jamf

Comprendre les cadres de sécurité

Les plans de cybersécurité atténuent les risques et protègent l'entreprise contre les menaces, en réduisant autant que possible les vecteurs d'attaque potentiels. Les stratégies de sécurité holistiques varient considérablement d'une organisation à l'autre, car elles doivent prendre en compte les spécificités de chacune. Le rôle de la conformité aux exigences réglementaires est directement lié aux besoins. Et nous ne parlons pas encore des innombrables aléas qui affectent la sécurité des organisations, confrontées au paysage moderne des menaces et à ses acteurs malveillants.

Avec toutes ces variables en jeu, on pourrait penser qu'un plan de cybersécurité est très difficile à établir, mais ce n'est pas forcément le cas.

C'est là qu'interviennent les cadres de sécurité et les avantages qu'ils procurent aux organisations de toutes tailles et de tous secteurs. Vous découvrirez, entre autres choses, leur rôle dans l'élaboration de stratégies cohérentes, conçues pour minimiser les facteurs de risque et atteindre les objectifs de conformité.

La mise en œuvre à grande échelle et la gestion quotidienne des contrôles et des solutions de cybersécurité sont le reflet de la qualité de la gestion des risques informatiques au sein de votre organisation – qu'elle soit bonne ou mauvaise.

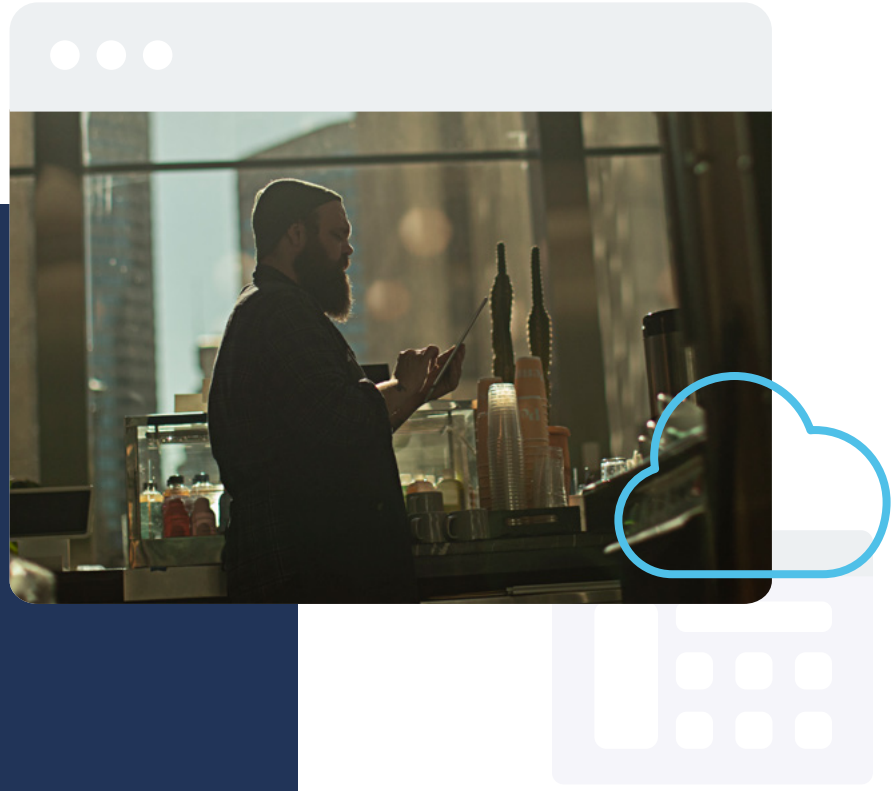
De nombreux facteurs influencent la réussite d'un plan de cybersécurité :

- La taille de votre organisation
- Les contraintes budgétaires
- Les exigences réglementaires (le cas échéant)
- Les besoins propres à la continuité des activités
- Des évaluations complètes et précises des risques
- Les connaissances et les compétences des équipes informatiques et de sécurité

La liste ci-dessus est loin d'être exhaustive, mais elle met en évidence les points essentiels à la réussite d'un plan de sécurité. Même armées de ces informations, les organisations peuvent hésiter à se lancer. Elles craignent qu'il n'existe **d'autres variables inconnues**, ou que des limitations touchant les facteurs ci-dessus ne créent des difficultés au moment de choisir le matériel, les logiciels, les configurations, les règles et les workflows qui répondront à leurs besoins de cybersécurité.

