jamf

Évaluer les besoins de sécurité dans l'enseignement supérieur

Une démarche essentielle pour votre posture de sécurité globale

Résumé

Pour bien évaluer les besoins de sécurité de l'enseignement supérieur, il faut faire preuve de nuance et prendre en compte de nombreux aspects simultanément. **Certains sont théoriques, d'autres pratiques.** Malgré cette dualité, il s'agit toujours d'exploiter les données télémétriques obtenues lors de l'évaluation des risques et de la surveillance, d'abord pour acquérir une visibilité sur les vulnérabilités, puis pour les atténuer avant qu'elles ne conduisent à un incident de sécurité.

Loin d'être autonomie, cette pratique doit être informée par une compréhension de l'impact que les menaces identifiées exercent sur votre conformité aux régulations et normes de sécurité en vigueur. Elle englobe, entre autres, la sécurité des données, la protection des dossiers des employés et des étudiants et le respect de la vie privée des utilisateurs. Tous ces éléments, lorsqu'ils sont combinés, orientent l'acquisition d'outils de sécurité et aident les organisations à atteindre (et préserver) leurs objectifs de conformité.

Dans ce document technique, nous abordons :

- Les types de risques qui affectent le secteur de l'éducation
- Comment les données télémétriques collectées apportent une visibilité sur l'état des appareils et la posture de sécurité globale
- Pourquoi l'évaluation des risques doit être une démarche récurrente et itérative, intégrée à la gestion de la pile de sécurité
- Comment ces données vous aident à déterminer les besoins de sécurité de votre organisation et à vous protéger contre les risques d'aujourd'hui et de demain
- Pourquoi l'intégration des données de risque aux solutions de sécurité des terminaux permet de maintenir une posture de sécurité forte tout en respectant les objectifs de conformité de l'établissement

Tout établissement d'enseignement doit connaître à tout moment sa posture de sécurité. Demandez à n'importe quel administrateur **comment il veille à la réussite des personnes dont il a la charge**, et il vous répondra certainement qu'il faut comprendre leurs besoins spécifiques, ceux de l'institution, et le juste équilibre entre les deux.

C'est la même chose pour votre programme de cybersécurité. Votre programme de sécurité repose sur la collecte d'informations utiles sur la santé des appareils et sur leur utilisation judicieuse. **Plus précisément, l'analyse de données télémétriques riches permet de prendre des décisions éclairées pour minimiser les risques tout en optimisant l'expérience utilisateur pour toutes les personnes concernées.** C'est particulièrement vrai dans l'enseignement supérieur, qui a gardé ses portes ouvertes malgré les crises sanitaires mondiales, les ralentissements économiques ou l'évolution des préférences des étudiants en matière d'apprentissage à distance.

La capacité d'adaptation a toujours été la clé du succès des établissements d'enseignement supérieur. C'est la même chose dans le domaine de la cybersécurité : il faut à la fois évaluer son infrastructure puis procéder aux ajustements nécessaires pour maintenir une posture de sécurité saine et robuste. *En d'autres termes, il faut avoir les moyens d'évaluer les besoins de sécurité* ***tout en*** *s'adaptant de manière dynamique pour répondre aux problèmes qui se manifestent.*

Comme l'apprentissage, la cybersécurité est un processus continu et évolutif.

Les administrateurs ne doivent pas seulement se tourner vers l'extérieur pour évaluer les besoins de leurs parties prenantes : ils doivent aussi rechercher en interne ce qui est nécessaire au maintien de processus informatiques et de sécurité capables de protéger les étudiants, les enseignants, le personnel, les données sensibles et les terminaux, dans l'ensemble de l'infrastructure. Cette réflexion fait partie intégrante de l'évaluation des risques, et les enseignements qu'on peut en tirer couvrent un large spectre : les appareils, les outils logiciels et l'infrastructure qui traite des données sensibles, bien sûr, mais aussi les processus et les règles qui les régissent et veillent à leur conformité. Tous ces aspects composent la posture de sécurité d'une institution.

L’évaluation des risques n’est pas un processus isolé.

Armées de ces informations, les équipes informatiques et de sécurité ont toutes les cartes en main pour évaluer les risques et les responsabilités propres à leur stratégie de cybersécurité actuelle. En vous situant sur votre parcours de conformité, cet instantané répond à la question **« Où en sommes-nous actuellement ? »**. Et en rapprochant les données d’évaluation des risques aux normes de sécurité de l’industrie, on répond à la question ***« Où devons-nous/souhaitons-nous aller ? »***. La distance qui sépare les deux points indique les étapes à suivre pour corriger le cap.

