jamf

Gestion de crise

Combler les lacunes de sécurité avec la réponse aux incidents et la reprise après sinistre

« La réponse aux incidents de sécurité informatique est devenue une composante essentielle des programmes informatiques. Parce qu'une réponse efficace aux incidents est une tâche complexe, la mise en place des capacités de réponse nécessite une planification soigneuse et d'importantes ressources. »

Cet extrait d'un document du National Institute of Standards and Technology (NIST) souligne l'importance de s'armer d'un plan solide pour faire face aux incidents de sécurité. Une réponse rapide et ciblée permet de contrôler les risques en limitant l'exposition. La phase de correction, déterminée par les outils disponibles, varie considérablement selon l'environnement.

Les angles morts sont inévitables.

Dans cet article, nous abordons plusieurs aspects clés :

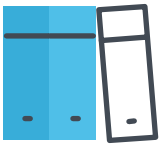
- Les cinq étapes de la réponse aux incidents – préparation, détection, rapports, réponse et correction – et ce qu'elles nous apprennent sur l'élaboration de stratégies de sécurité plus robustes pour faire face aux menaces
- Comment développer des playbooks efficaces et robustes pour gérer la prise en charge de menaces variées
- Pourquoi il faut impérativement comprendre la valeur des actifs et évaluer la potentialité des menaces pour assurer une réponse et une reprise efficaces
- Pourquoi une approche intégrée de la gestion et de la sécurité, reposant sur une solution spécialement conçue à cet effet, est le meilleur moyen de sécuriser votre flotte Apple

I. Préparation

Créez un environnement propice à la réussite.

Le dicton de Benjamin Franklin, « Une once de prévention vaut une livre de guérison », est tout aussi valable aujourd'hui qu'à l'époque où il a été prononcé. Et c'est particulièrement le cas dans l'informatique, et plus précisément, dans le domaine de la protection contre les menaces et les attaques de cybersécurité.

Les organisations ont besoin de règles, de personnel et d'outils appropriés pour limiter les incidents et remettre rapidement en état les appareils touchés. C'est comme cela qu'elles réduiront le risque qu'une menace compromette des services critiques ou la continuité de leurs activités.



Inventaire

Comment peut-on protéger ce dont tout le monde ignore l'existence ? La protection des actifs commence par un inventaire à jour. Cette bonne pratique permet aux organisations de savoir en permanence :

- Quels équipements, périphériques et ressources elles possèdent
- Comment ils sont configurés
- Où ils se situent
- À qui ils sont affectés
- Qui possède quelles autorisations d'accès

Les réponses à ces questions fournissent aux organisations des informations essentielles qui ont directement trait à la sécurité des appareils et des ressources professionnelles.

Un inventaire précis des équipements et de leurs usages donne aux organisations une image précise de leur parc. Il faut y inclure tous les services fournis par les appareils, en identifiant, par exemple, les serveurs publics de contenu web, les appareils mobiles de télésanté qui contiennent des dossiers médicaux ou les données privées de patients, etc.

Évaluation des risques

Après l'inventaire, la phase suivante consiste à évaluer les facteurs de risque, en déterminant :

- Les menaces auxquelles les appareils sont susceptibles d'être exposés
- La probabilité que la menace soit exploitée
- Les retombées potentielles
- Leur impact sur le plan de continuité des activités de l'organisation

L'évaluation des facteurs de risque est une tâche complexe qui exige une grande quantité d'informations pour décrire avec précision les appareils et les ressources de l'organisation. Pour réaliser une évaluation correcte, il faut détenir une connaissance approfondie des aspects techniques, sécuritaires, financiers, administratifs et juridiques de l'infrastructure. L'évaluation des risques ne se fait pas de manière isolée ; elle implique de nombreux acteurs qui vont soupeser de nombreux aspects avant de prendre une décision finale.

Prenons l'exemple d'un serveur web. Les serveurs web sont accessibles au public et sont plus vulnérables que les appareils protégés par des pare-feux. Si un serveur web se connecte à une base de données contenant des informations sur les utilisateurs, il devient une passerelle vers des données personnelles identifiables ou confidentielles, ce qui fait augmenter son risque.

Normes et règlements

L'évaluation des actifs de l'organisation et l'élaboration du plan de réponse aux incidents sont deux aspects distincts, mais interconnectés.

En cas d'incident de sécurité informatique, les équipes de réponse aux incidents de sécurité informatique (CSIRT) doivent pouvoir compter sur un playbook bien défini pour agir rapidement, quelle que soit la taille de l'équipe ou les partenariats externes. Ce plan clair et concis vise à :

1. Aligner les ressources de l'organisation sur les lois ou réglementations du secteur en établissant des bases de conformité.

2. Traiter efficacement les menaces détectées avant qu'elles ne s'aggravent, en décrivant le moyen le plus rapide de revenir à un statut conforme.

Les règles peuvent varier d'un secteur à l'autre, mais les critères du NIST offrent une base robuste pour élaborer les règles organisationnelles de réponse aux incidents. Ils aident notamment à définir une déclaration d'engagement, l'objectif de la règle et son champ d'application, les définitions, la structure organisationnelle, l'évaluation des risques, les mesures de performance et les procédures de rapports.