Les cadres visent spécifiquement ces écueils et bien d'autres en fournissant une feuille de route claire et concise pour accompagner les organisations dans la rédaction et la gestion de leurs plans de cybersécurité.

QU'EST-CE QU'UN CADRE ?



Nous avons utilisé le terme de « feuille de route » pour parler des cadres. Une autre analogie, peut-être plus précise sur le plan technique, serait « plan ». De la même manière qu'un entrepreneur utilise un plan pour construire un bâtiment solide, les équipes informatiques et de sécurité peuvent (et doivent) utiliser l'un de ces cadres pour déployer un plan de sécurité capable de :

- Identifier
- Protéger
- Détecter
- Répondre
- Restaurer

Les cadres mis en œuvre devraient fonctionner ensemble pour atténuer les risques de cybersécurité. Ils s'appuient pour cela sur des pratiques et des méthodes optimales, concises, organisées et approuvées par le secteur.

LES TYPES DE CADRES

Il existe plusieurs cadres différents. Chacun d'entre eux aborde et renforce un élément particulier de l'informatique ou de la sécurité de l'information. Certaines fournissent des conseils généraux pour protéger votre infrastructure contre les menaces actuelles et à venir. D'autres vous guident dans l'amélioration des processus afin de renforcer l'efficacité des services de gestion informatique. D'autres encore se concentrent exclusivement sur le renforcement de votre posture de sécurité dans le cadre de scénarios spécifiques. On les retrouve notamment dans les environnements réglementés, comme les secteurs de la santé, de la finance ou de l'éducation.

CADRES ET RÉGLEMENTATIONS COMMUNS DE CYBERSÉCURITÉ

CADRES

Cadre de cybersécurité (CSF) v1.1 du National Institute of Standards and Technology (NIST) : relevant du ministère américain du Commerce, le NIST a pour mission de promouvoir la compétitivité industrielle. Ses programmes s'étendent sur plusieurs laboratoires, notamment dans le domaine des technologies de l'information et de la sécurité. Le CSF est le fruit d'un effort continu de collaboration entre l'industrie, des universités et des administrations pour renforcer les infrastructures critiques de cybersécurité dont l'exploitation créerait des risques financiers et réputationnels importants.

Publication spéciale (SP) du NIST 800-53, Rév. 5 : traite des risques de sécurité et de confidentialité. Il fournit un catalogue de contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations, afin de les protéger contre un large éventail de menaces et de risques (mauvaises configurations, acteurs malveillants, erreur humaine, etc.). Flexibles et personnalisables, les contrôles préconisés aident les organisations à atténuer les risques tout en préservant la fonctionnalité et la fiabilité des systèmes informatiques.

ISO/IEC 27001 : Cette norme définit les critères que doivent remplir les systèmes de gestion de la sécurité de l'information (SGSI) et fournit des directives pour établir, mettre en œuvre, maintenir et améliorer en permanence un SGSI. Elle rassemble des bonnes pratiques et des principes au sein d'un standard internationalement reconnu, valable pour les entreprises de toutes tailles et de tous secteurs.

MITRE ATT&CK : c'est une 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.

