jamf



Guide pratique de la télémétrie des terminaux Apple

Tel écran – Tel écrit

La visibilité commence par la télémétrie

Avez-vous déjà pénétré dans une pièce plongée dans l'obscurité totale ? Sans lumière, impossible de distinguer clairement les formes, par exemple où se termine le mur et où commence le bord d'un meuble. La sécurité des terminaux, et par extension la conformité, fonctionnent de la même manière. Sans données de télémétrie, impossible de protéger ce que l'on ne voit pas.

Bien que cela puisse sembler évident, l'incapacité à recueillir des données d'intégrité actuelles sur les parcs Apple gérés représente aujourd'hui l'un des plus grands défis pour les organisations modernes. Certes, le service informatique peut facilement savoir combien d'appareils macOS, iOS et iPadOS sont inscrits, et les équipes de sécurité peuvent générer un rapport détaillant combien d'appareils ont été mis à niveau vers la dernière version majeure de macOS lors d'un projet de migration mené six mois plus tôt.

Mais vos équipes informatiques et de sécurité sont-elles capables de valider l'état de conformité de l'ensemble du parc Mac et mobile à cet instant précis ? **Autrement dit, dans quelle mesure vos équipes ont-elles confiance dans les données qu'elles utilisent pour vérifier :**

- Quels processus sont en cours d'exécution ?
- L'intégrité du système est-elle compromise ?
- Qui a effectué ces modifications ?
- Les terminaux sont-ils conformes ?

Remarquez la distinction subtile, mais importante, entre les termes *identifier* et *vérifier*. Car entre les deux se trouve la différence entre les appareils inscrits : ceux dont les informations, présentes dans votre solution de gestion des appareils mobiles (MDM), ne sont mises à jour qu'au moment des check-ins programmés (identifier). Et les terminaux conformes : une surveillance active recueille et analyse des données de télémétrie détaillées pour offrir, en temps réel, une vision claire de l'état d'intégrité des terminaux (vérifier).

La première approche repose sur le dernier check-in, qui, selon la fréquence et les ressources disponibles, peut être obsolète et exposer les organisations à des risques inconnus. La seconde s'appuie sur des données d'intégrité actuelles pour valider en temps réel la conformité des terminaux, en fournissant aux auditeurs une preuve horodatée de la conformité des appareils.

Pour les organisations de toute taille, la télémétrie est la clé pour combler l'écart entre identifier et vérifier. **Dans ce guide, nous mettons en lumière le rôle essentiel de la télémétrie dans les stratégies modernes de gestion et de sécurité, mais nous abordons également :**

- Ce qu'elle est et ce qu'elle n'est pas
- Son rôle dans la compréhension du parc
- Comment la visibilité :
  - Optimise l'ensemble des opérations informatiques
  - Permet d'atteindre les résultats commerciaux visés
  - Crée de la valeur grâce à un meilleur alignement
  - Renforce la posture de sécurité des organisations

Pour être clair, même si un centre des opérations de sécurité dédié, une équipe spécialisée d'analystes ou une expertise en intelligence des menaces sont un atout, ils ne sont pas indispensables. Il suffit de comprendre ce que la télémétrie apporte, afin que les équipes conçoivent des workflows proactifs fondés sur une prise de décision en temps réel et basée sur les données, plutôt que de s'appuyer sur des processus réactifs reposant sur des informations obsolètes.

Ce qu'est la télémétrie

Si l'on s'intéresse à l'étymologie du mot télémétrie, on découvre qu'il s'agit d'un composé de deux termes issus du grec : tele, qui signifie « au loin », et metron, qui signifie « mesure ». Ce terme désigne, littéralement, une « mesure à distance ».

Dans le contexte de la sécurité des terminaux, la télémétrie désigne le flux de mesures d'intégrité et d'activité qu'un appareil communique à son sujet : ce qui s'est exécuté, ce qui a changé, qui l'a modifié, quand, et à quoi l'appareil s'est connecté.