Processus de réponse aux incidents

Certains aspects régissent la prise en charge des incidents, d'autres concernent le plan d'intervention, qui détaille les acteurs et les étapes impliqués dans la résolution.

N'oubliez pas que chacun a un rôle à jouer, en intervenant directement ou en prenant des décisions à plus haut niveau. C'est fondamentalement un travail d'équipe. Le plan lui-même sert de feuille de route. Il décrit une approche ciblée et coordonnée pour répondre aux incidents en fonction des besoins de l'organisation, et en s'appuyant sur ses capacités et ses partenariats pour une efficacité maximale.

Comme les règles, le plan variera en fonction de la mission, de la taille, de la structure et des fonctions de l'organisation.

Mais l'élaboration d'un plan réussi passe nécessairement par les points suivants :

- Déclaration de mission
- Stratégies et/ou objectifs
- Approche organisationnelle
- Processus de communication approuvés
- Indicateurs d'efficacité
- Processus d'optimisation des capacités
- Intégration aux processus de l'organisation

Considérations administratives

Sur la base des recueillies jusqu'ici, l'organisation doit avoir une équipe en place ou, a minima, une idée précise des personnes concernées et de leur rôle dans le modèle de réponse aux incidents. Par exemple, les membres des services informatique et de sécurité de l'information formeront une équipe d'intervention idéale en raison de leur connaissance approfondie de l'infrastructure. Mais il faudra également des personnes ayant une expérience de la gestion de projet pour accélérer le processus de correction en organisant et en planifiant efficacement les ressources. Différentes approches sont possibles : les grandes organisations disposent généralement d'équipes internes dédiées à la gestion des problèmes de sécurité. Pour les plus petites, en revanche, il peut être intéressant de collaborer avec des fournisseurs externes pour pouvoir miser sur leur expertise en cas de besoin.

Mais ce type de partenariat ne se limite pas aux petites organisations ; des équipes étoffées et spécialisées collaborent souvent avec des fournisseurs, les forces de l'ordre et des entités telles que l'United States Computer Emergency Readiness Team (US-CERT) aux États-Unis, afin de coordonner les activités de réponse aux incidents. Les partenariats avec les fournisseurs peuvent être avantageux, et les organisations ont tout intérêt à connaître l'agence gouvernementale qui supervise la réponse aux incidents dans leur pays ou leur région pour bénéficier d'un soutien supplémentaire. C'est d'autant plus crucial dans les organisations qui manquent d'expertise spécifique ou qui sont touchées par des incidents graves ou des attaques à grande échelle. Des partenariats avec les FAI peuvent, par exemple, atténuer des menaces telles que les attaques DDoS.

Pour former des équipes d'intervention en phase avec les besoins de l'organisation, il faut répondre à plusieurs questions clés :

- L'équipe fonctionnera-t-elle mieux si elle est centralisée ou distribuée sur plusieurs sites ?
- Qui assurera la coordination entre les équipes internes et externes, y compris avec des entités comme l'US-CERT ?
- Quel est l'impact des réglementations sectorielles sur les types d'assistance à la réponse dont l'organisation peut bénéficier et sur ses possibilités de partenariat ?
- Le personnel interne est-il suffisant pour assurer une gestion rapide des incidents, ou faut-il recourir à une externalisation partielle, voire complète ?
- Quels sont les impératifs de disponibilité de l'équipe d'assistance ? Parle-t-on de rotations d'astreinte 24 heures sur 24, d'assistance à temps plein ou à temps partiel ?
- Quel est le budget nécessaire pour financer l'équipe, couvrir les salaires, les congés payés, les lacunes de compétences et la formation continue ?
- Dans les organisations de plus petite taille, quelles sont les options pour protéger les actifs lorsqu'il n'est pas possible de mettre en place une équipe dédiée, et quelle planification faut-il prévoir pour apporter une réponse rapide en cas de besoin ?

Ces informations sont essentielles pour prendre des décisions concernant les dispositifs de sécurité et les services à acquérir pour bénéficier d'une protection totale. Les solutions n'offrent pas toutes les mêmes fonctionnalités : dans ces conditions, pourquoi une solution générique serait-elle adaptée à des problématiques technologiques aussi dynamiques ? **Bien souvent – et c'est notamment le cas des produits Apple, les solutions génériques ne sont pas optimales. En effet, elles n'offrent pas la couverture et la visibilité complètes fournies par les produits conçus à cet effet tels que Jamf Protect, notre solution de sécurité des terminaux Apple.**

II : Détection et signalement

Identifier les menaces

Cette citation fait référence à la **loi de l'instrument**, un biais cognitif qui découle de la confiance excessive inspirée par un outil familier, et peut conduire à une vision partielle de la situation. Lorsqu'elle est considérée uniquement sous l'angle de la sécurité de l'information, la posture de sécurité des appareils de votre organisation est en partie obstruée, ce qui peut devenir dangereux si des informations essentielles sur la santé de vos appareils vous échappent. En dissimulant certaines menaces ou vulnérabilités, ce manque d'informations sur la santé des appareils peut avoir de graves répercussions sur la posture de sécurité de l'organisation.