Il faut ensuite introduire les changements nécessaires pour :

- Normaliser les pratiques de gestion
- Corriger les vulnérabilités
- Atténuer les menaces
- Réduire les risques
- Garantir la mise en conformité

L’évaluation des risques n’est pas un processus isolé. Les bonnes pratiques recommandent de la renouveler à intervalle régulier. La technologie évolue constamment, et tout état est nécessairement transitoire. Il en va de même pour la sécurité : de nouveaux bogues réapparaissent sans cesse et créent des vulnérabilités qui affaiblissent la posture de sécurité et élargissent la surface d’attaque. Les appareils, les utilisateurs et les données sont exposés à des risques de compromission.

Et nous n’avons pas encore abordé un sujet concret d’inquiétude, qui est que les acteurs malveillants ciblent activement les réseaux des établissements d’enseignement. C’est d’ailleurs ce que souligne le Rapport 2023 de Verizon sur les enquêtes sur les violations de données, qui révèle que l’éducation fait une fois de plus partie de la **liste des cinq secteurs les plus ciblés à l’échelle mondiale**.

En d'autres termes, les administrateurs informatiques des établissements d'enseignement ne doivent pas attendre que des pirates sondent et testent les défenses de leur réseau pour y déceler des faiblesses. Au contraire, ils doivent procéder régulièrement à des évaluations des risques de cybersécurité.

Les données évaluées ne doivent pas seulement servir à décrire l'état actuel de la sécurité de toutes les ressources : elles doivent aussi informer, de manière itérative, le plan global de cybersécurité et les stratégies de défense en profondeur qui s'attachent à :

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

Les administrateurs informatiques des établissements d'enseignement ne doivent pas attendre que des pirates sondent et testent les défenses de leur réseau pour y déceler des faiblesses. Au contraire, ils doivent procéder régulièrement à des évaluations des risques de cybersécurité.

Évaluation des risques

Nous avons compris l'importance de l'évaluation des risques, mais en quoi consiste-t-elle exactement ? *Quels actifs sont réellement en danger ?*

Les détails varieront d'une école à l'autre, mais il s'agit typiquement de comprendre :

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

Voyons à quelles questions une évaluation des risques doit répondre.

> « L'apprentissage n'est pas le fruit du hasard. Il doit être recherché avec ardeur et poursuivi avec assiduité. »
>
> **– Abigail Adams**

Où se situent les vulnérabilités de mon site ?

Un pirate peut utiliser de nombreux points d'entrée pour infiltrer votre système. Pensez au matériel, aux logiciels et aux interfaces, mais aussi au manque de personnel et aux interactions des fournisseurs – ou de tout autre acteur – avec votre infrastructure de réseau. Les vulnérabilités peuvent également se trouver dans les processus et les règles de sécurité de votre établissement.

Pour bien comprendre votre infrastructure, vous devez inventorier et classer tous ces composants. **Vous avez besoin de savoir :**

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

Quelles sont les menaces ?

L'évaluation des risques implique également de connaître les menaces existantes et l'impact qu'elles peuvent avoir sur vos appareils. Vos équipes informatiques et de sécurité pourront alors identifier les points les plus vulnérables, la probabilité d'une cyberattaque et ses conséquences potentielles sur votre établissement.

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

Si vous connaissez les vecteurs de menaces les plus courants, vous pourrez traiter en priorité les parties de votre infrastructure qui ont le plus besoin d'être défendues. Les menaces prennent de nombreuses formes. Selon le Rapport 2023 de Verizon sur les enquêtes sur les violations de données, les attaquants s'infiltrent dans les organisations **en volant des identifiants, en recourant au phishing et en exploitant des vulnérabilités.** En général, les violations de données proviennent de sources totalement externes **(72 %), mais une part non négligeable (jusqu'à 40 %) vise des identifiants compromis.** Pour se défendre contre ces menaces, il faut procéder à une analyse approfondie des configurations et des règles en vigueur. Nous y reviendrons plus tard.

72 %
des violations de données proviennent de sources externes

40 %
des violations de données ciblent des identifiants compromis

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

Comprendre la probabilité d'une menace permet d'établir des priorités dans votre stratégie de défense. Mais vous devez également évaluer l'impact d'une menace sur la mission de votre institution. Cet impact peut être financier : le coût moyen d'une violation de données dans une infrastructure critique (et le secteur de l'éducation en est une) s'élevait à **5,04 millions de dollars** en 2023, selon le rapport Coût d'une violation de données d'IBM. **Ce montant est supérieur de 1,26 million de dollars au coût moyen des autres secteurs, qui est de 3,78 millions de dollars**, soit une différence de 28,6 %. Pensez également au temps perdu, car il faut en moyenne 277 jours pour identifier et contenir une violation.