Pour les terminaux macOS, la télémétrie inclut généralement les éléments suivants :

- **Le suivi des accès** enregistre qui s'est connecté, quand et depuis où, quelles ressources ont été demandées et quelles autorisations ont été accordées ou refusées, par exemple les demandes d'élévation de privilèges.
- **L'exécution des processus** suit le lancement des apps, les tâches en arrière-plan, les processus enfants associés et leurs interactions avec le noyau et l'espace utilisateur.
- **Les événements système** consignent la dérive de configuration, les réussites et échecs des mises à jour, les modifications des fichiers système et les changements d'état matériel ou logiciel.
- **L'activité réseau** capture les détails de connexion, tels que le niveau de chiffrement et le type de réseau, les informations IP, les ports, les protocoles et les apps qui transmettent des données.
- **Les journaux de diagnostic** recueillent les données de fonctionnement et de performance du système, ainsi que les rapports de pannes, les états du code et les vidages mémoire.

Face à la télémétrie, il est courant d'écarter certains éléments isolés en les jugeant négligeables ou faciles à manquer. Pourtant, tout comme une seule pièce de puzzle ne représente pas grand-chose isolément, c'est en assemblant toutes les pièces que l'image complète apparaît. Ensemble, elles offrent aux équipes informatiques et de sécurité une analyse détaillée qui permet de vérifier l'intégrité d'un terminal à un instant donné.

Ce que les équipes font de ces mesures, qu'il s'agisse de recherche des menaces, de gestion des correctifs ou de validation de la conformité, relève d'une étape distincte.

Ce que la télémétrie n'est pas

Comme pour la plupart des contrôles de sécurité dans une stratégie de défense en profondeur, les administrateurs doivent comprendre où se situent les lacunes afin de superposer les défenses et de les combler aussi efficacement que possible. De même, pour l'utiliser efficacement, il est essentiel de connaître aussi bien les limites de la télémétrie que ses avantages.

La télémétrie n'est pas :

- Une surveillance de l'activité personnelle ou des habitudes de navigation d'un utilisateur.
- Un substitut aux outils qui exécutent les tâches de gestion ou les workflows de remédiation de sécurité.
- Une attestation globale de conformité tout au long du cycle de vie d'un terminal.

Les données de télémétrie ne sont que des informations recueillies sur un appareil (ou sur l'ensemble de votre parc d'appareils) et stockées dans des journaux. Sans action supplémentaire, la télémétrie a, en elle-même, peu d'utilité. La télémétrie crée de la valeur lorsque les organisations l'exploitent : d'abord en l'examinant ou en la transmettant à leur solution de gestion des informations et des événements de sécurité (SIEM) à des fins d'analyse, puis en appliquant ce contexte à une prise de décision fondée sur les données pour leurs workflows de gestion, de sécurité et de conformité.

Cette distinction est importante.

Collecter des données de télémétrie sans les appliquer à une solution MDM ou de sécurité des terminaux, c'est comme le bloc d'aluminium unique qu'Apple utilise pour fabriquer chaque MacBook. Seul, ce bloc d'aluminium n'aide en rien les utilisateurs à accomplir leurs tâches professionnelles. Mais en l'intégrant à ses processus de fabrication, Apple parvient à produire un ordinateur portable qui permet aux utilisateurs de remplir leurs responsabilités professionnelles ou de mener à bien leurs projets créatifs.

Dans cette analogie, la télémétrie est la matière première (l'aluminium). Ce n'est qu'en l'exploitant que les organisations peuvent construire leur programme de conformité, en commençant par une visibilité globale et par les tendances qui émergent de la combinaison des différentes données.

Comment fonctionne la télémétrie : de la requête à l'analyse

À présent que nous avons expliqué ce qu'est la télémétrie, changeons légèrement de perspective pour voir comment les données de télémétrie présentes sur les terminaux transforment la prise de décision relative à la posture de sécurité des appareils et de l'organisation.

Mieux comprendre le flux de télémétrie passe par l'examen de ses quatre étapes clé :

1 Collecte

La plateforme macOS génère un flux d'événements au niveau système qui capture, en temps réel, tout ce qui se produit sur un appareil. Ces données d'intégrité sont recueillies au niveau du noyau et à partir des capteurs matériels, en enregistrant les indicateurs de performance surveillés par l'API de sécurité des terminaux d'Apple.

2 Agrégation

Une fois les données brutes collectées, l'étape suivante consiste à analyser ces informations via le système de journalisation unifié (ULS) d'Apple. Au cours de cette phase, les données capturées sont mises en forme pour répondre aux exigences de structure et de stockage propres à chaque appareil.

3 Traitement

Une fois les données consignées, des outils natifs de macOS, comme XProtect et MRT, ainsi que des agents de sécurité tiers, puisent en temps réel dans ce flux de journaux. Ils lisent et analysent ce flux de données, en donnant la priorité aux événements les plus significatifs pour l'étape finale.