> « Si vous n'avez qu'un marteau, tout ressemble à un clou. »
>
> **– Benjamin Franklin**

La visibilité est essentielle pour apporter des réponses adaptées. Des outils adéquats, combinés à des données à jour, peuvent faire toute la différence dans deux phases clés de la résolution des problèmes :

1. Avant le déclenchement de l'alerte

2. Pendant la phase de correction proprement dite

Alertes et notifications

Pour recevoir une alerte, il faut qu'elle se déclenche. Idéalement, les outils de l'organisation doivent pouvoir générer des alertes en surveillant activement les terminaux par le biais de diverses méthodes, sans se contenter de rechercher les signatures de logiciels malveillants connus. Un processus robuste utilisant l'heuristique ou l'analytique peut détecter les logiciels malveillants potentiels et d'autres menaces, comme des actions à risque ou un comportement inhabituel chez un employé.

L'analyse comportementale est utile pour alerter les équipes des menaces liées à des logiciels malveillants inconnus pour lesquelles il n'existe pas encore de définition. Ce système permet à l'équipe informatique de hiérarchiser les indicateurs dès qu'une anomalie est détectée. Au cours de leur enquête, les membres de l'équipe doivent confirmer ces détections pour distinguer les faux positifs des vraies alertes. Confirmer les faux positifs permet d'économiser le temps et les ressources de l'organisation. Quant aux vrais positifs, ils déclencheront la mobilisation des ressources nécessaires pour contenir la menace avant qu'elle ne fasse davantage de dommages ou n'entraîne une violation de données.

Envoi des données de journalisation au SIEM

Les fichiers journaux ne servent pas seulement à localiser ou dépanner les applications : ils fournissent de précieuses informations sur les processus du système et des logiciels. Il peut sembler contre-productif de se plonger dans un océan de journaux pendant un incident de cybersécurité. C'est pourquoi il faut impérativement centraliser, organiser et analyser des données de sécurité pour en extraire des renseignements ciblés.

Mais collecter les logs de toute la flotte d'appareils d'une organisation reste une tâche titanesque, surtout lorsque les équipes sont réparties sur différents sites. Il faut parfois des heures – ou une grande équipe – pour trier et analyser manuellement les données des journaux.

C'est là qu'intervient le système de gestion des informations et des événements de sécurité, ou SIEM. Le SIEM joue un rôle crucial dans les processus de sécurité de votre organisation :

- Il identifie les menaces de sécurité actuelles affectant les terminaux.
- Il aide les équipes à trier et prendre rapidement en charge les incidents de sécurité pour accélérer la remédiation
- Il vérifie et garantit la conformité aux normes et aux réglementations.

Le SIEM analyse rapidement les journaux de tous les terminaux pour offrir un aperçu de l'état opérationnel, fonctionnel, technique et sécuritaire des applications et des données d'un terminal. Il répond à des questions telles que :

- Quels correctifs sont installés sur l'appareil ?
- Quelles opérations ont été réalisées par le système ?
- À quel moment des processus ont-ils été exécutés ?
- Depuis quel endroit l'appareil a-t-il communiqué ?
- Pourquoi l'appareil, l'application ou le thread s'est-il comporté d'une certaine manière ?
- Qui a accompli telle tâche ou réalisé telle opération ?
- Comment cette vulnérabilité a-t-elle été exploitée ?

III. Tri et analyse

Analyser les menaces

Avant d'agir sur chaque menace identifiée, il est important d'évaluer la possibilité de faux positifs ou de problèmes mal diagnostiqués.

Le tri et l'analyse ont plusieurs objectifs :

- Enquêter sur le problème détecté ou signalé
- Hiérarchiser les événements de sécurité en fonction de leur gravité
- Affecter les ressources nécessaires à l'analyse des données
- Déterminer la validité d'une menace ou d'une attaque

Rationaliser l'analyse grâce au SIEM

Votre SIEM collecte les données des journaux afin que vos équipes informatiques et de sécurité puissent les analyser avant de prendre des mesures précises pour atténuer les menaces et corriger les problèmes. Tout cela en dépensant le minimum de ressources. Vous pouvez même **étendre les fonctionnalités du SIEM** en l'intégrant aux solutions MDM et de sécurité des terminaux pour **visualiser les données de sécurité stratégiques** et déclencher des workflows de correction automatisés dès l'identification des menaces pour accélérer encore la réponse aux incidents et l'élimination des menaces.

Prévention des menaces connues

La réponse aux incidents intervient une fois la menace identifiée, mais la prévention joue un rôle plus important encore. Un plan complet de réponse aux incidents intègre des outils et des fonctionnalités visant à prévenir les problèmes de cybersécurité sous plusieurs angles. Une stratégie de défense en profondeur, conçue pour intercepter les menaces en multipliant les couches de défense, repose nécessairement sur une combinaison d'approches.

L'analyse représente une couche clé de la défense. Elle s'appuie généralement sur le **cadre MITRE ATT&CK,** un référentiel de tactiques et de techniques adverses. Cette base de connaissances mondiale favorise la collaboration entre les organisations, les développeurs, les professionnels de la sécurité de l'information et la communauté de la sécurité. Elle les aide à améliorer les pratiques de cybersécurité, à minimiser les risques et à optimiser la défense contre les menaces.

