférable d'automatiser la collecte, l'analyse et le tri des données télémétriques plutôt que d'effectuer chaque étape manuellement. Le volume de données à analyser est en effet considérable, chaque tâche doit être réalisée le plus rapidement possible – et les humains ont régulièrement besoin de s'arrêter pour se nourrir et se reposer.

Les ordinateurs ne font pas de pauses.

En confiant « le gros du travail » à des systèmes grâce à l'automatisation, les organisations gagnent du temps et économisent de précieuses ressources. Leurs équipes peuvent alors se concentrer sur la prévention des attaques plutôt que de faire face à leurs conséquences.

Après l'évaluation des risques, la surveillance active est la deuxième couche de votre plan de sécurité, et elle aussi permet d'établir les besoins de votre organisation. La surveillance continue de votre flotte collecte et transmet en temps réel des données télémétriques qui informent votre solution de sécurité des terminaux sur l'état des appareils. Les lacunes et les comportements anormaux détectés peuvent être automatiquement signalés aux équipes informatiques ou de sécurité (au minimum) qui pourront fixer les prochaines étapes. Les détections peuvent également servir à lancer des workflows automatisés de réponse aux incidents. Vous pourrez ainsi, par exemple, supprimer des logiciels suspects connus sur les appareils ou mettre en quarantaine des terminaux infectés par un ransomware

Des workflows plus sophistiqués encore deviennent possibles en intégrant les solutions de sécurité des terminaux à d'autres outils – gestion des identités, gestion des appareils mobiles (MDM) – pour décupler les capacités d'automatisation.

Conformité

Si ce document est ponctué de citations de L'art de la guerre de Sun Tzu, c'est pour relier d'un fil rouge les thèmes centraux que doivent aborder les professionnels de l'informatique et de la sécurité lorsqu'ils procèdent à l'évaluation des risques et des besoins de leur organisation en matière de sécurité. L'objectif est de combler les moindres lacunes tout en comprenant que chaque étape est cruciale en soi. Chacune d'elles collecte en effet des informations qui informent directement sur l'étape suivante.

Pour bien comprendre vos besoins de sécurité, vous ne devez pas seulement savoir quelles vulnérabilités sont présentes à un moment donné. Il faut également déterminer comment les corriger et quelles stratégies mettre en œuvre pour garantir la conformité de vos terminaux à vos règles, que votre organisation fasse ou non partie d'un secteur réglementé. L'objectif : rester en conformité aux normes de votre secteur ou, dans les secteurs non réglementés, à celles de l'entreprise. Dans les deux cas, vous cherchez à maintenir la sécurité et la confidentialité des utilisateurs en réduisant les risques. Pour cela, vous allez vous appuyer sur un cadre structuré pour préserver la posture de sécurité de vos appareils et de votre organisation.

> *« L'art suprême de la guerre consiste à soumettre l'ennemi sans combattre. »* **– Sun Tzu**

Dans n, les « ennemis » sont les pirates et tout ce qui peut introduire un risque dans votre organisation. Le risque provient en effet d'une vulnérabilité qui, si elle est exploitée, peut avoir des conséquences très lourdes. Mais au stade de l'évaluation des besoins, il n'est pas utile de s'inquiéter de la multitude d'ennemis potentiels qui planent au-dessus des réalités immédiates de votre réseau. Il vaut mieux s'intéresser à la diversité des risques eux-mêmes qu'à leur origine. C'est comme cela que les administrateurs pourront réellement déterminer la meilleure approche pour maintenir la conformité et protéger les appareils, les utilisateurs et les données contre les menaces actuelles et émergentes.

Quels workflows permettent d'identifier et de minimiser les différents types de risques ?

Il est important de faire la distinction entre directives, cadres et références avant de poursuivre. Les directives ont de simples affinités avec les bonnes pratiques. Il n'y a pas toujours de règles strictes à suivre – plutôt un ensemble de pratiques qui aident les organisations à gérer diverses formes de risque à un niveau général.