4 Rapports

À ce stade, les données de télémétrie détaillées, désormais structurées et traitées, sont transmises via des protocoles standards propriétaires, tels que les serveurs de diagnostic d'Apple pour l'examen des rapports de plantage et des statistiques d'utilisation, ainsi que via des outils d'analyse tiers.

Une fois les données de télémétrie acheminées à travers ce pipeline, les équipes informatiques et de sécurité examinent les journaux des appareils pour évaluer l'intégrité des terminaux et identifier les problèmes potentiels. Étant donné le volume de journaux générés par un seul appareil, multiplié par le nombre d'appareils du parc, il est vivement recommandé aux organisations d'alimenter leur solution SIEM avec ce flux continu de données, où elles sont classées selon les niveaux de gravité ou les besoins de conformité de l'organisation. En somme, plutôt que de trier des milliers d'entrées à la recherche de la fameuse aiguille dans une botte de foin, la technologie se charge du gros du travail en classant les événements les plus importants à examiner en priorité.

Selon la taille et les ressources de votre organisation, c'est à ce stade que des équipes interfonctionnelles s'appuient sur le détail des données de télémétrie pour résoudre les problèmes signalés.

Par exemple, dans les organisations disposant d'équipes informatiques et de sécurité dédiées, celles-ci se regroupent de plus en plus au sein d'un même département, en combinant leurs compétences pour appliquer une règle de conformité aux terminaux auxquels il manque un correctif critique. L'équipe de sécurité confirme qu'il s'agit d'un vrai positif, tandis que l'équipe informatique s'assure que les appareils non conformes sont regroupés en conséquence dans la solution MDM. C'est en travaillant en tandem que ces équipes atteignent le point de bascule : elles s'assurent que la remédiation automatique est effectuée par la solution de sécurité des terminaux, et que la conformité est validée par la collecte de données de télémétrie actualisées.

Précisons que comprendre comment la télémétrie éclaire les équipes ne demande pas de connaître par cœur chaque protocole, type de donnée ou appel d'API impliqué dans ce processus. Il s'agit plutôt de savoir comment les données circulent dans le pipeline et ce qu'elles révèlent aux équipes informatiques et de sécurité sur l'état actuel de leurs appareils, en mettant en évidence la voie la plus conforme à suivre.

La visibilité : le résultat que permet la télémétrie

La télémétrie et la visibilité se distinguent d'une manière essentielle : la télémétrie est l'entrée, la visibilité en est le résultat. Ces deux termes sont souvent utilisés de manière interchangeable en raison de leur similitude, mais il est important de ne pas les confondre, car leurs différences justifient une distinction claire.

Un moyen simple d'en saisir la différence : la cause et l'effet. La télémétrie met en lumière la « cause » d'un problème, comme un appareil mal configuré. La visibilité identifie précisément la nature de cette mauvaise configuration et les appareils concernés : c'est ce qu'on appelle l'« effet ».

Du point de vue opérationnel, la visibilité signifie que les équipes disposent d'une évaluation actuelle et précise de ce qui se passe dans l'ensemble de leur parc. Elle indique également une voie concrète pour atténuer le ou les problèmes détectés. Elle permet de répondre à des questions telles que :

- Le comportement observé est-il conforme à la référence ?
- Quels appareils sont en bon état ?
- Lesquels sont à risque ?
- Existe-t-il une menace active ?

La télémétrie est l'ensemble des données collectées qui rendent la visibilité possible. Elle regroupe les informations recueillies sur l'ensemble des terminaux gérés de votre parc, fournissant en temps réel des détails sur l'état d'intégrité des appareils, notamment :

- Les correctifs système ou de sécurité manquants
- Les apps non autorisées installées
- Les configurations qui se sont écartées de la référence

Si la télémétrie permet la visibilité, elle ne le fait pas automatiquement. Les organisations peuvent surveiller en permanence leurs terminaux et recueillir d'importants volumes de télémétrie, tout en manquant encore de visibilité sur l'état d'intégrité et de conformité de leur parc.

Télémétrie = entrée

Visibilité = résultat



Comment est-il possible de collecter de la télémétrie tout en manquant de visibilité ?

Télémétrie ≠ visibilité.