5,04 M USD
Le coût moyen d'une violation de données concernant une infrastructure critique

L'impact peut aussi prendre la forme d'une dégradation de vos relations avec vos parties prenantes. Votre réputation est en jeu, et les infractions aux réglementations telles que le Règlement général sur la protection des données (RGPD) vous exposent à de lourdes amendes. Celles-ci vont de 2 % des recettes annuelles mondiales (avec un plancher de 10 millions d'euros) pour les infractions les moins graves, à 4 % des recettes (avec un plancher de 20 millions d'euros) pour les violations de grande ampleur. Et nous ne parlons pas ici des amendes supplémentaires que peuvent imposer les différentes administrations si votre établissement n'est pas en conformité avec d'autres normes nationales, fédérales ou régionales.

Quelle est l'étape suivante ?

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

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

Il est maintenant temps de mettre en œuvre les enseignements tirés de votre évaluation des risques.

Dans les prochaines sections, nous verrons dans le détail comment évaluer la télémétrie de votre réseau et de vos appareils, ainsi que les directives à suivre pour élaborer et revoir vos règles de sécurité.

Visibilité et suivi

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

Peut-on dire que les équipes informatiques et de sécurité ont terminé leur travail et qu'elles peuvent prendre des vacances bien méritées ? ***Pas tout à fait.***

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

Les données télémétriques enregistrées par la surveillance active de l'état des appareils contiennent une mine d'informations essentielles pour préserver la posture de sécurité des appareils et de l'infrastructure.

En matière de conformité (à laquelle nous reviendrons plus tard), les données de télémétrie jouent un rôle décisif. Non seulement elles confirment que les terminaux sont configurés conformément aux exigences réglementaires, mais aussi elles apportent aussi la preuve qu'un terminal était effectivement conforme à un moment donné. Cette preuve de la conformité est indispensable pour une certification réglementaire telle que PCI-DSS, qui autorise les écoles à accepter et traiter des paiements par carte en toute sécurité.

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

> « Les analphabètes du XXIe siècle ne seront pas ceux qui ne savent ni lire ni écrire, mais ceux qui ne savent pas apprendre, désapprendre et réapprendre. »
>
> **– Alvin Toffler**

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

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

1. **Passive :** les données de santé sont collectées lentement, généralement sur une période définie pour minimiser l'impact sur l'utilisateur final ou les performances de l'appareil surveillé. Parce que la capture des données est intermittente, la collecte de la télémétrie peut être lente et retarder la création d'un profil de référence complet. En outre, tout retard peut avoir une incidence directe sur l'exactitude ou l'actualité des données, en particulier si des jours ou des mois s'écoulent entre les captures.

2. **Active :** les données de santé sont régulièrement communiquées par les terminaux. Cette fois, les terminaux sont sondés à intervalle régulier et les informations sont transmises à un référentiel centralisé, souvent en temps réel.

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

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

Si les deux types de surveillance ont leurs avantages et leurs inconvénients, le paysage moderne des menaces est trop vaste et changeant pour se passer d'une surveillance active. C'est le seul moyen efficace de recueillir les données les plus récentes sur l'état des appareils et de les utiliser pour combler les lacunes de votre plan de sécurité. Un axiome extrait d'un article de SecurityWeek résume précisément l'importance stratégique de ce processus : « vous ne pouvez pas protéger ce que vous ne voyez pas ».

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

Mises à jour des OS :

Identifiez la version du système d'exploitation (OS) pour savoir si les appareils possèdent les protections les plus récentes contre les menaces connues afin de minimiser les vulnérabilités, et s'ils prennent en charge les fonctionnalités les plus récentes.

Correctifs des applications :

Tout comme l'OS, les applications doivent recevoir des correctifs, qui garantissent la protection des données qu'elles traitent, rectifient des bugs et atténuent des vulnérabilités.

Paramètres de configuration :

Le renforcement des appareils est essentiel à la posture de sécurité. L'objectif n'est pas seulement de les configurer pour une sécurité maximale : cela permet également de minimiser le risque de mauvaise configuration, responsable de 21 % des failles de données causées par des erreurs (Rapport 2023 sur les enquêtes sur les violations de données, Verizon).

Activité du réseau :

Avec quel contenu web les appareils communiquent-ils ? Les connexions non fiables sont-elles sécurisées ? Sur quels ports voit-on des données circuler ? Les réponses à ces questions et à d'autres, essentielles, concernant l'utilisation du réseau, permettent de déterminer la posture de sécurité de vos appareils.

Analyse comportementale :

Les utilisateurs, qu'ils soient étudiants, enseignants ou chercheurs, sont généralement considérés – à raison – comme le maillon faible de la chaîne de sécurité. Ce sont en effet les disparités dans leur connaissance du sujet qui expliquent le succès des attaques d'ingénierie sociale. Avec une meilleure visibilité sur le comportement des utilisateurs, les administrateurs ont une idée plus précise de la manière dont ils peuvent introduire des risques introduits – et ainsi s'en protéger.

