jamf

Introduction à la conformité dans l'éducation

Élaborer un plan de conformité pour les établissements primaires et secondaires afin de protéger les élèves, les enseignants et les communautés

Le paysage moderne de la conformité dans l'enseignement primaire et secondaire

Quel que soit le secteur d'activité, la conformité de la sécurité des appareils et des réseaux peut être un défi d'une grande complexité. Les normes industrielles évoluent au fil du développement des capacités des appareils, parallèlement aux lois et aux bonnes pratiques.

Ces complexités sont accentuées dans les environnements de l'enseignement primaire et secondaire.

Découvrez :

- **Comment suivre l'évolution constante des exigences de conformité dans le secteur de l'éducation**
- **L'importance d'une approche stratégique de l'infrastructure de conformité**
- **Comment mettre en place des pratiques de conformité durables**

Ce document est fourni à titre d'information uniquement et ne constitue pas un avis juridique. Les exigences de conformité varient selon les juridictions et les institutions. Nous recommandons aux écoles et aux collectivités de consulter un conseiller juridique qualifié pour déterminer leurs obligations spécifiques en matière de conformité.

Les défis uniques de la conformité dans l'enseignement primaire et secondaire

Comme les entreprises, les établissements scolaires doivent sécuriser la grande diversité d'appareils et d'utilisateurs qui se connectent à leur réseau pour les protéger des cyberattaques.

Mais contrairement à elles, les écoles doivent aussi faciliter des communications libres et ouvertes avec les parents et le public, qui utilisent tous des appareils que votre district ne contrôle pas.

Le résultat : une grande surface d'attaque. Si l'on ajoute à cela les contraintes budgétaires qui pèsent sur de nombreux établissements, on comprend que la conformité en matière de sécurité soit un défi permanent.

Les utilisateurs des appareils et des réseaux scolaires sont uniques, eux aussi.

Si une chose distingue fondamentalement les entreprises et les écoles, c'est que les secondes sont au service d'une grande diversité d'utilisateurs : les enseignants, les administrateurs et le personnel administratif, bien sûr, mais aussi un public bien plus délicat, celui des enfants.

Les enfants sont curieux. Ils ont besoin d'outils d'apprentissage interactifs et immersifs. Ils doivent acquérir les compétences nécessaires pour devenir des citoyens numériques responsables et partager ce qu'ils ont appris avec leurs enseignants, leur famille et leurs camarades.

La curiosité des enfants n'a pas de limite.

C'est pourquoi le service informatique scolaire doit établir certaines limites. Sa mission : protéger les enfants contre les tentatives d'hameçonnage, les logiciels malveillants et les contenus dangereux ou inappropriés, sans freiner l'apprentissage ni l'enseignement au quotidien.

Les écoles doivent également trouver le juste équilibre entre les pratiques de cybersécurité et le respect de la vie privée des élèves. Pour certains des élèves particulièrement vulnérables, comme les enfants LGBTQIA+, une violation de confidentialité peut faire peser un grand danger sur leur santé mentale et leur sécurité physique.

Normes et exigences

Dans le monde entier, les établissements scolaires font l'objet d'une étroite surveillance et d'énormes pressions :

1. **Législation nationale et internationale**
2. **Lois et normes régionales**
3. **Organismes de supervision du secteur de l'éducation**

Dans l'UE, le Règlement général sur la protection des données (RGPD) protège les données des élèves, par exemple. Le Royaume-Uni a adopté une version britannique du RGPD, le UK RGPD, ainsi que la loi sur la Protection des données de 2018. À cela s'ajoutent des lois et réglementations qui s'appliquent spécifiquement aux enfants, comme la loi américaine sur la Protection des enfants sur Internet (Children Internet Protection Act).

Les établissements scolaires sont souvent soumis à des obligations qui touchent à la sécurité des données, du réseau et des appareils, comme la loi américaine sur les Personnes handicapées (Americans with Disabilities Act).

Pensez également aux certifications de sécurité comme StateRAMP et FedRAMP, deux niveaux de sécurité souvent exigés par les organisations gouvernementales pour nouer des partenariats avec des établissements scolaires.

Le défi de la transformation numérique

Dans le monde entier, la pandémie de COVID-19 et l'importance accrue de la sécurité dans les écoles ont entraîné un changement radical et rapide dans l'enseignement primaire et secondaire.

