5 principes de la sécurité moderne

à l'intention des administrateurs de l'enseignement supérieur

jamf

Dans l'enseignement supérieur, la sécurité peut être difficile à gérer efficacement. Bien sûr, les similitudes avec la sécurité d'entreprise sont nombreuses. Mais ce qui complique la tâche dans l'enseignement supérieur, ce sont les stratégies qu'il faut mettre en place pour protéger les étudiants et les enseignants, qui utilisent à la fois les appareils de l'établissement et les leurs, tout en sécurisant les données institutionnelles.

C'est un défi de taille pour l'enseignement supérieur, d'autant plus que les utilisateur, les appareils et les ressources sont de plus en plus dans le viseur. Par exemple, dans son Rapport 2024 sur les enquêtes sur les violations de données, Verizon observe que l'éducation se classe au 6e rang sur 21 en nombre total d'incidents survenus (1 780). Et elle arrive en tête de classement pour le nombre d'incidents ayant conduit à une violation de données, avec 1 537 incidents de ce type.

Les pirates ciblent de plus en plus l'enseignement supérieur. Pour exploiter les vulnérabilités et obtenir un accès non autorisé aux données personnelles, privées et institutionnelles, ils misent principalement sur l'infiltration de systèmes, l'ingénierie sociale et les erreurs de configuration.

Les perspectives (et votre mission)

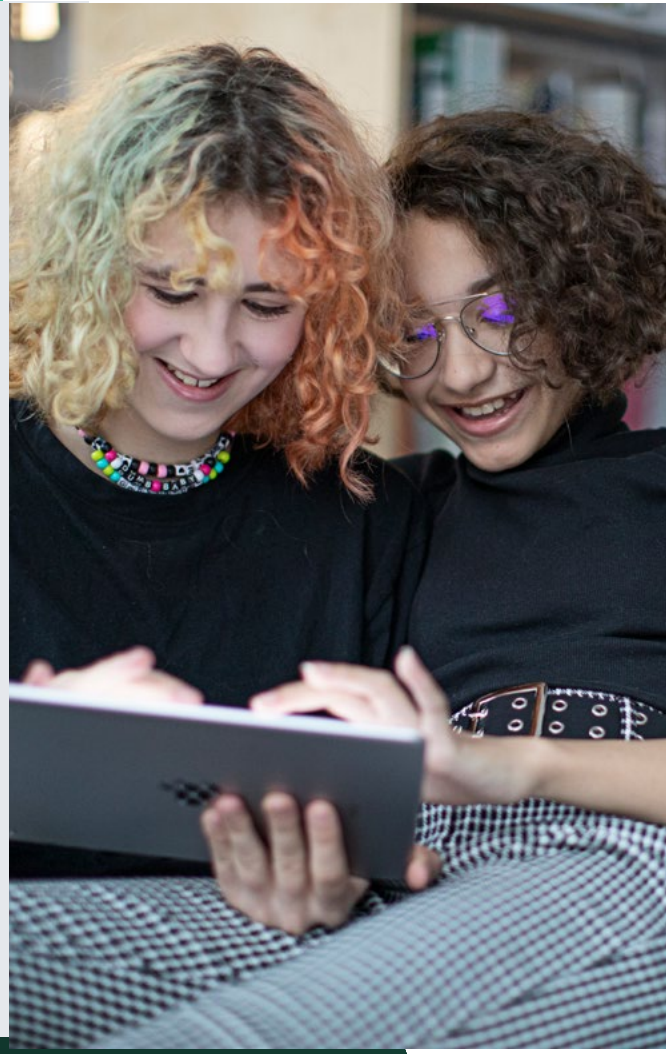
L'enseignement supérieur est confronté à des défis uniques en matière de sécurité et doit respecter de nombreuses exigences réglementaires en matière de collecte, d'utilisation, de partage, de stockage et de destruction des données. Ces défis sont accentués par l'évolution constante du paysage des menaces : les nouvelles techniques sophistiquées sont élaborées pour exploiter les vulnérabilités sont difficiles à neutraliser pour les équipes informatiques et de sécurité.

Mais vous n'êtes pas seul.

Dans cet e-book, nous examinons cinq principes essentiels que les administrateurs peuvent (et doivent) appliquer dès maintenant pour lutter à armes égales et protéger les utilisateurs, les appareils, les données, les réseaux et les infrastructures contre les menaces de sécurité.