Les cadres, quant à eux, ont ADN est similaire à celui des bonnes pratiques. Ils visent à concaténer l'ensemble des informations, pratiques, réglages, contrôles et workflows nécessaires pour atteindre ou dépasser un objectif spécifique, que ce soit celui de l'organisation ou d'une autorité de réglementation.

Les profils de référence ont des points avec les deux précédents types de guide : ils poursuivent également un objectif de conformité, mais leur angle est différent. Les directives suggèrent des bonnes pratiques, les cadres les organisent de manière structurée dans un objectif particulier, mais les références ne sont pas mises en œuvre de la même manière. Elles jouent un rôle de baromètre : les organisations les utilisent pour mesurer leur performance par rapport à un objectif réglementaire ou commercial.

Pour simplifier, on peut voir les directives comme des ingrédients. En les assemblant, on obtient des cadres – ou un plat, si vous voulez. Enfin, les références sont les critiques qui déterminent si le plat a été préparé correctement, selon les ingrédients et la recette choisis. Bon appétit.

Une fois ces nuances comprises, nous pouvons utiliser ces cadres et ces références pour comprendre nos besoins de sécurité et y répondre le plus précisément possible.

Cadres couramment utilisés dans la planification de la sécurité

Le document **National Institute for Standards and Technology (NIST) SP 800-53, Rev. 5** : Security and Privacy Controls for Information Systems and Organizations (Contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations) fournit un catalogue de contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations. Son but : protéger les opérations et les actifs des organisations d'un large éventail de menaces et de risques.

Le document **NISTIR 8011, Vol. 4** : Automation Support for Security Control Assessments (Prise en charge de l'automatisation pour l'évaluation des contrôles de sécurité), se concentre sur l'automatisation de l'évaluation des contrôles de sécurité au sein de chaque fonction de sécurité de l'information. Il aborde également la gestion des risques créés par les défauts présents dans les logiciels sur le réseau.

ISO/IEC 27001 : systèmes de gestion de la sécurité de l'information (SGSI), est l'une des normes les plus employées pour définir les exigences auxquelles doit répondre un SGSI. Le cadre fournit des orientations globales pour définir, mettre en œuvre, maintenir et améliorer en permanence un système de gestion de la sécurité de l'information.

Cyber Essentials : cette initiative britannique donne des conseils pour protéger votre organisation, quelle que soit sa taille, contre toute une série de cyberattaques courantes. Elle se décompose en plusieurs niveaux et inclut un contrôle technique pour vérifier la conformité.

MITRE ATT&CK : base de connaissances globale sur les tactiques utilisées par les pirates, reposant sur l'observation de techniques réelles. Ce cadre sert de fondement au développement de modèles de menaces et de méthodologies spécifiques. Il est utilisé par divers secteurs et communautés, et on le retrouve fréquemment dans les solutions de sécurité terminaux.

Objectifs de contrôle pour l'information et les technologies connexes (COBIT) 2019 : ce cadre créé par l'ISACA définit des processus génériques de gestion informatique et les relie aux objectifs de l'entreprise et de l'informatique. Il décrit également des mesures pour assurer la responsabilisation des équipes. Flexible, il peut être à d'autres cadres, comme ISO 27001, ITIL et autres cadres de gestion de projet répandus.

Norme de sécurité des données de l'industrie des cartes de paiement (PCI-DSS) : ce standard de facto régit les exigences techniques et opérationnelles propres au traitement des données de paiement par carte de crédit. Il est appliqué par les principaux émetteurs de cartes à l'échelle mondiale.

Certification du modèle de maturité de la cybersécurité (CMMC) 2.0 : basé sur les exigences de sécurité de plusieurs publications spéciales du NIST, ce modèle à plusieurs niveaux fournit des niveaux de certification pour les organisations qui remplissent les critères cumulatifs des niveaux CMMC et respectent les pratiques associées dans tous les domaines.