Quand cette fonctionnalité est intégrée à votre solution de sécurité des terminaux, les appareils qui accèdent aux ressources de l'organisation contre les risques des menaces connues et leurs vecteurs d'attaque. MITRE ATT&CK **associe chaque menace à une analyse dans votre solution de sécurité des terminaux**, qui peut ainsi bloquer ou mettre en quarantaine les menaces rencontrées pendant la surveillance active.

Ces analyses couvrent les systèmes d'exploitation des ordinateurs de bureau, mais aussi les menaces modernes qui ciblent les appareils mobiles utilisés par les entreprises et les particuliers. Cette approche holistique de la prévention des menaces combine la défense contre les menaces mobiles (MTD) à la sécurité des OS de bureau. Face aux menaces complexes qui exploitent plusieurs techniques pour échapper à la détection, l'analyse collabore avec les solutions de gestion des appareils pour mettre sur pied des workflows automatisés de type SOAR (orchestration, automatisation et réponse de sécurité). Lorsqu'il faut intervenir, les données et les analyses guident l'équipe de réponse aux incidents et suggèrent des mesures adaptées : limitation de la connexion au réseau, confinement de l'infection au terminal affecté et prévention de la propagation des menaces dans le réseau de l'organisation.

Recherche des menaces inconnues

L'intégration du SIEM à la sécurité des terminaux met des capacités d'analyse avancées à la disposition des équipes de sécurité chargées de rechercher les menaces. En combinant la télémétrie riche fournie par les produits de sécurité des terminaux et la puissance d'un SIEM à leur expertise, les chercheurs peuvent explorer les processus système. Les données de télémétrie et les journaux sont centralisés dans une seule interface qui facilite la recherche, l'identification et la prise en charge des menaces inconnues.

Des équipes spécialisées dans la recherche des menaces, comme **Jamf Threat Labs (JTL)**, étudient constamment les menaces émergentes et actualisent les règles de sécurité des terminaux pour les protéger contre les nouvelles formes d'attaque. Mais les organisations n'ont pas toutes une équipe dédiée à la recherche de menaces. Dans ce cas, on recommande vivement de choisir un produit adossé à d'importantes ressources dans ce domaine pour maintenir une sécurité des terminaux optimale face à l'évolution rapide des tactiques adverses.

Les petites organisations ont tout intérêt à se tourner vers des fournisseurs de services pour mettre en place une fonction de recherche des menaces. Une collaboration de ce type permet d'identifier de manière proactive les menaces passées inaperçues ou inconnues, et donc de protéger l'organisation contre les violations de données.

IV. Confinement et neutralisation

Réponse et correction

Le processus de réponse aux incidents englobe la surveillance, la détection, l'investigation et la correction. La correction s'attaque aux problèmes confirmés et emploie différents outils pour rétablir l'état normal des appareils affectés. L'efficacité de la réponse aux incidents et de la correction dépend de facteurs propres à chaque organisation. Facteurs de risque, réglages de sécurité, outils de technologie, partenariats, règles, règlements, plans de sécurité et budget sont autant d'éléments qui influent sur l'approche à adopter.

Les outils de gestion des terminaux doivent offrir une prise en charge robuste des appareils qu'ils doivent gérer. Dans un environnement Apple, un outil incapable de prendre en charge les derniers cadres de sécurité et de gestion des appareils du constructeur Apple peut empêcher l'organisation de réagir rapidement aux menaces. Une prise en charge complète s'aligne sur les règles informatiques et de sécurité de l'organisation. Elle réduit le stress des équipes en cas d'incident ou d'initiative de changement.

Il est essentiel de disposer des bons outils pour éviter les coûts liés aux retards, aux problèmes de signalement ou à un manque d'efficacité dans la correction L'intégration fluide de processus coordonnés et de technologies spécifiques permet de protéger les appareils en arrière-plan et de remédier rapidement aux problèmes. Et c'est précisément ce qui caractérise les solutions Jamf pour l'infrastructure Apple. Ces solutions réunissent sécurité, performances optimales et conformité, adossées à une prise en charge immédiate des fonctionnalités les plus récentes d'Apple.

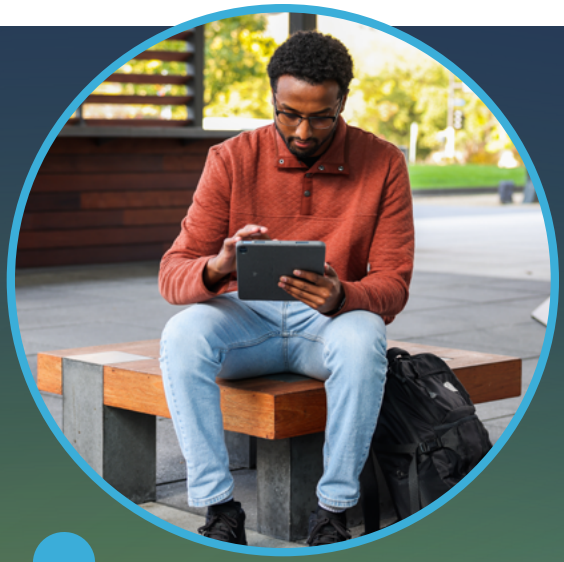
Des workflows avancés pour sécuriser votre environnement et soutenir la réponse aux incidents et la correction.