La première permet et alimente la seconde, mais uniquement lorsque les données sont examinées, replacées dans leur contexte et transformées en décision ou en action. Sans examen des données ni prise de décision, la télémétrie est comme un livre que l'on ne lit jamais – il reste rangé, plein d'un savoir extraordinaire, sans jamais profiter à quiconque.

Plutôt que de considérer la visibilité comme un simple interrupteur marche/arrêt, il est plus juste de la voir comme un spectre continu. À une extrémité, la visibilité existe ; à l'autre, elle est absente. Dans cet esprit, demandez-vous où se situe votre organisation sur cette échelle de visibilité.

Pendant que vous y réfléchissez, examinons l'exemple d'une entreprise placée aux deux extrémités opposées du spectre de visibilité :



Aucune visibilité : une organisation exige que les appareils soient inscrits dans une solution MDM et utilise un intervalle de check-in par défaut de 12 heures pour mettre à jour les informations des appareils ; ce scénario n'offre qu'une vision limitée de l'intégrité des appareils et aucune visibilité en temps réel. En raison du délai entre les check-ins, les données recueillies ont, au mieux, 12 heures de retard. Si un appareil manque un check-in programmé, la collecte ne reprendra qu'à la prochaine fenêtre prévue, rendant ces informations encore plus obsolètes.

Si une solution MDM est capable de beaucoup de choses, elle n'a pas été conçue pour remplacer une solution de sécurité des terminaux. Cela signifie que les indicateurs de risque, comme la présence de logiciels malveillants ou la surveillance de comportements suspects, ne sont pas collectés. De plus, les workflows de confinement ne peuvent pas s'exécuter automatiquement, ce qui affecte la posture de sécurité en raison de ce manque de visibilité.



Visibilité activée : une organisation exige que les appareils soient inscrits dans une solution MDM, utilise un intervalle de check-in par défaut de 12 heures pour mettre à jour les informations des appareils, et intègre une solution de sécurité des terminaux qui les surveille activement. Ensemble, elles offrent une vision complète de l'intégrité des appareils et une visibilité en temps réel. Malgré le délai des check-ins programmés de la solution MDM, la surveillance active signifie que l'agent de sécurité transmet en permanence des données de télémétrie via le pipeline, ce qui garantit une intégrité précise et en temps réel pour chaque appareil du parc.

Grâce à l'intégration d'une solution de sécurité des terminaux à une solution MDM, les comportements, apps et codes à risque sont surveillés en permanence et, une fois détectés, bloqués automatiquement. Des workflows tels que la mise en quarantaine des terminaux compromis et l'atténuation des risques peuvent également être exécutés, tout en fournissant aux équipes des données d'intégrité actuelles pour appliquer la conformité via une gestion basée sur des règles, ou pour la valider auprès des auditeurs à l'aide de preuves horodatées.

En somme, la visibilité est le résultat de l'exploitation de la télémétrie comme un véritable atout de sécurité. Il ne s'agit pas d'augmenter les effectifs ou d'acheter davantage d'outils, mais plutôt de transformer en informations exploitables la télémétrie que vos appareils macOS, iOS/iPadOS génèrent déjà. Ces informations servent alors de socle à des décisions et actions évolutives, fondées sur la certitude de connaître l'état d'intégrité réel de votre parc en pleine croissance – et non ce qu'il pourrait être, ou ce qu'il était un jour ou deux plus tôt, lors de la dernière vérification.

La détection, l'investigation et la réponse sont portées par la visibilité.

La valeur de la visibilité ne se limite pas aux informations qu'elle apporte aux équipes techniques sur la conformité et son impact sur la posture de sécurité. Sa valeur s'étend aussi aux opérations informatiques et de sécurité du quotidien, à savoir :



Détection

Le service informatique utilise des références pour définir des procédures de fonctionnement normales et des niveaux de performance, fondés sur les bonnes pratiques et adaptés à l'organisation. La télémétrie, et par extension la visibilité, donnent aux équipes une vision de l'intégrité des appareils, par exemple pour savoir si les configurations correspondent aux références établies ou s'en sont écartées. La visibilité met également en évidence les comportements anormaux, y compris tout ce qui s'écarte de la référence. C'est particulièrement utile à mesure que les parcs grandissent, car cela permet de détecter les anomalies plus tôt. Autrement dit, la visibilité en temps réel détecte de manière proactive des problèmes qui, sans cela, resteraient latents et passeraient inaperçus jusqu'à devenir un incident.