La transformation numérique des écoles a plusieurs volets :

- **Passage d'un environnement d'apprentissage papier à un environnement numérique**
- **Obligations accrues en matière de collecte et de stockage des données**
- **Mise en place de l'apprentissage à distance et hybride et prise en compte de ses effets sur la conformité**

Des thèmes de conformité communs à tous les cadres

Comme on l'a vu, de nombreuses différences distinguent la situation des entreprises et des écoles. Ces dernières doivent d'ailleurs respecter des exigences et des bonnes pratiques dans plusieurs domaines :

- Protection des données et confidentialité
- Sécurité des appareils et des réseaux
- Contrôle d'accès et authentification
- Réponse aux incidents et notification des violations
- Pistes d'audit et rapports

Les cyberattaques se multiplient dans l'enseignement primaire et secondaire

Malheureusement, les administrations scolaires sont une cible de choix pour les cybercriminels.

Les données hébergées par les établissements (numéros de sécurité sociale et autres identifiants) sont particulièrement lucratives. En outre, certaines administrations conservent les informations de carte de crédit des parents dans leurs dossiers pour les repas scolaires et les frais de scolarité.

Le phénomène est très répandu ; selon l'enquête britannique sur les Violations la cybersécurité en 2025, 44 % des écoles primaires et 60 % des écoles secondaires ont subi des failles ou des attaques cette année-là.

Le coût de la non-conformité

De nombreux établissements ont payé ce prix. Certains ont été contraints de payer des rançons, d'autres ont été poursuivis par des parents pour des fuites de données. D'autres encore ont fait la une des journaux parce qu'ils avaient été incapables de protéger leurs réseaux et leurs données ou de signaler correctement les violations.

Sanctions financières et conséquences juridiques

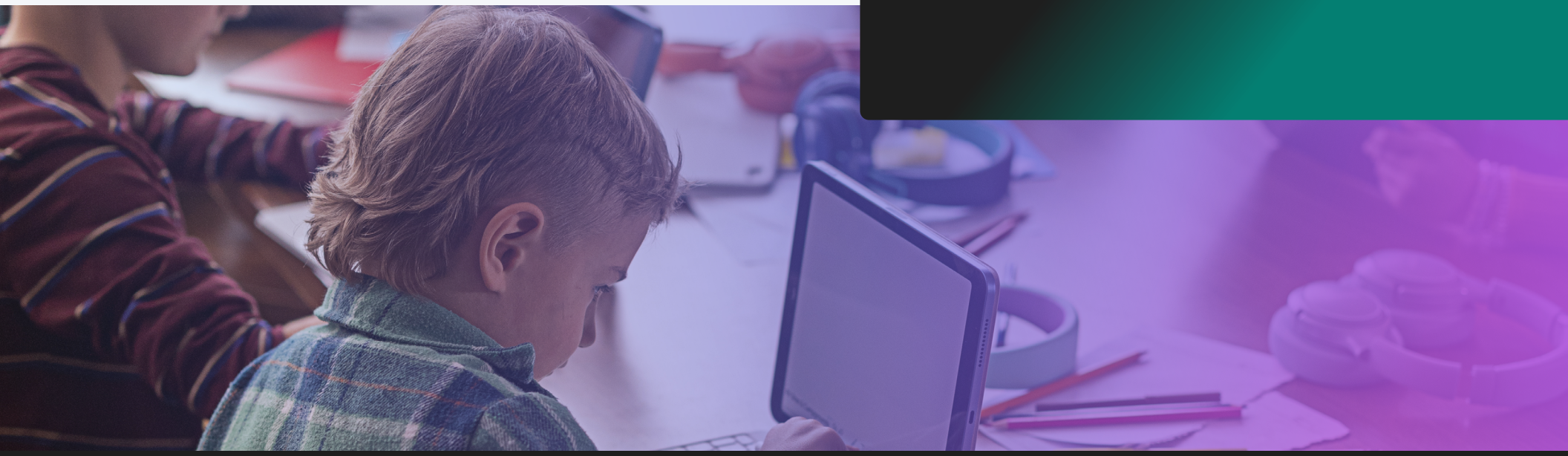
Comme nous l'avons dit, les établissements, les administrations et même les fournisseurs qui ne respectent pas des règles strictes de conformité en matière de sécurité et de protection des données peuvent se retrouver exposés à des difficultés financières et juridiques.