Les cinq principes de sécurité abordés dans ce livre :

1. Intégration des solutions
2. Durcissement de la configuration des appareils
3. Sécurisation de tous les terminaux
4. Gestion de la conformité
5. Cycles de vie itératifs



Les conditions du succès de la sécurité

Comme dans tout environnement d'apprentissage, il y a quelques règles à respecter pour réussir. Et dans notre cas, ces « règles » exigent de satisfaire certaines attentes avant de commencer.

En effet, les solutions présentées dans cet e-book ne seront pas pleinement efficaces si les outils et les processus de sécurité de base ne sont pas déjà en place.

Voici ces conditions :

- **Des évaluations des risques** régulières et soigneusement examinées
- **Un logiciel de gestion des appareils mobiles (MDM)** pour gérer et **déployer les appareils Apple**
- **Une solution d'identité basée dans le cloud** et configurée pour approvisionner les comptes et les autorisations
- Des mesures de sécurité de base, à commencer par des pare-feux et **une surveillance active des terminaux**
- Des contrôles administratifs, comme des **règles d'utilisation acceptable** alignées sur les besoins et les exigences de l'institution

1. Intégration des solutions

L'intégration des solutions ouvre la voie au renforcement des protections et à l'élaboration de workflows avancés qui réduisent le délai entre la découverte des problèmes et la mise en œuvre des mesures correctives.

Pourquoi l'intégration est-elle essentielle pour faire face aux menaces modernes ?

En faisant converger les outils de votre pile de sécurité, notamment vos solutions de MDM et de sécurité des terminaux, vous comblez le fossé entre sécurité et gestion. Ces deux outils forment alors une solution unique et puissante qui offre des workflows combinés de protection et d'atténuation.

« Quand elle est partagée, la connaissance a un pouvoir exponentiel. »

– Myra Gray

Les données télémétriques recueillies grâce à la surveillance active permettent aux administrateurs d'identifier en temps réel les vulnérabilités présentes dans les appareils utilisés sur les réseaux de l'établissement. En transmettant ces données en toute sécurité à la solution MDM, il devient possible de mettre en place une gestion basée sur les règles : des workflows de correction sont automatiquement déployés pour **mettre à jour les applications** et corriger les vulnérabilités afin d'empêcher la compromission des appareils personnels et institutionnels.

Quelques avantages clés de l'intégration des solutions de gestion, d'identité et de sécurité :

- Les données de télémétrie sont partagées en toute sécurité et en temps réel, ce qui permet d'agir en fonction des **informations les plus récentes sur la santé des appareils**.
- Correction simple et rapide des menaces et des vulnérabilités, basée sur des règles, sans interaction de l'utilisateur.
- Prévention globale des menaces et **chiffrement de l'accès aux ressources protégées** sur n'importe quelle connexion réseau.
- Maintien de la conformité des appareils, quel que soit le modèle de propriété, grâce à l'alignement des exigences de conformité sur les plans de sécurité.

2. Durcissement de la configuration des appareils

Sécurisez les appareils scolaires et personnels en transmettant des données télémétriques riches à toutes les solutions pour assurer la conformité des terminaux.

Comment sécuriser des appareils s'ils ne sont pas gérés efficacement ? Inversement, peut-on considérer que des appareils sont gérés s'ils ne sont pas également sécurisés ?

La gestion et la sécurité sont indissociables.

Dans le monde de l'enseignement supérieur, le terme « appareil » désigne toute technologie informatique employée par les étudiants, les enseignants et le personnel pour soutenir l'apprentissage, quels que soient :

- Le propriétaire de l'appareil
- Le type d'appareil
- Le système d'exploitation utilisé

Un appareil personnel, s'il est vulnérable, peut tout aussi bien être à l'origine d'une violation des données qu'un appareil appartenant à l'établissement. Il ne s'agit pas d'interdire l'utilisation des appareils personnels car, soyons réalistes, les listes de blocage qui semblent judicieuses en théorie fonctionnent très mal dans la pratique. Pénibles et chronophages, elles souffrent en outre d'un manque d'efficacité, comme l'ont prouvé des décennies de pratiques rigoristes de la gestion informatique. D'ailleurs, **le monde de la sécurité est perclus d'idées reçues** qui n'empêchent pas les utilisateurs de se servir de leurs appareils personnels pour accéder à des ressources protégées. Le risque est donc constant.