CADRES

Contrôles des systèmes et des organisations (SOC) de l'American Institute of Certified Public Accounts (AICPA) : cette suite de trois rapports, intitulés SOC 1, SOC 2 et SOC 3, fournit des informations détaillées et des garanties sur les contrôles à mettre en place au sein d'une organisation de services. Ces contrôles concernent la sécurité, la disponibilité et l'intégrité des systèmes utilisés dans la manipulation et le traitement des données sensibles, et s'accompagnent de garanties pour les utilisateurs des services.

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 forment même la base fondamentale de certaines solutions de sécurité des terminaux.

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 défense (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 pour la sécurité et la conformité des appareils macOS d'Apple.

RÉGLEMENTATIONS

Loi sur la portabilité et la responsabilité en matière d'assurance santé (HIPAA) : cette loi modernise la circulation des informations de santé et impose plusieurs exigences au traitement des informations de santé protégées (PHI), notamment en stipulant des limites à la divulgation des données de santé des patients ainsi que les conséquences en cas de violation de la loi.

Loi Sarbanes-Oxley de 2002 (SOX) : cette loi fédérale impose aux organisations du secteur financier un certain nombre d'obligations concernant la tenue des registres et la déclaration des informations financières dans le secteur de la finance.

Directive sur la sécurité des réseaux et des systèmes d'information (NIS) : ce mandat européen de l'Agence de l'Union européenne pour la cybersécurité (ENISA) exige que les États membres incorporent dans leurs lois nationales respectives des règlements visant à augmenter le niveau de protection de cybersécurité. Ces obligations couvrent aussi bien le signalement des incidents de sécurité que la façon dont les équipes de sécurité doivent les traiter.

Règlement général sur la protection des données (RGPD) : cette loi axée sur la confidentialité a été développée pour l'Europe, mais elle a un impact sur toutes les organisations qui traitent des données de citoyens de l'UE. Les directives de conformité couvrent tous les aspects de la vie privée des utilisateurs : utilisation des cookies, vie privée en ligne, « droit à l'oubli » de l'utilisateur et bien d'autres encore.

Loi sur les droits et la confidentialité en matière d'éducation(FERPA) : cette loi fédérale américaine protège la confidentialité des étudiants et les données de leur dossier scolaire. Elle prévoit le droit d'accéder à ces informations et de modifier toute information incorrecte. Pour les mineurs, ce droit est étendu au parent ou au tuteur. Toutefois, lorsque l'étudiant atteint l'âge légal (18 ans aux États-Unis) ou fréquente un établissement d'enseignement supérieur, ces droits lui sont transférés de façon exclusive.

COMMENT UTILISER CES CADRES DANS LE CADRE D'UNE STRATÉGIE DE SÉCURITÉ GLOBALE ?

Il n'est pas forcément difficile de mettre en œuvre un cadre visant à renforcer votre posture de sécurité en s'appuyant sur les bonnes pratiques et des méthodologies solides. Avec une bonne approche, cette démarche peut s'intégrer à votre plan de sécurité et vos outils actuels. Elle va alors renforcer la conformité par le biais de processus et de workflows sécurisés.

La méthode « traditionnelle » d'implémentation consiste à comparer manuellement une évaluation récente de votre posture de sécurité aux critères d'un cadre. Vous allez ensuite, point par point, identifier les configurations, les réglages, les protocoles, les processus, les workflows et les règles qui ne répondent pas aux exigences de conformité. Et ce n'est que la première partie du processus manuel. La deuxième consiste à corriger manuellement chaque élément anormal pour le mettre en conformité.

Et comme la sécurité évolue constamment, le processus sera à renouveler. Il faut en effet vérifier régulièrement que les terminaux sont sécurisés et conformes.