Investigation

C'est sans doute là que la visibilité joue son rôle le plus déterminant. Dès qu'une anomalie est détectée, les équipes de sécurité passent en mode investigation pour valider le problème, puis répondre à toute une série de questions, telles que :

- Que s'est-il passé ?
- Quand cela s'est-il produit ?
- Pourquoi cela s'est-il produit ?
- Quelle est l'ampleur de l'impact ?

Pour le dire sans détour, sans télémétrie, les réponses à ces questions critiques – et à d'autres – ne reposeraient que sur des suppositions, des conjectures et les dires des utilisateurs concernés. Cela ne veut pas dire que ces témoignages sont erronés, mais seulement qu'ils imposent aux équipes techniques une charge plus lourde pour les corroborer. La télémétrie, elle, constitue une preuve – une démonstration claire de ce qui s'est produit tout au long de la chronologie des événements.



Réponse

La meilleure formule pour décrire l'influence de la visibilité sur cette étape est : « *quand la compréhension devient action* ». Après détection du problème et examen des preuves, la télémétrie guide les équipes de sécurité à travers un workflow de réponse aux incidents reproductible, maximisant la remédiation et limitant l'exposition :

- Isoler les terminaux compromis pour contenir l'impact.
- Prioriser les menaces selon leur niveau de gravité et de criticité.
- Atténuer le ou les risques pour éradiquer les menaces persistantes.
- Remédier aux terminaux en rétablissant leurs performances de référence.

> > >

En réponse : sans et avec visibilité

Plus tôt dans cet e-book, nous avons mis en évidence le contraste entre une organisation avec de la visibilité et une organisation en l'absence de visibilité. La différence clé résidant dans le fait d'exploiter activement les données de télémétrie collectées dans le premier cas, contre le fait de les recueillir sans les utiliser (ou de s'appuyer sur des données obsolètes) dans le second. Si ce type d'exemple apparaît clairement tout au long de ce guide, il n'est jamais aussi manifeste que lorsque les équipes techniques travaillent sous pression pendant une réponse à incident.

Les points suivants illustrent le contraste frappant entre deux équipes (A et B) chargées de répondre au même incident : une application vulnérable et non autorisée, installée sur un appareil fourni par l'entreprise, entraîne une attaque par rançongiciel.



Équipe A : sans visibilité

- **Travaille avec des informations partielles :** peut voir les apps installées, mais ne peut pas vérifier leur niveau de vulnérabilité.
- **Réagit à l'apparition des symptômes :** les performances de l'appareil ralentissent d'abord, puis les données deviennent inaccessibles.
- **Sources de données non vérifiables :** les informations proviennent du point de vue de l'utilisateur concerné et ne peuvent pas être attestées.
- **La résolution demande un travail supplémentaire :** en l'absence d'indicateurs corroborants, davantage d'étapes de dépannage sont nécessaires pour remédier à la cause profonde.
- **Ne s'adapte pas à la croissance du parc :** à mesure que les parcs d'appareils grandissent, la charge de travail augmente de façon exponentielle, tout comme les facteurs de risque et les fenêtres d'exposition.



Équipe B : avec visibilité

- **Des données complètes comblent les lacunes :** elle observe le même incident de l'intérieur, avec la cause, la séquence et l'effet clairement exposés.
- **De la détection à la résolution :** elle remédie à l'incident avec une compréhension complète de la chronologie – sans recourir à des suppositions.
- **Des données actuelles, précises et validées :** les informations attestent de l'état d'intégrité des terminaux, aussi bien pour les équipes que pour les auditeurs.
- **Examine les données en contexte :** les informations recueillies comprennent des indicateurs collectés au niveau du noyau et des capteurs, dressant un tableau complet.
- **Faire croître le parc, pas la charge de travail :** pensés pour l'évolutivité, les processus et les workflows s'adaptent sans alourdir la charge administrative.

Travailler plus intelligemment – pas plus dur

La télémétrie est un moteur de l'automatisation.

En intégrant la gestion des appareils mobiles, la sécurité des terminaux et la gestion des identités et des accès, les workflows pilotés par la télémétrie peuvent enrichir les stratégies de gestion des appareils et de sécurité de façons inédites, en s'appuyant sur la technologie pour effectuer le gros du travail dans de nombreux scénarios. Les administrateurs peuvent ainsi consacrer leurs compétences à offrir de meilleures expériences et à mieux aligner les opérations sur les objectifs commerciaux.