Approvisionnement des appareils

Le déploiement de nouveaux appareils, comme l'octroi d'accès spécifiques aux appareils personnels des employés, ajoute une couche de risque. Les utilisateurs ont-ils configuré correctement leur appareil personnel ? Comment le service informatique peut-il vérifier que les solutions de sécurité sont activées sur les terminaux ? Que peut-on faire pour limiter l'exposition des appareils compromis ?

La réponse à ces questions : des workflows d'approvisionnement liés à des identifiants de compte, eux-mêmes gérés de manière centralisée au sein d'une **solution de gestion des identités et des accès (IAM)**. Ces workflows doivent couvrir l'ensemble du cycle de vie de l'appareil, dès le déploiement initial. Grâce à l'IAM, les autorisations d'accès sont intrinsèquement liées aux identifiants de l'utilisateur. Cela permet de n'accorder que les autorisations aux ressources nécessaires, avec un accès établi de façon ponctuelle en cas de besoin.

En outre, les workflows de déploiement sans contact fournissent un premier niveau de support pour la réponse aux incidents et la correction. **Ils ne veillent pas seulement à ce que les terminaux soient configurés correctement dès le départ** : en cas d'incident, ils facilitent la mise en place de protections supplémentaires pour atténuer les risques, minimise les attaques et accélérer les processus de rétablissement.



Identité et accessibilité

La gestion des identités et des accès (IAM) ne s'arrête pas aux comptes et aux mots de passe : elle sécurise l'échange de données sensibles. Elle a évolué pour devenir une **solution de sécurité complète reposant sur l'identité**, et protège efficacement l'entreprise contre les menaces d'aujourd'hui grâce à des workflows sophistiqués qui font bien plus que sécuriser les connexions aux ressources et exiger un mot de passe fort.

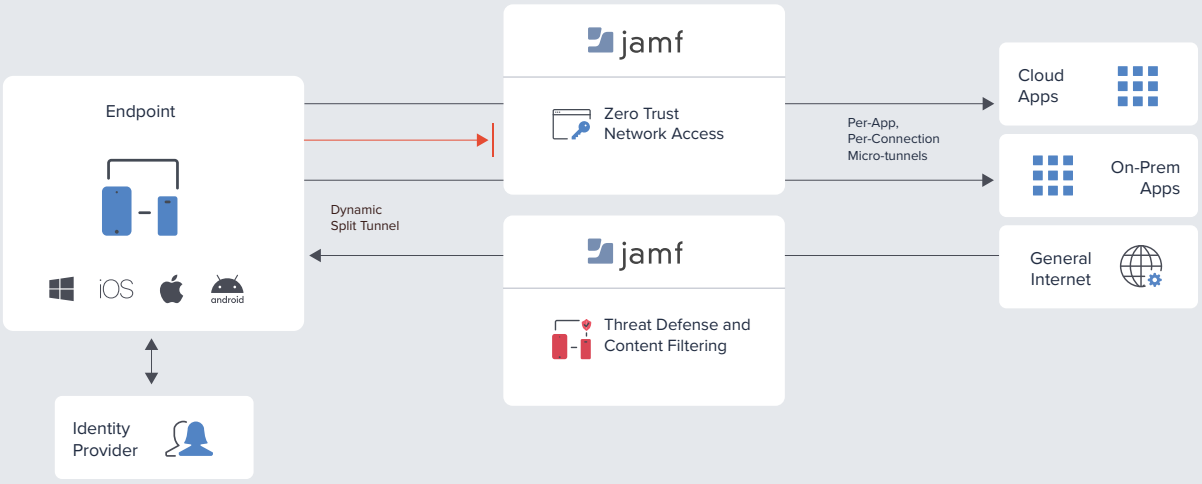
Application des règles

La gestion basée sur des règles est essentielle pour maintenir la posture de sécurité d'un appareil en conformité avec la base de référence. La posture de sécurité est influencée par plusieurs facteurs :

- Mise à jour des applications
- Version de l'OS
- Correctifs de sécurité
- Évolution des besoins de l'organisation
- Comportement de l'utilisateur
- Menaces émergentes

Les règles permettent de maintenir un niveau de sécurité déterminé malgré la nature imprévisible de ces facteurs.

La technologie de l'accès réseau zero-trust (ZTNA) utilise un cadre basé sur des règles. Les appareils et les utilisateurs font l'objet d'une évaluation des risques lorsqu'ils demandent l'accès à une ressource protégée. Dans une approche zero-trust, l'accès est refusé par défaut et doit être accordé sur la base de critères organisationnels. L'accès reste refusé si l'appareil ou l'utilisateur ne répond pas à ces critères.



Des connexions réseau sécurisées

Pour faire face efficacement aux menaces d'aujourd'hui, il faut des technologies modernes. Le VPN, une technologie ancienne qui sécurise les connexions réseau depuis des décennies grâce au chiffrement et à des identifiants utilisateur, ne répond plus aux besoins des environnements actuels et à l'évolution du paysage des menaces. Le VPN n'est pas évolutif. Il n'applique ni le principe de moindre privilège ni de contrôles compensatoires pour les attaques par mouvement latéral. Il n'évalue pas les risques en fonction de l'état des appareils et des utilisateurs, et ne s'intègre pas aux solutions d'identité centralisées.