Rançons exorbitantes, infractions aux lois fédérales ou internationales sur la confidentialité des élèves, poursuites en justice par les parents… la liste est longue.

Quand l'attaque cible le fournisseur

En 2024, une plateforme de gestion des informations des élèves (SIS) et de technologie éducative très répandue a dû verser une rançon de 2,85 millions de dollars à un pirate qui menaçait de divulguer les données des étudiants.

L'année suivante, le même pirate a contacté des administrations scolaires équipées de ce même logiciel pour leur présenter des demandes similaires.



Des dommages pour la réputation et la confiance de la communauté

Les établissements scolaires peuvent perdre la confiance des bailleurs de fonds, des parents et des entreprises locales, en particulier lorsqu'elles n'ont pas fixé de règles claires sur la communication des violations.

Quand les pirates s'en prennent à l'administration scolaire

Au cours d'une attaque de ransomware en 2023, un district scolaire d'une ville américaine n'a pas informé le public que des pirates menaçaient de divulguer des données extrêmement sensibles si on ne leur versait pas de rançon. L'administration a refusé de payer et les informations ont été rendues publiques. Pourtant, elle a encore attendu des mois avant d'informer les élèves concernés. Ces manquements ont suscité une profonde indignation dans l'opinion publique et dégradé la réputation du district.

Les gens sont naturellement sensibles aux questions de confidentialité qui touchent aux enfants. En l'absence de lignes directrices claires, les écoles et les administrations sont confrontées à une multitude de conseils différents et parfois contradictoires. Lorsque les autorités scolaires agissent de manière incohérente, le public imagine souvent le pire.

Perturbation des opérations et affectation des ressources

Si les cyberattaques ont presque toujours le profit pour but ultime, leurs modalités peuvent perturber les systèmes scolaires de différentes manières :

- **Ralentissement du versement des salaires**
- **Retard dans les corrections de devoirs**
- **Fermeture complète de l'école pendant plusieurs jours**

Quand l'école doit fermer

En janvier 2026, une cyberattaque visant un établissement secondaire du Royaume-Uni a entraîné sa fermeture totale pendant une semaine. Elle a en effet mis à mal « l'ensemble du système informatique de l'école [...], y compris le téléphone, le courrier électronique, Google Classroom, les systèmes de gestion de l'école et Microsoft SharePoint ».

Maintenant que vous comprenez ces risques, explorons les fondamentaux d'un plan de conformité solide.

Les quatre piliers de la conformité dans l'enseignement primaire et secondaire

1. Confidentialité des données des élèves

Que sont les données des élèves ?

Pour créer des règles et des procédures visant à protéger les données des élèves (ainsi que celles des enseignants et des parents), il faut d'abord comprendre de quoi elles sont composées. Un rapide inventaire non exhaustif :

- Noms, dates de naissance, adresses postales et adresses électroniques personnelles
- Nom des parents, informations sur le lieu de travail et numéros de carte de crédit
- Données pédagogiques (notes et résultats)
- Registres de santé, de comportement et d'assiduité

Principes de minimisation des données

En réduisant au minimum la quantité de données collectées et la durée de leur conservation, vous contribuerez grandement à préserver la confidentialité des informations des élèves. Ne collectez que ce qui est nécessaire à vos opérations, pendant le temps requis par vos obligations. Les pirates ne peuvent pas accéder aux informations que vous ne possédez pas !

N'accordez aux différents acteurs que l'accès aux données dont ils ont spécifiquement besoin. Un accès limité réduit la surface d'attaque.

Fixer des exigences en matière de consentement et de notification. Faites preuve de transparence lorsque vous demandez des données en précisant les motivations de la collecte, ainsi que la durée et le lieu de stockage. Cela contribuera grandement à renforcer la confiance de la communauté.

Gérez attentivement les fournisseurs tiers, en particulier les éditeurs de logiciels de test ou d'applications éducatives.Vérifiez qu'ils respectent bien les protocoles de sécurité et de confidentialité. Définissez des politiques et des workflows pour encadrer étroitement les données auxquelles ils peuvent accéder ainsi que les modalités de leur exploitation. Cela peut vous mettre à l'abri du type d'attaque le plus courant : les attaques ciblant la chaîne d'approvisionnement.