Prenons l'exemple d'une automatisation basée sur des règles, où la sécurité des terminaux signale une app vulnérable et déclenche la remédiation via votre solution MDM. Ce workflow simple préserve la posture de sécurité et atténue le risque sans perturber l'utilisateur, sans impliquer l'assistance informatique et sans devenir un incident.

Les organisations modernes ont pu constater à quel point les technologies d'IA/ML peuvent démultiplier les capacités d'équipes de toutes tailles. Les processus pilotés par l'IA peuvent traquer des menaces sophistiquées sur l'ensemble d'un parc à une vitesse impressionnante. Elle corrèle les données de télémétrie recueillies sur les terminaux, les analyse et les recoupe en temps réel avec de multiples bases de données d'intelligence des menaces, ouvertes et propriétaires, afin de détecter les menaces inconnues et d'en alerter les équipes. Et grâce à des options d'automatisation évolutives, il est tout aussi simple d'intégrer à votre workflow un contrôle humain pour les incidents qui le nécessitent que des workflows basés sur des règles qui traitent seuls les problèmes moins graves.

En personnalisant les solutions selon les besoins propres à votre organisation, les incidents sont résolus plus rapidement et avec de meilleures informations, ce qui réduit les risques et les efforts manuels tout en optimisant l'efficacité opérationnelle et l'efficacité des résultats.



La télémétrie en contexte : conformité, opérations et valeur organisationnelle

Au-delà des avantages en matière de chasse aux menaces et de réponse aux incidents évoqués précédemment, deux autres domaines méritent une attention égale dans la façon dont les organisations envisagent la télémétrie.

Conformité

Des secteurs comme la santé, la finance et l'éducation font l'objet d'un contrôle réglementaire toujours plus strict à l'échelle mondiale. Les réglementations nationales et régionales exigent des organisations qu'elles démontrent que leurs données restent sécurisées et que les appareils qui y accèdent demeurent configurés conformément aux exigences de conformité.

Un point mérite d'être répété : toute affirmation de conformité doit être vérifiée. La position par défaut de la plupart des auditeurs repose sur ce principe : si vous ne pouvez pas prouver qu'un appareil était conforme, alors il ne l'était pas. Aussi simple que cela.

La télémétrie est l'ingrédient clé qui permet cette validation. Comme mentionné précédemment, la télémétrie n'est, en elle-même, rien de plus qu'un ensemble de données. Sans examen, mise en contexte, décisions ou actions, elle ne permet pas la visibilité. De même, sans contrôles de sécurité et règles adéquats déjà en place, la télémétrie ne garantit pas la conformité.

Une fois le contexte appliqué et les contrôles en place, la télémétrie devient le moteur qui permet de prouver (ou d'infirmer) leur bon fonctionnement au moment de l'évaluation. En dehors des audits formels, les données probantes (la télémétrie) jouent aussi un rôle dans d'autres enjeux de conformité : les opérations, que nous aborderons dans la section suivante, et l'assurance cybersécurité. Dans ce cas précis, les assureurs demandent souvent aux organisations de prouver leurs pratiques de sécurité avant le début ou le renouvellement de la couverture, ou lors du dépôt d'une réclamation.

Opérations

Ces mêmes données de télémétrie profitent également aux opérations informatiques, comme l'ont montré plus haut les exemples de détection, d'investigation et de réponse. Cela aide les équipes informatiques et de sécurité à mener à bien les tâches liées à leur rôle, mais donne aussi aux leaders du service informatique et aux dirigeants une vision en temps réel de l'intégrité et de la conformité de l'organisation, sans nécessiter de processus distinct, de tâches supplémentaires ou de rapports individualisés.

La télémétrie est multidimensionnelle : en fondant les rapports sur une télémétrie en temps réel, elle remplit un double rôle. Elle est utile au quotidien pour les équipes techniques, tout en soutenant les cas d'usage métier grâce à une documentation crédible et étayée par des preuves sur les statuts de conformité et les évaluations de risques, alimentant ainsi les discussions sur la croissance future et fondant la prise de décision sur des données précises et actuelles.