En d'autres termes, lesquels des appareils suivants sont les plus faciles à sécuriser : ceux que vous pouvez voir ou ceux que vous ne voyez pas ?

Le deuxième cas ouvre la porte à un cercle vicieux qui contraint les personnes impliquées à poursuivre dans une voie pourtant visiblement néfaste. Le premier, en revanche, vise à parvenir à la sécurité en misant sur la souplesse pour s'adapter.

Dans le cas de la cybersécurité, **les bonnes pratiques de durcissement appliquées à tous les terminaux** ayant accès aux ressources de l'établissement permettent de préserver à la fois la sécurité et la vie privée :

- Les protections, normalisées, s'alignent étroitement sur les besoins, la tolérance au risque et la posture de sécurité globale de l'institution.
- La détection des vulnérabilités et des menaces s'appuie sur des cadres de sécurité qui permettent d'**établir des configurations de référence sécurisées** renforçant la posture de sécurité des appareils.
- La conformité est assurée par des workflows de gestion basés sur des règles qui se déclenchent automatiquement en cas de modification de l'état des appareils en temps réel.
- Les cycles de gestion des correctifs suivent un rythme régulier pour que tous les appareils, quel que soit le modèle de propriété, reçoivent les mises à jour nécessaires.

3. Sécurité des terminaux

Appliquer des protections complètes selon une approche multicouche pour assurer une défense en profondeur contre de nombreux vecteurs de menaces, en recherchant activement les menaces et en déployant des workflows de correction automatisés.

La somme des parties

L'objectif global de ce guide est de protéger les appareils, les utilisateurs et les données contre les menaces modernes en misant sur l'intégration des technologies. Une telle approche transforme des contrôles de sécurité déconnectés en workflows complets, indispensables pour faire face à l'évolution constante des défis dans le secteur de l'éducation.

« Arrêtez d'essayer de conduire en ligne droite quand les virages se profilent. »
– Jay Shetty

C'est indéniable, les outils de sécurité jouent un rôle stratégique dans cet effort. Si les contrôles ponctuels sont limités par leur isolement, l'intégration lève ces obstacles et permet de créer des solutions robustes qui étendent les mesures de protection à l'ensemble de votre infrastructure.

La protection contre les logiciels malveillants est un élément essentiel de la **sécurité des terminaux**. Elle constitue une ligne défense sur les appareils eux-mêmes, mais que faire contre les menaces basées sur le réseau ? C'est là que la gestion des identités et des accès, combinée à la sécurité des terminaux, joue un rôle crucial. Ces mesures arrêtent les attaques au sein du réseau de deux façons : en exigeant que l'utilisateur s'authentifie avant de lui accorder l'accès aux ressources éducatives, puis en chiffrant les connexions pour garantir l'intégrité des données sur n'importe quel réseau. Elles protègent également contre des menaces courantes basées sur le réseau, à commencer par les attaques dites « de l'homme du milieu » (MitM).

Dans la section précédente, nous avons évoqué les avantages de l'intégration de la gestion et de la sécurité. Outre les workflows de correction automatisés, des fonctionnalités supplémentaires permettent aux administrateurs d'enrichir l'expérience des étudiants et des enseignants.

Le machine learning (ML), par exemple, qui est un domaine de l'intelligence artificielle (IA), soutient les activités de recherche des menaces des professionnels de la cybersécurité. Il facilite **l'identification et l'atténuation des menaces sophistiquées** et inconnues, qui se dissimulent sur votre réseau et collectent des données de reconnaissance à votre insu, jusqu'à ce qu'un incident se produise.

Puisqu'on parle d'inconnu, on ne sera pas surpris que le **phishing reste la méthode de choix des pirates** pour atteindre leurs victimes. Ces attaques anonymes permettent de jeter un vaste filet pour faire un maximum de prises en déployant le moins d'efforts possible.