Évaluation des risques de l'OWASP : composé d'outils de test de sécurité, d'évaluation des risques et d'analyse, ce cadre de l'OWASP vise à éliminer l'incertitude liée à la compatibilité et à la complexité des processus de configuration de l'environnement. Son but : fournir un moyen simple « d'analyser et d'examiner la qualité et les vulnérabilités du code sans aucune configuration supplémentaire » et « aider les développeurs à écrire et à produire du code sécurisé ».

Projet de conformité de la sécurité macOS : projet conjoint de l'équipe opérationnelle de sécurité informatique fédérale du NIST, de la NASA, de l'Agence des systèmes d'information de la défence (DISA) et du Laboratoire national de Los Alamos (LANL), cet effort open source vise à fournir une approche programmatique pour générer des conseils de sécurité. Il propose notamment des réglages de configuration qui peuvent être déployés pour se mettre en conformité avec des objectifs réglementaires spécifiques.

Le rôle des références dans la cybersécurité

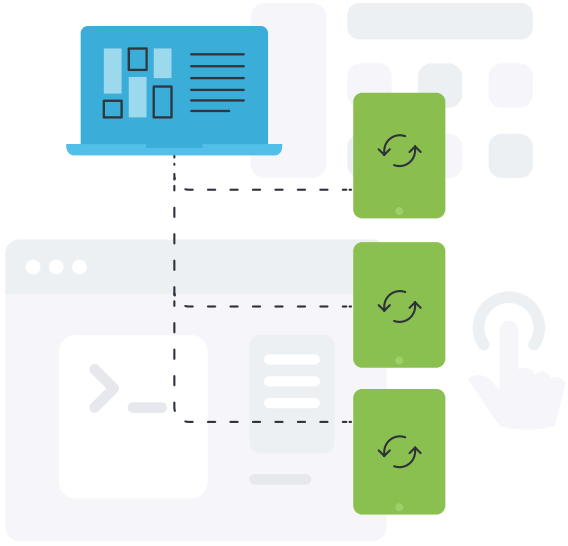
Guides de mise en œuvre technique de la sécurité (STIG) de l'Agence des systèmes d'information de la défense (DISA) : ces normes de configuration sont administrées par le ministère américain de la défense (DoD) et contiennent des exigences spécifiques pour la sécurisation des systèmes informatiques. Elles couvrent un large éventail de domaines – configurations logiques, protocoles et logiciels – et visent à « améliorer la sécurité des logiciels, du matériel, des architectures physiques et des architectures logiques afin de réduire davantage les vulnérabilités. »

Normes de traitement des informations fédérales (FIPS) 200 : également développées par le NIST pour les États-Unis, ces normes s'appliquent aux appareils et systèmes informatiques non militaires utilisés par l'administration américaine et ses sous-traitants. Si les standards FIPS couvrent un large éventail de bases de sécurité, FIPS 200 s'assure que les données utilisées par les agences fédérales ou en leur nom répondent aux exigences minimales de sécurité de l'information dans plusieurs catégories d'objectifs. Elles garantissent des niveaux appropriés de sécurité par rapport à différents degrés de risques et déterminent les niveaux d'impact des exigences de sécurité **selon la triade de la CIA**.

NIST SP 800-39 : orientations générales utiles lors de l'intégration à une solution de gestion pour les entreprises (ERM) complète. Le document fournit des détails spécifiques sur l'évaluation, la prise en charge et la surveillance des risques sur une base continue, en conjonction avec d'autres normes, directives et cadres.

Centre pour la sécurité d'Internet (CIS) : les critères du CIS sont des recommandations de configuration qui concernent plus de 25 familles de produits. Chaque critère est le fruit des efforts communs d'experts mondiaux en cybersécurité. Ces guides de configuration sécurisés sont acceptés et utilisés par les administrations et les secteurs dans le monde entier ; ils sont même intégrés comme base fondamentale dans certaines solutions de sécurité des terminaux.