Les quatre piliers de la conformité dans l'enseignement primaire et secondaire

2.

Les fondamentaux de la gestion des accès

Principes de l'accès basé sur le rôle

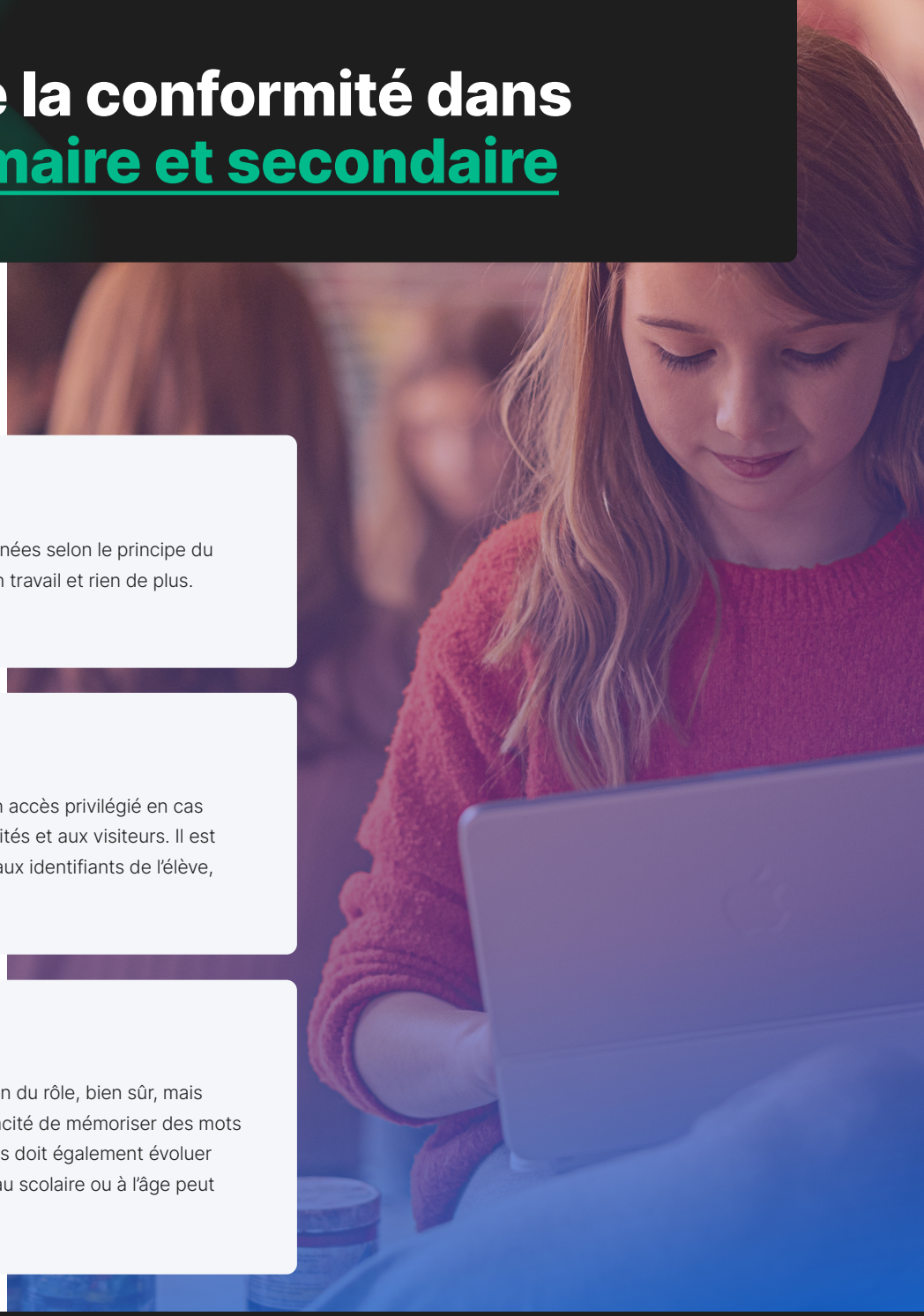
Comme on l'a vu, il est essentiel de gérer l'accès aux réseaux et aux données selon le principe du minimum nécessaire : donnez à chacun ce dont il a besoin pour faire son travail et rien de plus. Posez-vous la question : qui doit avoir accès à quoi et quand ?