Les filtres de contenu peuvent certes limiter l'accès aux sites web de phishing connus, mais il suffit qu'un utilisateur clique sur un lien malveillant pour ouvrir une brèche. L'intégration étroite des outils de sécurité ajoute des couches de protection aux appareils mobiles. Elle assure la sécurité des utilisateurs même lorsqu'ils cliquent sur des liens malveillants, pour une **prévention** efficace des menaces de phishing « zero-day ». Et parce qu'elle est basée sur le réseau, cette solution couvre indifféremment tous les OS. Autrement dit, tous les appareils sont protégés, qu'ils fonctionnent sous macOS, iOS/iPadOS, Android ou Windows.

4

Gestion de la conformité

Veillez à ce que vos plans de sécurité s'alignent sur les objectifs de conformité et les exigences réglementaires. Harmonisez les initiatives de conformité en mettant en œuvre des normes et des cadres de sécurité dans l'ensemble de votre infrastructure et en appliquant les directives de façon systématique à tout appareil pouvant se connecter aux ressources de l'établissement.

Un manuel pour atteindre la conformité

L'évaluation des risques est généralement la première étape de toute démarche de conformité. Une fois que vous connaissez les enjeux, vous pouvez mettre en œuvre des mesures de protection adaptées.

Toutefois, vous devez avoir à l'esprit une sorte de principe tacite. Il faut comprendre que la mise en conformité et son maintien forment un processus continu. Il faut en effet mettre en œuvre et appliquer des mesures holistiques à tous les appareils communiquant avec les infrastructures de l'établissement. On peut comparer cela au **Pacte d'Ulysse**.

Qu'est-ce qu'un Pacte d'Ulysse et en quoi peut-il soutenir les efforts de conformité de mon université ?

Pour résumer, cela consiste à prendre dans le présent des décisions ou des mesures conçues pour vous empêcher de les modifier à l'avenir. Pour prendre un exemple, nous avons établi que la conformité doit s'appliquer autant aux appareils personnels qu'à ceux qui de l'établissement.

Si l'on applique le principe du Pacte d'Ulysse, exiger l'inscription des deux types d'appareils dans la solution MDM institutionnelle garantit l'application des configurations de référence à tous sans discrimination. La solution MDM fait appliquer les normes de conformité que vous avez établies. Il est possible d'utiliser à la fois deux types de profils : l'inscription des appareils et l'inscription des utilisateurs. Grâce à cela, la gestion sépare les données de l'établissement des données privées sur les appareils personnels, pour **sécuriser le matériel et les données sans porter atteinte à la vie privée de l'utilisateur**.

On trouve un autre exemple de « Pacte d'Ulysse technique » dans la convergence de la gestion des appareils et des normes de cybersécurité au service de la conformité. **Jamf Compliance Editor** (JCE), un outil basé sur le Projet Conformité de sécurité macOS (mSCP), permet de **créer des profils de configuration personnalisés et renforcés sur la base des normes de sécurité établies** par différentes instances :

- Institut national des standards et de la technologie (NIST)
- Agence des systèmes d'information de la défense (DISA)
- Centre pour la sécurité Internet (CIS)
- Certification du modèle de maturité de la cybersécurité (CMMC)
- Comité d'instruction des systèmes de sécurité nationale (CNSSI)

Une fois personnalisé en fonction de vos besoins de conformité, JCE s'interface nativement avec votre instance de Jamf Pro et importe les configurations. Les administrateurs peuvent ensuite les déployer sur les appareils gérés et configurer les réglages de sécurité qui répondent le mieux aux obligations de conformité de l'institution.

Enfin, l'application des règles par la solution MDM fait respecter les normes de conformité en corrigeant les appareils qui présentent un défaut involontaire de configuration ou qu'un événement de sécurité a intentionnellement rendus non conformes.

5 Cycles de vie

Créez une boucle de rétroaction pour informer les phases successives du processus du cycle de vie des appareils. Ce processus doit changer, se développer et s'adapter en permanence pour répondre aux défis du paysage moderne des menaces et à l'évolution des besoins de l'institution.

« La vie ne peut être comprise qu'à rebours ; mais elle doit être vécue en allant de l'avant. »

– Sören Kierkegaard

Éducation permanente

Cette citation de Kierkgaard illustre une dichotomie entre les stratégies proactives et réactives. Ce n'est qu'après une violation de données qu'on peut évaluer le véritable impact des incidents de cybersécurité. Pourtant, quelle que soit leur tolérance au risque, les institutions doivent faire tout ce qui est en leur pouvoir pour éviter cette situation.