Processus système :

Les administrateurs ont besoin de savoir quelles applications s'exécutent sur les appareils qu'ils supervisent. Non seulement cela les informe de la conformité au profil de référence, mais ils sont avertis en cas d'utilisation d'outils non validés (Shadow IT) ou interdits, susceptibles de dégrader la sécurité, de faciliter les fuites de données ou de mettre à mal la confidentialité des utilisateurs.

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

Code malveillant :

Le code malveillant peut se manifester sous différentes formes. Un cheval de Troie déguisé en application légitime, la visite involontaire d'un site web compromis, une menace fonctionnant silencieusement en arrière-plan… Toutes ces nuisances peuvent compromettre la conformité d'un appareil, en particulier dans le contexte de la multiplication des attaques visant désormais les mobiles autant que les ordinateurs classiques.

Audit d'authentification :

Les protocoles d'authentification et la gestion des mots de passe protègent les appareils et les données sensibles qu'ils contiennent. Mais aussi robuste et complexe soit-il, un verrou ou un mot de passe complexe ne vous dit pas si les utilisateurs partagent leurs identifiants ou si leurs comptes ont été compromis. Et l'enjeu est d'autant plus grand dans les environnements d'apprentissage à distance, où enseignants et étudiants utilisent aussi bien des appareils institutionnels que personnels au quotidien. La gestion basée sur des règles renforce la sécurité des terminaux distants et protège les ressources sensibles, quel que soit le type d'appareil ou son OS.

Enregistrement des erreurs :

Les appareils enregistrent tout. Plus le parc à surveiller est vaste, plus il est difficile pour les équipes informatiques et de sécurité de traiter chaque problème signalé. Ce qui arrange bien les pirates. Mais ce n'est pas une fatalité : avec une bonne gestion et l'appui d'une solution de gestion des informations et des événements de sécurité (SIEM) pour trier et interpréter ce grand flux de télémétrie, les administrateurs peuvent trier, classer et hiérarchiser efficacement les problèmes en fonction de leur degré de gravité.

Conformité aux audits :

La visibilité de la santé des terminaux concerne autant sur ce qu'on connaît que ce que l'on ignore. C'est particulièrement crucial dans les secteurs réglementés comme l'éducation. Un campus doit impérativement pouvoir se situer sur son parcours de conformité et savoir comment résoudre ses lacunes. Surtout, il doit pouvoir apporter la preuve que les problèmes ont été corrigés pour respecter pleinement la législation et la réglementation de sécurité des données et de protection de la vie privée.

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

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

- Nombre et diversité des appareils à gérer
- Nécessité d'assurer la sécurité d'une flotte composée d'appareils institutionnels et personnels
- Prise en charge des utilisateurs distants et des pratiques hybrides
- Convergence de deux types de menaces ou plus dans le cadre d'attaques complexes sur plusieurs fronts
- Application de réglages de sécurité pour maintenir la conformité des terminaux

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

La technologie ne fait pas de pauses.

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

Après l'évaluation des risques, la surveillance active est la deuxième couche de votre plan de sécurité, et elle aussi permet d'établir les besoins de votre établissement d'enseignement supérieur. La surveillance continue de votre flotte collecte et transmet en temps réel des données télémétriques Ces données sont ensuite analysées et traitées par les solutions de sécurité des terminaux pour déterminer le niveau de sécurité de chaque appareil. Au minimum, les lacunes et les comportements anormaux détectés doivent déclencher des alertes qui avertissent automatiquement les équipes informatiques ou de sécurité. Alors que les processus manuels nécessitent une intervention humaine, l'automatisation détermine et accomplit les étapes suivantes des workflows de réponse aux incidents. C'est notamment le cas de la protection contre les logiciels malveillants connus qui, selon le rapport de Verizon, étaient présents dans 40 % des failles. Ou encore celui de la mise en quarantaine des terminaux infectés par un ransomware (présent dans 30 % des failles).

Des workflows plus sophistiqués encore deviennent possibles en intégrant les solutions de sécurité des terminaux à d'autres outils – gestion des identités, gestion des appareils mobiles – pour décupler les capacités d'automatisation. Nous y reviendrons dans la section suivante.

Conformité

Des citations sur l'éducation, judicieusement placées tout au long de ce document technique, font le lien entre ses analyses et ses thèmes. Ces citations parleront certainement aux professionnels de l'informatique et de la sécurité chargés d'évaluer les risques et les besoins de leur institution en matière de sécurité. L'objectif est de combler les moindres lacunes tout en comprenant que le processus est essentiel en soi. En outre, chaque phase de ce processus est liée à la suivante : les données qu'elle collecte informent directement la suite des événements.