Plusieurs défis affectent la fréquence, la précision et le succès de l'intégration manuelle des cadres à votre plan de cybersécurité :

- Nombre et types d'appareils dans votre flotte
- Taille et compétences de vos équipes informatiques et de sécurité
- Les ressources – temps, budget – allouées à ce processus
- Niveau de soutien de la direction
- Conflit avec les impératifs de la continuité des activités
- Impacts sur la productivité des utilisateurs, temps d'arrêt et obstacles
- Capacités des outils de sécurité actuels

Maintenant que nous avons vu le processus manuel éliminé, passons à ce que les administrateurs espèrent vraiment : un moyen automatisé d'intégrer les cadres à leur plan de cybersécurité. Une solution qui n'alourdisse pas encore la charge des équipes informatiques et de sécurité, mais qui les aide au contraire :

- À prendre en charge les préoccupations de sécurité de façon rapide et efficace
- À intégrer en toute simplicité les outils de gestion les plus performants
- À utiliser des workflows avancés et une gestion basée sur des règles pour automatiser les mesures d'atténuation
- À confier les tâches les plus pénibles aux outils de sécurité, quelle que soit la taille de l'équipe.
- À éliminer les lourdeurs administratives pour consacrer plus de temps à d'autres tâches
- À surveiller les terminaux en permanence, pour fournir une visibilité en temps réel sur la santé des appareils
- À corriger les appareils non conformes partout, à tout moment, grâce à des solutions basées dans le cloud
- À automatiser les processus en continu en s'adaptant de manière dynamique à l'évolution de la posture de sécurité, afin d'assurer la conformité avec les cadres au fil du temps

Pour automatiser la mise en œuvre des cadres de sécurité, on peut notamment utiliser des solutions de sécurité des terminaux qui intègrent déjà ces cadres. Par exemple, le cadre MITRE ATT&CK figure dans plusieurs solutions de sécurité des terminaux en tant que composant de base. Elles rapprochent les données d'analyse comportementale des menaces répertoriées dans la base de données MITRE ATT&CK pour accélérer la détection. D'autre part, des workflows de correction intégrés remédient aux risques dans le cadre d'une surveillance continue.

Une autre approche consiste à tirer parti de votre solution de gestion des appareils mobiles (MDM) et du cadre mSCP : vous générez les fichiers nécessaires à la conformité et vous les importez dans votre solution MDM afin d'automatiser la mise en conformité.

EXEMPLE

Une organisation peut, par exemple, utiliser mSCP pour établir une base de référence personnalisée répondant aux exigences d'HIPAA en s'appuyant sur le cadre NIST SP 800-53r5, afin de mettre en conformité HIPAA les terminaux inscrits dans votre MDM. L'étape suivante consiste à utiliser mSCP pour générer des fichiers personnalisés :

- **Profils de configuration :** fournit les réglages gérés, personnalisés selon les besoins de votre organisation.
- **Scripts de conformité :** deux scripts ; le premier pour auditer les appareils gérés et établir leurs besoins de sécurité, le deuxième pour apporter les corrections requises par le niveau de conformité souhaité.
- **Fichiers PLIST :** ces fichiers sont utilisés pour vérifier l'état de la conformité et enregistrer les résultats des audits.
- **Feuilles de calcul :** à remettre aux contrôleurs et enquêteurs tiers chargés de déterminer les niveaux de conformité.
- **Rapports :** rapports HTML et PDF décrivant chaque paramètre contrôlé du point de vue de la conformité, et fournissant des informations sur les aspects vérifiés, les réglages conformes et les mesures de correction à appliquer.

Ces fichiers permettent aux administrateurs d'importer des profils de configuration personnalisés (qui n'existent pas encore dans la MDM) et les déployer dans leur flotte. Mais c'est lors du chargement des scripts de conformité que la magie opère. Quand le script d'audit est configuré pour s'exécuter selon votre calendrier – une fois par jour, par exemple, il actualise quotidiennement l'enregistrement de l'appareil dans la MDM et ses données d'inventaire. Cela permet d'automatiser la collecte indispensable des données télémétriques, qui déterminent si un appareil conforme à la loi HIPAA. On charge ensuite le script de correction, configuré pour s'exécuter dans le cadre d'une règle. Les administrateurs ont ainsi la possibilité de cibler la correction, qui se produira uniquement sur les appareils non conformes. Quand le script de correction s'achève, il déclenche une actualisation de l'inventaire des appareils afin de mettre à jour leurs enregistrements et transmettre leur statut de conformité à la MDM.