Le ZTNA, en revanche, sécurise les connectivités réseau comme les solutions VPN traditionnelles, mais sans leurs inconvénients. Les workflows de sécurité du ZTNA s'intègrent aux solutions modernes et sont donc compatibles avec un large éventail d'appareils sur l'ensemble de l'infrastructure. Il élimine les défis administratifs liés à la maintenance de configurations complexes, de même que les coûts liés à la gestion du matériel VPN.

Gestion des appareils

La gestion des appareils mobiles (MDM) n'est plus un luxe lorsqu'il s'agit de gérer les aspects qui ont un impact sur la sécurité. À l'échelle de chaque terminal comme de l'ensemble de votre flotte, elle est indispensable pour protéger la posture de sécurité globale de votre organisation. Son rôle est crucial, car elle constitue une partie intégrante d'une approche holistique de la protection des appareils contre les menaces. Les solutions de sécurité des terminaux sont, elles aussi, étroitement liées à la gestion des appareils. En effet, comment être parfaitement sûr qu'un appareil est sécurisé s'il n'est pas géré ? Et comment gérer correctement un appareil qui n'est pas sécurisé ?

Voici quelques exemples de fonctions de gestion qui renforcent la sécurité de votre environnement tout en facilitant la réponse aux incidents et la correction :

Inventaire

Il est indispensable de tenir à jour l'inventaire des appareils, et ce pour plusieurs raisons : pour suivre de l'état des appareils, identifier les facteurs de risque et garantir que chacun dispose des bons outils de travail, notamment. La gestion d'inventaire ne se contente pas de tracer l'équipement. Elle est essentielle pour maintenir la liaison avec les utilisateurs, leurs appareils et les données de l'organisation et assurer leur contrôle.

Un programme mature de gestion des actifs informatiques (ITAM) fournit des informations précieuses pour le plan de sécurité de votre organisation :

1 Informations essentielles sur les appareils

- Détails du matériel : type d'appareil, modèle et numéro de série
- Informations sur les logiciels : version de l'OS, applications installées avec leur version
- Configurations de sécurité : réglages gérés, profils de durcissement et état du chiffrement
- Informations de gestion : méthode d'inscription, informations de garantie et état de gestion/supervision

2. Fondement de l'évaluation des risques

- Permet de mettre en place des processus d'évaluation et de quantification des risques, afin d'éclairer l'élaboration de stratégies de sécurité globales.

3. Données exploitables

- Convertit les données d'inventaire en informations exploitables qui orientent les étapes à suivre et les tâches informatiques itératives.

4. Soutien des équipes de sécurité

- Fournit aux équipes de sécurité des informations actualisées sur les appareils qui, une fois rapprochées de bases de référence, facilitent le tri des incidents, la réponse et la correction.

Automatisation

Automatiser les processus, ce n'est pas seulement miser sur la technologie pour faciliter le travail de l'administrateur. Bien sûr, cela allège des tâches administratives courantes et répétitives, comme le déploiement d'applications gérées et de profils de configuration, ou encore la gestion des correctifs.

Mais en réalité, le grand avantage de l'automatisation est qu'elle minimise le risque d'erreurs humaines susceptibles de nuire à l'efficacité de votre plan de sécurité.

L'automatisation peut sauver une posture de sécurité :

Scénario idéal	Scénario catastrophe
Les **App Installers** déploient et mettent à jour les applications. Ils veillent à ce que la dernière version soit toujours installée afin de minimiser les vulnérabilités.	Différentes versions des applications sont installées, certaines sont à jour, d'autres non.
Les profils de configuration sont gérés, définis et déployés via votre solution MDM, sans aucune interaction de l'utilisateur.	Les administrateurs comptent sur les utilisateurs finaux pour configurer les appareils.
Un workflow normalisé configure le chiffrement, l'active et conserve une clé de récupération de façon sécurisée.	Le chiffrement des volumes est recommandé pour assurer la sécurité des données.
Les informations de garantie sont consignées dès la date d'achat.	En cas de dommage à un appareil, il faut contacter le service après-vente du fournisseur.
Le déploiement zero-touch fait en sorte que les appareils d'entreprise sont gérés et utilisables dès leur sortie de l'emballage.	C'est aux utilisateurs d'inscrire les appareils d'entreprise dans la solution MDM de l'organisation.
L'organisation peut tracer les appareils perdus, les verrouiller et les effacer à distance à l'aide de commandes MDM pour protéger les données.	En cas de perte ou de vol, les utilisateurs sont tenus de protéger les données contre tout accès non autorisé.
Des workflows basés sur des règles appliquent les mises à jour conformément aux exigences de l'organisation afin de minimiser les risques liés aux vulnérabilités des OS obsolètes.	Les utilisateurs sont tenus de mettre à jour de l'OS de leurs appareils.

Prenons le scénario suivant : l'appareil personnel d'un utilisateur utilise un OS obsolète. L'utilisateur a choisi de repousser la mise à jour parce qu'il utilise quotidiennement une application qui n'est pas encore compatible avec la nouvelle version de l'OS. Malgré ce que cela implique pour la sécurité, il continue d'utiliser son appareil vulnérable pour le travail en plus de son usage personnel.