> « Le but de l'éducation est de transformer les miroirs en fenêtres. »
>
> **– Sydney J. Harris**

Pour bien comprendre vos besoins de sécurité, vous ne devez pas seulement savoir quelles vulnérabilités sont présentes à un moment donné : vous devez aussi savoir quoi faire pour les résoudre, et quelles stratégies mettre en œuvre pour garantir la conformité de vos terminaux à vos règles L'objectif : rester en conformité avec les exigences réglementaires en vigueur, mais aussi avec les règles et normes internes. Ce sont en effet les deux piliers de la sécurité et de la protection de la vie privée des utilisateurs. **En résumé, vous allez atténuer les risques en vous appuyant sur un cadre structuré pour préserver la posture de sécurité de vos appareils et de votre organisation.**

> « Si vous pensez que l'éducation coûte cher, essayez d'estimer le coût de l'ignorance. »
>
> **– Howard Gardner**

Les acteurs malveillants comptent sur l'ignorance des bonnes pratiques, qui visent à se prémunir des vulnérabilités et des risques. Et cela concerne toute personne susceptible d'introduire un risque, sciemment ou non. Le risque provient en effet d'une vulnérabilité qui, si elle est exploitée, peut entraîner une violation de données.

Mais au stade de l'évaluation des besoins, il n'est pas aussi utile de s'inquiéter de la multitude d'adversaires potentiels que des réalités immédiates de votre réseau. Il vaut mieux s'intéresser à la diversité des risques eux-mêmes qu'à leur origine. Grâce à ce cadrage, les administrateurs pourront réellement comprendre les menaces et déterminer la meilleure approche pour maintenir la conformité et protéger les appareils, les utilisateurs et les données contre les menaces actuelles et émergentes.

Quelles directives permettent d'identifier et de minimiser les différents types de risques ?

Il est important de faire la distinction entre directives, cadres et références avant de poursuivre. Les **directives** sont proches des bonnes pratiques. Il ne s'agit pas de règles strictes à suivre – plutôt un ensemble de pratiques éprouvées qui aident les organisations à prendre les bonnes décisions pour gérer diverses formes de risque à un niveau général.

Les **cadres**, quant à eux, ont un ADN similaire à celui des bonnes pratiques. Ils visent à synthétiser l'ensemble des informations, pratiques, réglages, contrôles et workflows nécessaires pour atteindre ou dépasser un objectif spécifique, qu'il s'agisse d'une politique interne ou d'une obligation réglementaire.

Les profils de référence ont des points avec les deux précédents types de guide : ils poursuivent également un objectif de conformité, mais leur angle est différent. Si les directives suggèrent des bonnes pratiques et les cadres les organisent de manière structurée dans un objectif de conformité particulier, les références ne sont pas mises en œuvre de la même manière. Elles jouent un rôle de baromètre : les administrateurs les utilisent pour se situer sur leur parcours de conformité ou mesurer leur performance par rapport aux objectifs de l'institution.

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

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

Cadres couramment utilisés dans la planification de la sécurité

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

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

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

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

MITRE ATT&CK :
base de connaissances globale sur les tactiques utilisées par les pirates, reposant sur l'observation de techniques réelles. Ce cadre sert également 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 des terminaux.

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

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

Certification du modèle de maturité de la cybersécurité (CMMC) 2.0 :
basé sur les exigences de sécurité de plusieurs publications spéciales du NIST, ce modèle à plusieurs niveaux propose différentes certifications pour les institutions de l'enseignement supérieur qui travaillent avec le gouvernement pour les aider à remplir les critères cumulatifs de paradigmes robustes de cybersécurité. Ces critères correspondent aux « niveaux CMMC et aux pratiques associées dans tous les domaines ».

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

Projet Conformité de sécurité macOS (mSCP) :
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, comme ceux de la FERPA et de PCI-DSS.

Le rôle des références dans la cybersécurité

Guides de mise en œuvre technique de la sécurité (STIG) de l'Agence des systèmes d'information de la défense (DISA) :

ces normes de configuration sont administrées par le ministère américain de la Défense (DoD) et contiennent des exigences spécifiques pour la sécurisation des systèmes informatiques. Elles couvrent un large éventail de domaines – configurations logiques, protocoles et logiciels – et visent à « améliorer la sécurité des logiciels, du matériel, des architectures physiques et des architectures logiques afin de réduire davantage les vulnérabilités. »

Normes de traitement des informations fédérales (FIPS) 200 :

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

NIST SP 800-39 :

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

Centre pour la sécurité Internet (CIS) :

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

Objectifs de performance de cybersécurité (CPG) de l'Agence pour la cybersécurité et la sécurité des infrastructures (CISA) :

développés en coordination avec la CISA, le NIST et la communauté interagences, les CPG définissent « des objectifs cohérents pour tous les types d'infrastructure critique », comme les établissements d'enseignement. Ils aident des institutions de toutes les tailles à mettre en place des initiatives de cybersécurité, et jouent le rôle de critères pour mesurer et améliorer la maturité en matière de cybersécurité. Le but : arrêter les menaces les plus graves qui pèsent sur l'enseignement supérieur, à commencer par l'intensification des campagnes de ransomware.