Objectifs de performance de cybersécurité (CPG) de l'Agence pour la cybersécurité et la sécurité des infrastructures (CISA) : développés en coordination avec la CISA, le NIST et la communauté interagences, les CPG définissent des objectifs cohérents pour tous les types d'infrastructure critique. Ils aident en particulier les petites et moyennes organisations à mettre en place des initiatives de cybersécurité, et jouent le rôle de critères pour mesurer et améliorer la maturité en matière de cybersécurité.



Évaluation des risques + surveillance continue + directives de sécurité = conformité gérée.

> *« Connais-toi toi-même et tu gagneras toutes les batailles* **» – Sun Tzu**

Pris isolément, ces composants ont une vertu limitée pour les organisations. Mais si vous les réunissez, vous pourrez, dans un premier temps :

- Identifier vos points faibles
- Connaître l'état de santé de vos terminaux
- Réduire la surface d'attaque à l'aide de configuration durcies
- Atteindre vos objectifs de conformité

Mais ce n'est pas tout : vous allez aussi maintenir la conformité en établissant des références que vous suivrez grâce à une surveillance proactive et à des données télémétriques riches. Vous instaurerez ainsi un cercle vertueux qui améliorera en continu la posture de sécurité de vos appareils et celle de votre infrastructure dans son ensemble.

Comme on l'a vu, c'est un processus itératif, et pas un projet isolé. La boucle évoquée ci-dessus est celle d'un cycle permanent. L'ensemble des phases et des composants – contrôles de sécurité, processus, workflows, exigences, politiques, réglages des appareils, utilisateurs finaux et donnée sensible – s'informent et s'ajustent constamment les uns les autres.

Votre organisation fait peut-être partie d'un secteur réglementé. Ou bien, quelle que soit sa taille, elle souhaite tout simplement aligner sa stratégie de cybersécurité sur des règles des contrôles administratifs, une règle d'utilisation acceptable, par exemple. Dans tous les cas, vous pouvez voir tous ces composants comme les rouages d'une machine qui permet de mieux comprendre vos besoins de sécurité et quelles informations permettront de combler les lacunes.

Vous vous dites peut-être : « Je suis administrateur Mac. Je sais quels risques existent au sein de mon organisation et je suis submergé de données sur la santé des appareils. Toutes ces directives mettent en évidence le gouffre qui sépare notre situation actuelle de la conformité. Que devons-nous faire maintenant ? Comment parvenir la situation idéale ? »

C’est là que Jamf intervient.

Aider les organisations à réussir avec Apple.

Plus qu’un simple slogan, ces mots résument à eux seuls toute la mission de Jamf. C’est notre cœur de métier, tout simplement. Et quand nous affirmons que Jamf est la référence pour la gestion d’Apple en entreprise, ce ne sont pas que des mots. Jamf doit sa réputation aux solutions de pointe que nous développons et qui aident d’innombrables organisations à gérer et sécuriser des millions d’appareils, dans tous les secteurs d’activité et dans le monde entier.

Jamf vous accompagne jour après jour pour vous aider à exploiter tout le potentiel des produits Apple au travail. Vous vous demandez sans doute comment nous pouvons fournir les outils nécessaires à une gestion complète de votre flotte Apple, tout en comprenant et en répondant spécifiquement aux besoins et aux objectifs de conformité de votre organisation.

Éliminez l’incertitude de la validation des terminaux.

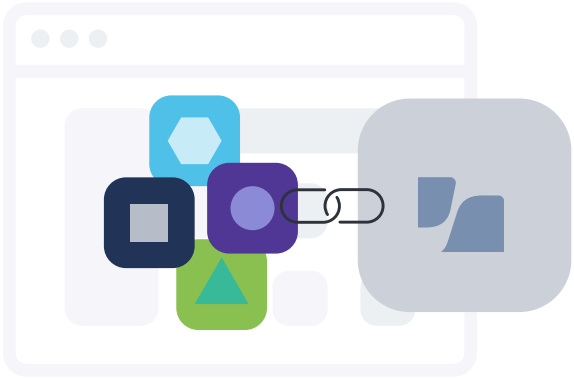
Pour comprendre vos besoins de sécurité, vous devez connaître l’état des terminaux utilisés au sein de votre organisation. Sans des données télémétriques détaillées pour vérifier l’état de chaque appareil, les administrateurs ne peuvent qu’émettre des suppositions qui, en cas d’erreur, peuvent avoir des conséquences désastreuses.