En résumé : la valeur fondamentale de la télémétrie ne varie pas selon la taille de l'équipe ou la structure de l'organisation. La télémétrie remplit la même fonction, qu'elle soit examinée par un seul responsable informatique ou par toute une équipe d'analystes de sécurité. Elle mérite une place plus large au sein de l'organisation. Plutôt qu'un outil « réservé aux équipes de sécurité », la télémétrie sert des objectifs différents selon qui en a besoin.

Évaluer votre posture de télémétrie et de visibilité

Comprendre la télémétrie et la visibilité sur le plan conceptuel est utile. Savoir comment elles aident les organisations à évaluer leur situation l'est encore plus. Une auto-évaluation de votre propre niveau de télémétrie et de visibilité constitue un excellent point de départ pour les organisations, sans nécessiter l'achat de nouveaux outils, de formation spécialisée ni de modification de la configuration de votre pile technologique existante.

Commencez par répondre aux questions suivantes :

1. Votre organisation conserve-t-elle les données de journalisation des terminaux sur l'appareil, ou les transmet-elle à un emplacement central (solution SIEM) pour analyse ?
2. Votre équipe pourrait-elle déterminer avec certitude la posture de sécurité actuelle de n'importe quel appareil de votre parc ?
3. Est-elle capable de reconstituer la chronologie d'un incident à partir de preuves, ou doit-elle se fier uniquement au récit de l'utilisateur concerné ?
4. Votre organisation peut-elle produire une vérification de conformité horodatée pour un audit, si cela lui était demandé aujourd'hui ?
5. Lorsque des violations de conformité sont détectées, sont-elles corrigées automatiquement ou nécessitent-elles un suivi manuel ?

Les réponses à ces questions révèlent beaucoup de choses sur la posture de sécurité de votre organisation, et plus précisément sur **la capacité de votre équipe à atténuer les risques de façon proactive plutôt que d'y réagir** à un incident déjà survenu. Voici quelques lacunes courantes à surveiller :

- Une télémétrie riche, stockée sur les terminaux ou partagée avec votre pile technologique existante, peut introduire des lacunes de visibilité que les équipes risquent de manquer.
- Transmettre certains événements (Windows) tout en cloisonnant les autres (Apple) dans des environnements multiplateformes expose toujours l'organisation à des risques.
- Collecter de la télémétrie n'est qu'une partie de la solution : elle doit être examinée régulièrement et suivie d'actions pour révéler toute sa valeur.

À l'inverse, les piles de sécurité matures partagent généralement les caractéristiques suivantes :

- La télémétrie circule en continu et fait partie intégrante des workflows, plutôt que d'être examinée seulement quand quelqu'un s'en souvient.
- Les données collectées sont analysées au regard de multiples sources, corrélées et hiérarchisées selon leur gravité. Le tri manuel risque de faire passer à côté de détails critiques.
- Les équipes qui réussissent leurs programmes de conformité ne sont pas nécessairement les plus grandes ni celles qui disposent des budgets les plus importants. Ce sont celles qui exploitent la télémétrie générée avant de prendre une décision ou d'agir.
- Construire la visibilité à partir de vos données existantes est presque toujours plus rapide que de la construire à partir de nouveaux outils non intégrés.

Conclusion

Cela mérite d'être répété : sans examen, la télémétrie n'est que des données rassemblées dans un fichier.

Ce flux constant de faits horodatés sur l'activité d'un appareil, son état de configuration ou son niveau de vulnérabilité ne devient utile que lorsque les organisations exploitent ces informations pour agir avant qu'un problème mineur ne se transforme silencieusement en une coûteuse violation de conformité.

La capacité des données de télémétrie brutes à permettre une prise de décision fondée sur les données, menant à une action rapide basée sur l'état d'intégrité en temps réel – voilà ce qu'est la visibilité. La précision et l'actualité des données ajoutent un niveau de confiance qui les accompagne tout au long de leur parcours : du pipeline jusqu'aux décideurs qui les reçoivent.

L'écart entre géré et sécurisé peut être comblé. Cela ne nécessite pas toujours de nouveaux achats, une expertise poussée au sein des équipes, ou des changements majeurs dans votre pile technologique existante. Les appareils de votre parc sont conçus pour consigner leur activité, et ils vous disent déjà tout ce qui se passe.

La vraie question est de savoir si votre organisation est prête à écouter, et à agir en fonction de ce qu'elle entend.



Vous voulez voir tout cela en action ?

Découvrez Jamf dès aujourd'hui