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

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

Identifier vos points faibles

Connaître l'état de santé de vos terminaux

Réduire la surface d'attaque à l'aide de configurations durcies

Atteindre vos objectifs de conformité

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

Comme on l'a vu, c'est un processus évolutif, et pas un projet isolé. Plus un chemin qu'une destination, la boucle mentionnée dans le paragraphe précédent ne se referme pas une fois terminée. L'ensemble des phases et des composants – contrôles de sécurité, processus, workflows, exigences, politiques, réglages des appareils, utilisateurs finaux et donnée sensible – s'informent et s'ajustent constamment les uns les autres.

> « Tout apprentissage véritable aboutit au changement. »
>
> **– Leo Buscaglia**

Vous êtes peut-être l'administrateur informatique d'une grande université, chargé de mesurer le niveau de conformité de votre environnement. Ou bien un professionnel de la sécurité dans établissement d'enseignement supérieur plus modeste, désireux d'aligner les règles et contrôles internes, comme une politique d'utilisation acceptable (PUA) sur des stratégies de cybersécurité référence. Dans tous les cas, envisagez chaque élément de base comme les pièces d'un puzzle plus grand.

Ces composants forment les rouages d'une machine qui permet de mieux comprendre vos besoins de sécurité et quelles informations permettront de combler les lacunes.

Vous vous dites peut-être : « Je suis administrateur Mac. Je sais exactement quels risques pèsent sur le réseau du campus, mais je suis submergé de données sur la santé des appareils. Toutes ces directives mettent en évidence le gouffre qui sépare notre ***situation actuelle*** de ***l'objectif de conformité***. Que dois-je faire de tout ça ?

Comment parvenir la situation idéale ? »

C'est là que Jamf intervient

Aider les institutions d'enseignement supérieur à réussir avec Apple. Plus qu'un simple slogan, ces mots résument à eux seuls toute la mission de Jamf. C'est notre cœur de métier, tout simplement. Jamf n'est pas la solution de référence pour la gestion et la sécurité d'Apple simplement parce que nous l'affirmons. Jamf doit sa réputation aux solutions de pointe que nous développons et qui aident d'innombrables clients à gérer et sécuriser des dizaines de millions d'appareils, dans tous les secteurs d'activité et dans le monde entier.

Choisir Jamf, ce n'est pas seulement signer un contrat, c'est nouer une relation. C'est un processus qui commence dès le premier contact avec le service des ventes et se poursuit avec les membres des équipes d'ingénierie et de réussite client. Nous avons un but : vous donner la possibilité d'exploiter tout le potentiel des produits Apple dans votre environnement. Dans les sections ci-dessous, nous allons voir comment Jamf répond aux besoins de votre institution en mettant à sa disposition les outils nécessaires à une gestion complète de votre flotte Apple. Puissantes et flexibles, les solutions Jamf de gestion des appareils, des identités et de la sécurité soutiennent également vos objectifs de conformité.

Éliminez l'incertitude de la validation des terminaux.

Pour comprendre vos besoins de sécurité, vous devez connaître l'état des terminaux utilisés au sein de votre campus comme en dehors. Sans des données télémétriques détaillées pour vérifier l'état de chaque appareil, les administrateurs ne peuvent qu'émettre des suppositions. En cas d'erreur, ces conjectures hasardeuses peuvent avoir des conséquences désastreuses et mettre en péril les ressources de votre réseau.

Pour dire les choses simplement, un administrateur n'a pas seulement **intérêt** à connaître sa posture de sécurité en permanence, c'est un véritable **impératif**. Pour garantir la conformité de l'environnement aux réglementations comme aux politiques de l'établissement, il doit pouvoir vérifier l'état de santé des terminaux à tout moment et fournir sur demande la preuve horodatée que les critères de conformité sont bien remplis.

L'ingénierie sociale est un vecteur d'attaque de choix pour les pirates. Les campagnes d'hameçonnage, une menace bien réelle qui cible l'enseignement supérieur et compromet les identifiants de la victime, sont arrêtées par Jamf Safe Internet qui empêche l'accès aux domaines malveillants. Pour prendre un autre exemple, l'exécution du code d'un ransomware sur un appareil donne aux attaquants la possibilité d'étendre l'attaque à d'autres appareils du réseau. Certes, les ransomwares sur Mac ne sont pas aussi nombreux que sur les autres plateformes. Cela n'empêche pas Jamf Protect d'empêcher l'exécution des logiciels malveillants, surtout quand on sait que les ransomwares figurent toujours dans le top 5 des menaces sur macOS. En effet, les **auteurs de logiciels malveillants maintiennent la pression sur les appareils Apple**, comme on a pu le voir récemment, ne serait-ce qu'en décembre 2023.