En tant qu’administrateur, **ce n’est pas tant que vous voulez savoir : vous devez savoir.** Pour être en conformité avec les réglementations comme avec les règles de l’organisation, vous devez vérifier l’état des terminaux en permanence.

L’ingénierie sociale est un vecteur d’attaque de choix pour les pirates. Elle cible spécifiquement le risque actuel d’une organisation et introduit un risque plus important encore, en compromettant des identifiants ou en injectant du code malveillant dans vos systèmes via des appareils infectés.

Des technologies telles que l’**accès réseau zero-trust** (ZTNA) protègent vos appareils en comparant l’état des terminaux à une série de critères ; seuls ceux qui répondent à un niveau de sécurité minimal reçoivent l’accès aux ressources qu’ils demandent. Conformément au credo « ne jamais faire confiance, toujours vérifier », une solution ZTNA telle que **Jamf Connect** vérifie que l’accès provient d’un appareil inscrit et fiable. Avec cette approche, la gestion des identités et des accès devient la pierre angulaire de votre stratégie de sécurité.

Les solutions de sécurité des terminaux, comme **Jamf Protect**, ajoutent un filet de sécurité à vos appareils macOS, iOS, iPadOS, Android et Windows. Elles les protègent, de même que leurs utilisateurs, contre les menaces potentielles, logiciels malveillants en tête. Pour ce faire, elles recherchent les menaces sur l’appareil et le réseau pour accélérer la réponse aux incidents et déclencher des workflows automatisés d’atténuation et de correction. **Et tout cela sans jamais faire de compromis sur la sécurité, la confidentialité et les performances.**



Cultivez la confiance dans votre infrastructure.

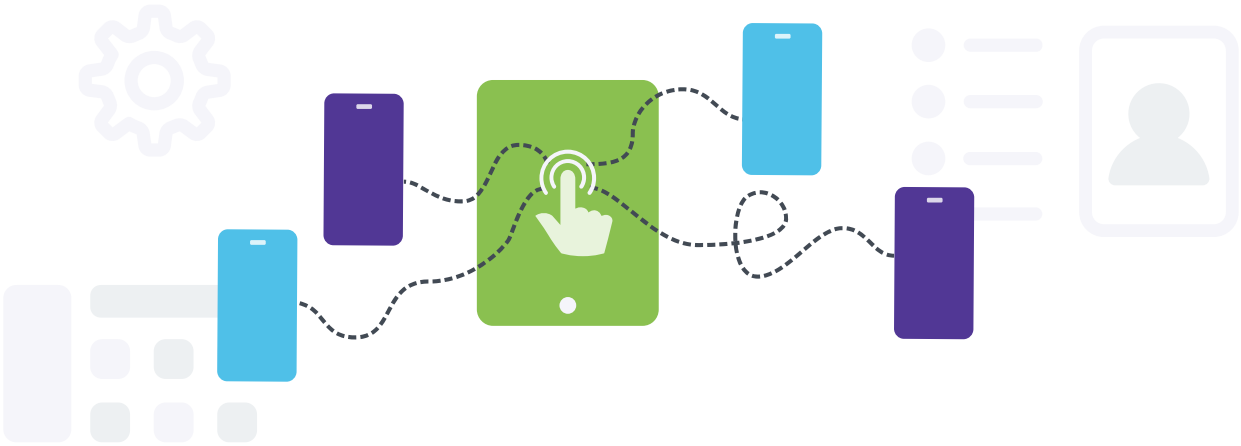
L'histoire ne commence pas au moment où un appareil se connecte pour la première fois aux ressources de l'entreprise, mais bien avant cela – avant même que l'appareil ne soit déballé. Je m'explique.