Comment peut-on atténuer ce risque de façon automatique afin de protéger les données de l'entreprise ?

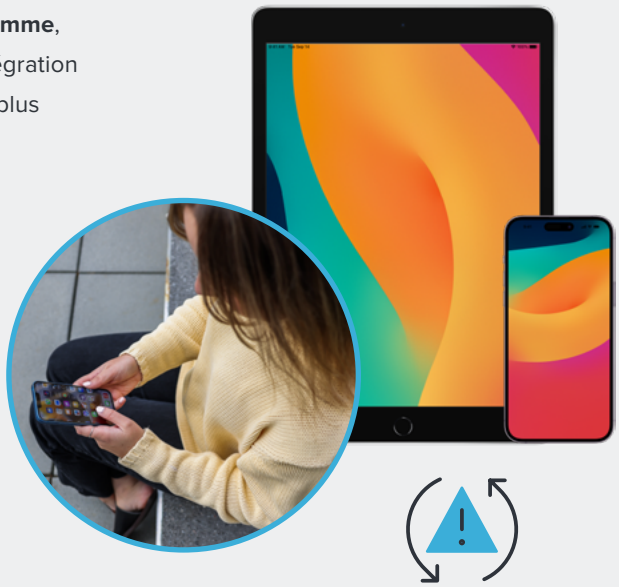
L'intégration de la solution MDM et de la sécurité des terminaux offre de puissantes possibilités aux équipes informatiques et de sécurité, et met à leur disposition des workflows sophistiqués de réponse et de correction.

Le logiciel de sécurité des terminaux compare les données télémétriques des appareils personnels à un ensemble de critères minimum avant d'autoriser l'accès aux ressources de l'entreprise.

Si la demande est refusée pour des raisons de sécurité, les données télémétriques de l'appareil sont transmises en toute sécurité à la solution MDM. Les règles de gestion exigent que l'appareil utilise la version la plus récente de l'OS. Une tâche de correction est donc immédiatement déclenchée pour le mettre à jour.

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.

L'automatisation ne s'arrête pas là. Votre **solution MDM haut de gamme**, déjà enrichie de capacités liées aux identités et aux accès par l'intégration des solutions IAM, peut s'intégrer à d'autres logiciels pour devenir plus puissante encore.



Ne jamais faire confiance, vérifier systématiquement !

Sécurité des terminaux

Dans un scénario idéal, une solution complète de protection des terminaux maintient tous les ordinateurs et appareils mobiles Apple à l'abri des menaces modernes. Mais le monde de l'entreprise ne repose pas entièrement sur le matériel Apple, et être le spécialiste d'Apple ne signifie pas s'y limiter.

La plupart des environnements sont mixtes. La protection des terminaux doit donc s'étendre aux terminaux Windows et Android pour assurer une protection efficace contre les menaces émergentes. Cette approche holistique permet de mettre en œuvre des stratégies de défense en profondeur couvrant un large éventail d'appareils et de systèmes d'exploitation (OS).

Aucun OS n'étant à l'abri des menaces. Il faut donc des solutions de sécurité offrant des workflows à la fois puissants et flexibles pour sécuriser aussi bien les appareils mobiles Apple que les autres. Ces solutions préservent la sécurité des données, la vie privée des utilisateurs et la productivité des utilisateurs finaux.

Les fonctions de sécurité des terminaux, et en particulier la défense contre les menaces mobiles et la gestion des vulnérabilités, se combinent pour gérer et sécuriser les appareils tout au long de leur cycle de vie.

Défense contre les menaces mobiles (MTD)

La sécurité des données est d'autant plus difficile à garantir quand les équipes sont dispersées. Le manque d'intégration entre les outils de gestion et de sécurité vient encore aggraver la situation alors que les tactiques adverses évoluent constamment. Dans ces conditions, les professionnels de la sécurité de l'information ne sont pas en mesure de réagir rapidement et efficacement aux menaces.

Les menaces mobiles représentent une nouvelle frontière pour les incidents de sécurité. On estime le nombre d'utilisateurs de smartphones à 6,7 milliards dans le monde, et le travail se fait de plus en plus sur mobile. On ne sera donc pas surpris que les pirates concentrent leurs attaques sur ces plateformes (prévisions 2023 de Statista). Les appareils mobiles englobent les smartphones, les ordinateurs portables, les tablettes, les dispositifs corporels et même certains appareils IoT, et exploitent donc une grande diversité de systèmes d'exploitation – Apple, Windows, Android et Google Chromebooks en particulier.

Le risque élevé associé aux appareils mobiles souligne l'importance d'une solution de sécurité complète, qui donne la priorité à la protection des ressources professionnelles en alignant les contrôles de sécurité. L'objectif : des appareils mobiles aussi efficacement protégés que le reste du parc de l'entreprise.

Gestion des vulnérabilités

Œuvre du NIST, la base CVE (vulnérabilités et expositions communes) répertorie les vulnérabilités de cybersécurité connues et leur assigne un numéro d'identification, une description et au moins une référence publique. Elle permet d'identifier, de décrire et de référencer les vulnérabilités dans le code informatique.

Mais pour recenser les vulnérabilités présentes dans les OS ou les applications de votre environnement, il faut souvent recourir à des logiciels autonomes. Utilisés par les pentesters, ces logiciels détectent les menaces et les classent en fonction de leur niveau de gravité.