Une solution de protection des terminaux pour macOS, telle que Jamf Protect, ajoute un filet de sécurité à votre flotte. Sur les appareils mobiles iOS et iPadOS, Jamf Safe Internet protège les utilisateurs contre les menaces, logiciels malveillants en tête. Pour ce faire, elles recherchent les menaces sur l'appareil et le réseau pour accélérer la réponse aux incidents et déclencher des workflows automatisés d'atténuation et de correction. **Et tout cela sans jamais faire de compromis sur la sécurité, la confidentialité et les performances.**

Étendre les protections à l'ensemble de votre infrastructure

Tout au long de ce guide, nous avons discuté de l'évaluation des besoins de sécurité de l'enseignement supérieur et de son rôle décisif pour votre posture de sécurité globale. Nous allons maintenant voir quelles solutions Jamf permettent de transformer les données de télémétrie statiques en workflows performants pour aider les administrateurs à gérer leurs terminaux et les maintenir en conformité, sur le campus et à distance.

L'histoire ne commence pas au moment où un appareil se connecte pour la première fois aux ressources de l'institution, mais bien avant cela – avant même que l'appareil ne soit déballé. Laissez-nous vous expliquer.

Avec le déploiement zero-touch, **un appareil est prêt à l'emploi dès que l'utilisateur final l'allume** pour la première fois. Pour mettre en place ce processus, il faut bien comprendre les besoins de l'institution et les risques auxquels elle est exposée. Le but étant d'intégrer parfaitement le workflow de déploiement depuis l'achat auprès d'Apple jusqu'à l'inscription automatique et sécurisée dans Jamf.

Pour couvrir aussi bien les appareils institutionnels que personnels, **Jamf Pro** prend en charge plusieurs modèles de propriété, dont le BYOD. Tout cela en préservant la vie privée des utilisateurs. En matière de sécurité, notre solution MDM garantit **la prise en charge le jour même de toutes les nouveautés d'Apple, y compris les améliorations de sécurité et de confidentialité**. L'équipe informatique du campus peut prendre en charge et gérer les fonctionnalités qui aident les utilisateurs à travailler intelligemment sans avoir à faire de compromis entre la sécurité et la qualité de l'expérience.

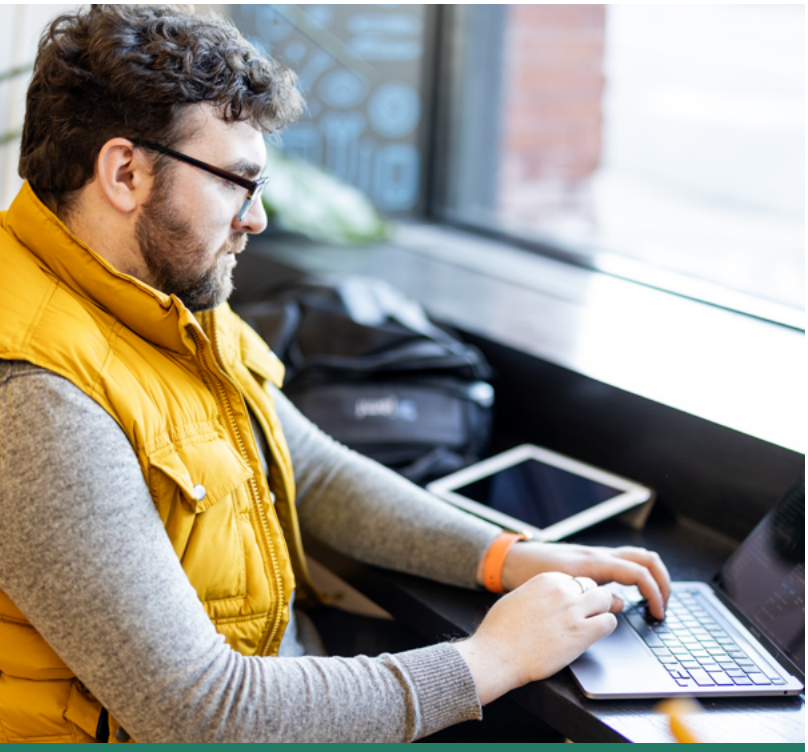
La gestion des correctifs est un élément essentiel de l'équation de la sécurité. Le déploiement des mises à jour des systèmes d'exploitation (OS) et des applications est un enjeu majeur pour la réussite de tout plan de sécurité. En effet, à quoi bon comprendre vos besoins de sécurité si vous ne pouvez pas y répondre ? Une fois de plus, Jamf Pro s'illustre en **simplifiant la gestion du cycle de vie des applications pour les administrateurs Mac** : des commandes de gestion permettent d'appliquer les mises à jour de l'OS à des groupes d'appareils. Vous vous interrogez sur la gestion des applications ? Qu'elles soient distribuées par l'App Store ou des boutiques tierces, le catalogue d'apps de Jamf garantit leur provenance et automatise les mises à jour. Cette fonctionnalité simplifie la gestion des correctifs et laisse aux administrateurs plus de temps pour aider les utilisateurs à tirer le meilleur parti de leur technologie.