En automatisant la conformité grâce à l'intégration des cadres via votre solution MDM, vous pourrez appliquer aux appareils une configuration sécurisée afin d'atteindre vos objectifs de conformité, en bénéficiant des avantages des outils cloud en termes de sécurité des terminaux et de confidentialité. Si un appareil devient non conforme, les scripts automatisés identifient les paramètres concernés et corrigent le problème. La remédiation se fait à tout moment, partout et sur n'importe quel réseau, sans que les équipes informatiques ou de sécurité n'aient à intervenir physiquement sur l'appareil. En intégrant vos solutions MDM et de sécurité des terminaux via une connexion API sécurisée, vous pouvez partager la visibilité et la surveillance continue. Cette approche permet de créer des workflows avancés pour accélérer la réponse aux incidents, dans l'esprit de la technologie SOAR (orchestration et automatisation de la réponse de sécurité), afin d'automatiser la coordination des tâches de remédiation.

AVANTAGES ET LIMITES DES CADRES DE SÉCURITÉ

Les cadres sont excellents pour aborder une myriade de problématiques. Nous avons vu ce que sont (et ne sont pas) les cadres. Nous allons maintenant nous pencher sur ce qu'ils peuvent faire et ne pas faire.

Ils peuvent

- Structurer les exigences de conformité en ensembles de catégories organisés
- Mettre en forme les détails des atténuations conformément aux bonnes pratiques et aux méthodologies du secteur
- Servir de modèle aux organisations dans leur démarche de conformité
- Fournir une base solide pour la mise en place d'un programme complet de cybersécurité

Ils ne peuvent pas

- Protéger les organisations contre les conséquences des risques atténués ou non atténués
- Être obligatoires – rien n'oblige à les implémenter, en partie ou en totalité
- Prescrire explicitement le respect de la solution. De nombreux cadres de conformité, comme l'HIPAA, ne sont pas normatifs : ils ne disent pas explicitement comment mettre en œuvre la conformité au mieux
- Assurer eux-mêmes la protection. Ils ne font que donner des indications sur ce que devrait être un plan de sécurité complet
- Limiter le délai entre deux mises à jour. Par conséquence, certaines informations peuvent être au mieux obsolètes, au pire en décalage total par rapport au paysage moderne des menaces.
- Être ajoutés aux contrôles de sécurité : ils ne permettent pas d'assurer la sécurité ou la conformité en dehors d'un plan de défense en profondeur
- Assurer un état de conformité constant. Il n'y a pas de solution de sécurité miracle, et cela vaut également pour les cadres. Ce n'est pas parce que votre organisation est conforme aujourd'hui qu'elle le sera demain.

L'INTÉRÊT DES CADRES DE SÉCURITÉ NATIFS D'APPLE

Vous ne le savez peut-être pas, mais Apple développe un ensemble unique de cadres de sécurité : c'est la Sécurité de la plateforme Apple. Ces cadres prennent en charge chaque système d'exploitation et s'articulent à d'autres cadres axés sur la confidentialité pour protéger toute la gamme de produits Apple.

Ils couvrent aussi bien le matériel que le logiciel, mais aussi la sécurité physique et la façon dont les données sont traitées, manipulées, stockées, transmises et consultées par les utilisateurs sur les appareils Apple. En matière de confidentialité, Apple a développé le cadre Transparence du suivi des applications, qui contrôle la collecte et le partage des données des utilisateurs finaux. Son objectif : limiter ce qui est autorisé et interdire ce qui ne l'est pas, pour préserver la vie privée des utilisateurs.

Avec ces cadres, Apple est à la pointe de la sécurité et de la confidentialité. Le constructeur les intègre à ses OS et les met fréquemment à jour pour rester en phase avec l'évolution des menaces, dans le souci constant de protéger la sécurité des informations et la confidentialité des utilisateurs.