Ce type d'outil mobilise davantage de ressources que l'intégration directe de cette fonctionnalité dans votre solution de sécurité des terminaux. Pour atténuer les risques et maintenir la conformité des appareils avec une efficacité maximale, elle doit faire partie intégrante de vos workflows de prévention des menaces, de réponse aux incidents et de correction.

L'intégration de la gestion des vulnérabilités dans Jamf Protect rend la réponse aux incidents plus performante en donnant aux professionnels de la sécurité les moyens d'atténuer les risques en amont. C'est tout l'inverse d'une approche réactive, qui attendrait qu'une application ou un OS soit compromis pour déclencher une intervention.

Trusted Access

Trois paradigmes de sécurité, **une seule solution holistique.**

Une solution complète, centralisée et dédiée à Apple, qui intègre la gestion des appareils, l'approvisionnement des identités, la connectivité sécurisée et la sécurité des points d'extrémité…

…mais qui soit suffisamment souple pour étendre ses fonctions de sécurité réseau multicouches et fournir à toutes les plateformes prises en charge des workflows de réponse et de correction harmonisés.

Gestion	Identité	Sécurité
• Installer les mises à jour et les correctifs sur les terminaux et les applications • Garantir des performances optimales sans compromettre la **sécurité** ou la **confidentialité** • Automatiser la correction des menaces de sécurité afin de réduire les risques • Maximiser les **couches de protection** et la défense en profondeur	• Maintenir la conformité grâce à des règles **adaptées au contexte** • Approvisionner les identités cloud et centraliser la gestion des mots de passe. • Sécuriser les connexions à distance grâce à la technologie **ZTNA** de nouvelle génération • Mettre en œuvre des workflows **d'authentification multifacteur** (MFA) pour une couche supplémentaire de sécurité d'accès.	• Surveiller les processus système et prévenir les menaces liées aux logiciels malveillants • Analyser fréquemment la santé des terminaux pour corriger tout écart par rapport à la référence • Obtenir de riches données de télémétrie pour éclairer les décisions des équipes informatiques et de sécurité • Le machine learning (ML) avancé et le moteur de renseignement sur les menaces (MI:RIAM) soutiennent la recherche et la prévention des menaces, sur l'appareil et dans le réseau.

Alignement de la conformité

Il est crucial de maintenir la conformité face à des menaces constantes et à l'émergence de nouvelles attaques qui font régulièrement la une des journaux et exercent une pression sur les équipes informatiques. S'ajoutent à cela des mandats réglementaires qui font de la conformité des appareils, des utilisateurs et des données un défi majeur.

Un exemple : les appareils mobiles sous iOS 17, conformes le 24 octobre 2023 à 9 h 59, sont techniquement devenus non conformes une minute plus tard, quand iOS 17.1 a été publié. Ce cas illustre à quel point la conformité est subjective et éphémère.

Il est important de faire la distinction entre conformité et protection de sécurité. La conformité est un état flottant, tandis que la sécurité est la feuille de route qui permet d'y parvenir. L'intersection des exigences de conformité et des contrôles de sécurité forme un cadre qui oriente les pratiques des équipes informatiques et de sécurité.

C'est en combinant des solutions que les professionnels de la sécurité, aidés de workflows de gestion basés sur des règles, pourront garantir la conformité de leur environnement. L'automatisation garantit la remise en conformité des appareils à risque suite au signalement d'une application manquante ou d'une erreur de configuration après une mise à jour d'OS.

V. Activité post-incident

Informer les processus et pratiques de demain

Documentez les résultats
Enregistrez toutes les observations, quelles que soient leur taille et leur importance. La documentation informe tous les acteurs concernés des causes des problèmes et de leur résolution. Elle favorise la collaboration et l'élaboration de meilleures solutions, et sert de base pour optimiser la réponse aux incidents, les workflows de correction et les règles.

Tirez les enseignements
La documentation ne se contente pas de consigner le déroulement des événements, elle fournit de précieuses informations. Une revue attentive des conclusions enrichit le processus de réponse aux incidents et de correction. Elle permet de gagner en efficacité en éliminant les étapes inutiles et en améliorant la valeur globale.

Surveillance continue
Les processus doivent être considérés comme cycliques et non linéaires. Après avoir mis en œuvre un workflow, il faut en présenter les résultats aux acteurs concernés pour qu'ils les examinent. Cette approche itérative, qui englobe l'analyse et la comparaison aux données de référence, permet de s'adapter aux évolutions des technologies et des processus. Elle vise à réduire les risques et à minimiser les impacts en améliorant considérablement l'efficacité.

Formation

L'objectif est de créer des workflows performants et uniformisés pour faire un usage optimal des efforts de sécurité. Il s'agit d'aligner les plans de réponse et de correction sur les missions des équipes informatiques et de sécurité. L'objectif est de répondre aux besoins uniques des organisations et des utilisateurs tout en minimisant les temps d'arrêt.

Résumé

Si vous êtes prêt à créer ou à renforcer votre plan de réponse et de correction, Jamf peut vous aider.

Essayez gratuitement nos solutions pour découvrir leur fonctionnement, ou contactez votre revendeur habituel pour commencer.