La simplification de l'approvisionnement des identités et des accès est l'un des piliers d'une stratégie de sécurité globale de défense en profondeur. Lorsqu'il s'agit de gérer des appareils, l'application des autorisations de sécurité change la donne : elle veille en effet à ce que les utilisateurs de confiance – et eux seulement – puissent accéder aux appareils et aux ressources, partout et à tout moment. C'est particulièrement vrai lorsque l'apprentissage à distance et que les enseignants et les étudiants peuvent être loin les uns des autres et en dehors du campus. Facilitez également la vie des utilisateurs en leur offrant un moyen facile de s'authentifier sur leurs appareils, lorsqu'ils reçoivent l'appareil la première fois (avec le déploiement zero-touch) et au quotidien. Intégrez **Jamf Connect** avec votre fournisseur d'identité (IdP) cloud pour renforcer la sécurité de l'authentification multifacteur (MFA). Vous aurez ainsi l'assurance que les individus sont bien ceux qu'ils prétendent être, en gardant en tête qu'on ne peut se passer **d'une sécurité efficace, adaptative et flexible.**

En matière de sécurité des terminaux, qu'il s'agisse de Mac ou d'appareils mobiles, l'un des vecteurs d'attaque les plus importants est la connexion réseau. Dans notre monde de connectivité permanente, la prévention des menaces sur le réseau représente une protection indispensable. **Jamf Safe Internet** bloque l'accès aux domaines utilisés dans les attaques de phishing de type « zero-day », même si un utilisateur clique sur un lien suspect diffusés sur le web, par e-mail ou par SMS. La protection ne s'arrête pas là : la technologie DNS-over-HTTPS (DoH) arrête les contenus nuisibles sans porter atteinte à la vie privée des utilisateurs.

S'il faut exercer un contrôle plus fin du trafic web, pour bloquer des sites web au contenu dangereux ou illégal, par exemple, le filtrage de contenu intégré permet aux administrateurs de personnaliser le niveau de contrôle d'accès selon les besoins de votre institution. L'intégration de Jamf Safe Internet et de Jamf Protect réunit des capacités informatiques et de sécurité qui ont le double avantage d'être faciles à déployer et de protéger les utilisateurs contre les menaces présentes sur l'appareil et sur le réseau.

Trois éléments de sécurité essentiels, une plateforme fiable



« Dis-moi et j'oublierai, enseigne-moi et je me souviendrai, implique-moi et j'apprendrai. »

– Benjamin Franklin

L'**approche holistique** de Jamf en matière de sécurité couvre chacun des aspects évoqués ici et offre une solution complète qui **répond aux besoins de gestion et de sécurité de l'enseignement supérieur**. Elle s'étend à l'ensemble de votre infrastructure et intègre les solutions de gestion, d'identité et de sécurité.

Elle allie :

- **Visibilité et conformité**
- **Protection des terminaux**
- **Gestion des appareils**

Chacune de ces solutions joue un rôle décisif dans la stratégie de défense en profondeur d'une université. Cette stratégie doit superposer des contrôles d'accès avancés et des configurations sécurisées pour protéger les appareils, les utilisateurs et les données. Elle s'appuie également sur des données de télémétrie pour s'adapter à toute évolution de la posture de sécurité de vos appareils ou de votre institution, avec un triple objectif : maintenir la sécurité, préserver la confidentialité et rester en conformité avec la loi.

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

Lancez-vous !

jamf

www.jamf.com/fr

Études de cas

Ne vous contentez pas de nous croire sur parole : lisez les témoignages d'établissements d'enseignement supérieur qui ont choisi les solutions Jamf pour sécuriser leur environnement et atteindre leurs objectifs de conformité en un temps record.

Université de Glasgow
Les appareils Apple protégés par les solutions de sécurité Jamf.

Université de Shenandoah
Une plateforme standardisée pour une meilleure expérience d'apprentissage

Texas A&M
Efficacité et innovation dans l'enseignement supérieur avec les solutions Jamf

Université d'Oxford
Pour un enseignement de pointe

Université du Wisconsin-Eau Claire
Offrir aux étudiants et aux enseignants un environnement universitaire high-tech

Université de Washington
Simplifier la gestion de la technologie et respecter les engagements en faveur de l'éducation

Université d'État de l'Ohio
Adosser l'expérience Mac à un outil de gestion robuste

Université de Maryville
Remettre en question les normes traditionnelles et offrir aux étudiants une expérience pratique qui s'adapte au style d'apprentissage de chacun

Université de Colgate
Intégrer la technologie à la philosophie de l'institution et miser sur une solution unique pour relever de nombreux défis