OÙ INTERVIENT JAMF ?

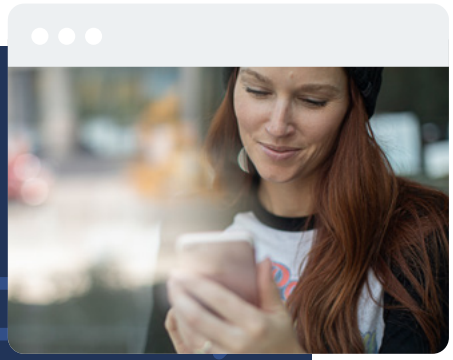
Vous connaissez l'engagement d'Apple en matière de sécurité et de confidentialité. Mais saviez-vous à quel point les solutions Jamf soutiennent vos équipes informatiques et de sécurité ?

Eh bien, c'est le cas. Jamf fournit des solutions qui permettent aux organisations de réussir avec Apple et s'appuie pour cela sur une longue expérience. Que ce soit au travail, à l'école ou dans les loisirs, Jamf complète les cadres natifs développés par Apple. Nos solutions apportent de la visibilité sur ces cadres et répondent aux questions que les professionnels de la sécurité devraient se poser sur leurs appareils Apple :

- Comment sont-ils configurés ?
- Quand sont-ils utilisés ?
- Pourquoi a-t-on accédé à cette ressource ?
- Qui y accède ?
- Les appareils sont-ils utilisés de façon sûre ?
- Comment peut-on les sécuriser davantage ?
- Comment mesurer la conformité ?
- Que faut-il pour assurer la conformité ?

Mais ce n'est pas tout.

JAMF VOUS AIDE À METTRE LA THÉORIE EN PRATIQUE



Les cadres ne suffisent pas à renforcer la sécurité. Des données télémétriques riches peuvent offrir un aperçu de la santé des terminaux et de leur conformité. Mais pour atténuer les risques, ces données doivent être exploitables.

Si notre solution MDM phare, Jamf Pro, est la référence en matière de gestion des appareils Apple, ce n'est pas juste parce que nous l'affirmons : dans le monde entier et dans tous les secteurs, des millions d'appareils gérés le confirment. Jamf aide les organisations de toutes tailles à rapprocher leur évaluation des risques du cadre de leur choix pour déterminer les besoins de sécurité des données et de conformité, puis à intégrer ces informations dans Jamf Pro. Elles peuvent alors gérer les configurations des appareils, minimiser la surface d'attaque grâce au durcissement des appareils et déployer des politiques de mise en conformité active.

Grâce à des workflows automatisés pilotés par Jamf Protect, la meilleure solution de sécurité des terminaux dédiée à Apple, les équipes informatiques et de sécurité comblent rapidement les lacunes.

Les outils Jamf de sécurité des terminaux prennent en charge les critères CIS. Autrement, que votre organisation découvre le monde de la sécurité et de la conformité ou qu'elle soit composée de professionnels chevronnés, Jamf vous aide à sécuriser votre infrastructure rapidement, dès le départ. Vous voulez aller encore plus loin pour renforcer votre conformité et votre sécurité ? Dans ce cas, vous pouvez travailler avec des cadres supplémentaires, comme MITRE ATT&CK, ou répondre à des exigences de conformité plus complexes – NIST et mSCP, par exemple.

Quand les appareils Apple sont équipés des solutions Jamf, les équipes informatiques et de sécurité peuvent se consacrer à des initiatives stratégiques et offrir une assistance de premier ordre. Elles ont les moyens de suivre, comprendre et prendre en charge les besoins de sécurité de l'entreprise au fil de son évolution, avec un maximum d'efficacité.

Découvrez-le par vous-même en faisant un essai gratuit ou en contactant votre revendeur préféré.

Lancez-vous !