Avec le déploiement zero-touch, **un appareil est prêt à l'emploi dès que l'utilisateur final l'allume** pour la première fois. Ce workflow de déploiement intègre Apple Business Manager ou Apple School Manager avec Jamf, de façon automatique et parfaitement sécurisée.

Les appareils peuvent appartenir à l'entreprise ou aux utilisateurs finaux : **Jamf Pro** prend en charge plusieurs modèles de propriété, dont le BYOD. L'inscription de l'appareil par l'utilisateur garantit sa sécurité sans sacrifier le respect de la vie privée. Et puisque nous parlons de sécurité, notre solution MDM **prend en charge toutes les nouvelles fonctionnalités d'Apple le jour de leur sortie, à commencer les améliorations de sécurité et de confidentialité**. Vous pouvez ainsi faire profiter vos utilisateurs des outils qui les aident à être plus efficaces sans faire de compromis ou d'exceptions en matière de sécurité des terminaux.

La gestion des applications est un élément central de la sécurité. Le déploiement des mises à jour des systèmes d'exploitation (OS) et des applications est un enjeu majeur pour la réussite de tout plan de sécurité. En effet, à quoi bon comprendre vos besoins de sécurité si vous ne pouvez pas corriger les problèmes qui surviennent ? Une fois de plus, Jamf Pro s'illustre en **simplifiant la gestion du cycle de vie des applications pour les administrateurs Mac** : des commandes de gestion permettent d'appliquer les mises à jour de l'OS à des groupes d'appareils. Et n'oubliez pas les applications ! Le catalogue d'applications **Self Service** de Jamf, associé à la puissance des App Installers, met à la disposition des utilisateurs finaux toutes les applications utiles. Et vous ces applications sont toujours gérées, automatiquement mises à jour et dans leur état le plus sécurisé.

La simplification de l'approvisionnement des identités et des accès est l'un des piliers d'une stratégie de sécurité globale de défense en profondeur. Lorsqu'il s'agit de gérer des appareils, en particulier ceux d'équipes distribuées, l'approche Trusted Access change la donne : elle veille en effet à ce que les utilisateurs de confiance – et eux seulement – puissent accéder aux appareils et aux ressources, partout et à tout moment. Dotés d'un moyen simple de s'authentifier sur leurs appareils, les utilisateurs ont toutes les cartes en main pour réussir : de l'expérience d'onboarding transparente grâce au déploiement zero-touch à l'accès aux ressources d'entreprise dans leurs tâches quotidiennes. Le ZTNA et l'accès conditionnel avec **Jamf Connect** concrétisent l'idée qu'**une sécurité efficace, évolutive et flexible n'est pas un luxe mais une nécessité**.



Trois éléments de sécurité essentiels, une plateforme fiable

> *« Les opportunités se multiplient quand on les saisit. »* **– Sun Tzu**

Trusted Access est une approche holistique de la sécurité. Complète, elle répond aux besoins de gestion et de sécurité de toutes les organisations, quel que soit leur secteur d'activité.

Chaque élément de Trusted Access – **gestion des appareils**, **protection des terminaux**, **visibilité et conformité** – joue un rôle crucial dans une stratégie de sécurité efficace de défense en profondeur. Cette approche superpose des contrôles d'accès avancés à des configurations sécurisées pour les appareils, les utilisateurs et les données. Elle s'appuie également sur des données de télémétrie pour s'adapter à toute évolution de la posture de sécurité de vos appareils ou de votre organisation, avec un triple objectif : maintenir la sécurité, préserver la confidentialité et rester en conformité avec la loi.

Pour votre flotte Apple, c'est une garantie de flexibilité et de sécurité partout, à tout moment, sans la moindre complexité.

Jamf peut vous aider à évaluer vos besoins de sécurité. Contactez-nous pour découvrir nos solutions de référence.

Lancez-vous

Vous pouvez également contacter votre revendeur pour essayer Jamf gratuitement.

jamf

www.jamf.com/fr