L'informatique et la sécurité s'appuient sur des cycles de vie pour simplifier la gestion d'un grand nombre d'aspects, des appareils aux applications en passant par les contrôles de cybersécurité, entre autres. L'objectif principal de ces cycles de vie est de minimiser les risques à chaque phase. Tout comme les stratégies de défense en profondeur reposent sur des contrôles de sécurité multicouches, une approche de la cybersécurité basée sur le cycle de vie gère les risques à chaque étape de la vie utile d'un appareil. Elle s'appuie sur la force de chaque étape pour consolider la suivante.

Par exemple :

- Achats : acquisition de matériel et de logiciels auprès de partenaires et de développeurs de confiance, en intégration directe avec la gestion des appareils pour sécuriser la chaîne d'approvisionnement.
- Approvisionnement : alignement des besoins de l'établissement sur des normes et des cadres appliqués à des solutions intégrées, afin de créer des profils de conformité de référence.
- Déploiement : installation de configurations standardisées et renforcées et d'applications gérées sur la base des profils de référence, afin d'optimiser les performances et la sécurité.
- Gestion : surveillance active et continue de l'état des terminaux, combinée à des procédures régulières de gestion des correctifs afin de minimiser les risques et de maintenir la conformité.
- Mise hors service : effacement sécurisé des données, récupération des licences, suivi de l'inventaire et mise au rebut (ou redéploiement) des appareils ; atténuation des pertes de données.

La nature itérative du cycle de vie assure la transmission des informations nécessaires à l'étape suivante. Ces informations n'aident pas seulement les administrateurs à relever les défis de la phase en cours, mais aussi à traiter les risques résiduels ou les lacunes qui peuvent être présents. Gage de cohérence pour l'ensemble de votre infrastructure, cette approche **renforce les mesures prises et les workflows à chaque étape**. L'objectif final est de combler des lacunes susceptibles d'introduire des risques imprévus – vulnérabilités, compromissions et violations de données – qui pourraient échapper à votre plan de cybersécurité.

Points clés

Pour l'enseignement supérieur, la feuille de route est claire : intégrer les outils de gestion individuelle, d'identité et de sécurité de manière à ce qu'ils forment une solution holistique. Cette solution ouvre la voie à des workflows avancés et permet de coordonner des contrôles complets pour mettre en œuvre une stratégie de défense en profondeur. Il s'agit d'identifier les menaces, de prévenir les attaques sophistiquées et d'atténuer les vecteurs de risques nuisibles à l'apprentissage sur tous les appareils mobiles et de bureau, où qu'ils soient et y compris lorsqu'ils utilisent des connexions non fiables.

Plusieurs mesures permettent de parvenir à cet équilibre :

- Développer un plan de sécurité basé sur une stratégie de défense en profondeur
- Intégrer les outils de gestion, d'identité et de sécurité dans une solution globale
- Mettre en place des workflows sophistiqués et informés par une surveillance active, et partager des données télémétriques riches sur l'état des appareils, en temps réel et de façon sécurisée.
- Fournir des identifiants cloud et les lier à des autorisations pour limiter l'accès aux seuls utilisateurs autorisés.
- Uniformiser le durcissement des appareils et le déploiement de configurations sécurisées en établissant des profils de référence visant à aligner la posture de sécurité des appareils sur la tolérance au risque.
- Déployer des contrôles de sécurité des terminaux sur l'appareil et le réseau pour atténuer les vecteurs de risque, corriger les vulnérabilités et empêcher l'exfiltration des données.
- Incorporer des technologies sophistiquées basées sur des modèles zero-trust pour chiffrer les demandes de connexion aux ressources protégées en fonction de la tolérance au risque.
- Appliquer systématiquement des profils de référence répondant aux besoins institutionnels et aux exigences de conformité, en s'appuyant sur les bonnes pratiques et les cadres de sécurité du secteur.
- Maintenir la conformité en instituant une gestion basée sur les règles qui atténue automatiquement les risques en corrigeant les appareils non conformes.
- Tirer parti de l'IA/ML pour systématiser la recherche des menaces inconnues au-delà de la protection contre les attaques sophistiquées et convergentes.

jamf

www.jamf.com/fr

Découvrez comment Jamf peut vous aider à mettre en place une solution globale de gestion et de sécurité des appareils Apple sur votre campus.