Appliquer des règles d'accès basé sur le rôle

Assurez-vous que vous disposez d'un moyen de donner au personnel un accès privilégié en cas de besoin, tout en appliquant le principe du minimum nécessaire aux invités et aux visiteurs. Il est souvent plus facile de contrôler ces autorisations lorsqu'elles sont liées aux identifiants de l'élève, du parent ou de l'enseignant.

Flexibilité en fonction de l'âge

Les exigences en matière d'accès et d'authentification varient en fonction du rôle, bien sûr, mais aussi en fonction de l'âge. Les jeunes élèves n'ont pas forcément la capacité de mémoriser des mots de passe complexes, contrairement à leurs camarades plus âgés. L'accès doit également évoluer en fonction des programmes scolaires. L'attribution de rôles liés au niveau scolaire ou à l'âge peut considérablement simplifier l'administration à long terme.



Les quatre piliers de la conformité dans l'enseignement primaire et secondaire

3.

Exigences de l'infrastructure de sécurité

Une infrastructure de sécurité clairement définie et des stratégies vigoureuses de protection des points terminaison peuvent limiter le rayon d'impact d'une violation et éviter des compromissions d'appareils.

Stratégies de protection des points de terminaison

Mettez en place une protection des points de terminaison combinant les fonctionnalités suivantes :

- Prévention et remédiation automatisées des menaces
- Analyse sur l'appareil et rapports proactifs
- Application automatisée des règles de consommation des données

Aussi important que les fonctionnalités elles-mêmes : la mise en œuvre de votre solution ne doit pas compromettre la sécurité, la confidentialité, ni les performances de l'environnement.

Considérations sur la segmentation du réseau

L'un des meilleurs moyens d'éviter qu'une faille locale ne devienne une violation majeure consiste à segmenter le réseau en fonction de ses utilisateurs ou de la partie de l'organisation à laquelle il est destiné. Vous pouvez ainsi créer des réseaux d'administrateurs et d'enseignants, des réseaux d'élèves et des réseaux d'invités.

Suite...

Les quatre piliers de la conformité dans l'enseignement primaire et secondaire

3. Exigences en matière d'infrastructure de sécurité

Normes de chiffrement et mise en œuvre

Examinez attentivement les stratégies de chiffrement et de mise en œuvre exigées par vos différents organismes de réglementation, ainsi que les bonnes pratiques à respecter :

- Algorithmes de chiffrement puissants
- Gestion sécurisée des clés
- Chiffrement des données lors de leur stockage et de leur transmission

Évaluations régulières de la sécurité

Avec le renouvellement des populations d'élèves et l'évolution des technologies éducatives, il est indispensable de procéder à des évaluations de sécurité régulières, et ce, pour garantir la continuité des activités.

Cela vous donnera l'occasion :

- D'intégrer des technologies innovantes et émergentes
- De créer des politiques pour répondre aux modifications des bonnes pratiques et des exigences de conformité internes ou externes.
- De vérifier s'il y a des angles morts dans les rapports
- D'évaluer vos fournisseurs et de déterminer s'ils sont à la hauteur de l'évolution de vos besoins

Les quatre piliers de la conformité dans l'enseignement primaire et secondaire

4. Documentation et préparation aux audits

La préparation des audits peut être pénible. Pourtant, une bonne préparation aura le double avantage de vous faire gagner du temps une fois le moment de l'audit venu et de renforcer la sécurité de vos réseaux et de vos données.

Abordez-la de façon méthodique :

Catégories de données à gérer et à inclure dans les rapports

Vous avez trois grands groupes de données à suivre :

Données sur les élèves : assiduité, notes et comportement
Données opérationnelles : rapports sur les actifs informatiques, configurations de réseau et journaux de sécurité.
Données juridiques : documents de conformité, contrats avec les fournisseurs et rapports d'audit.

Pratiques d'archivage importantes

Les données doivent être sécurisées, centralisées et conformes en tout temps. Pour atteindre cet objectif, il faut :

Utiliser un système d'information sur les étudiants (SIS)

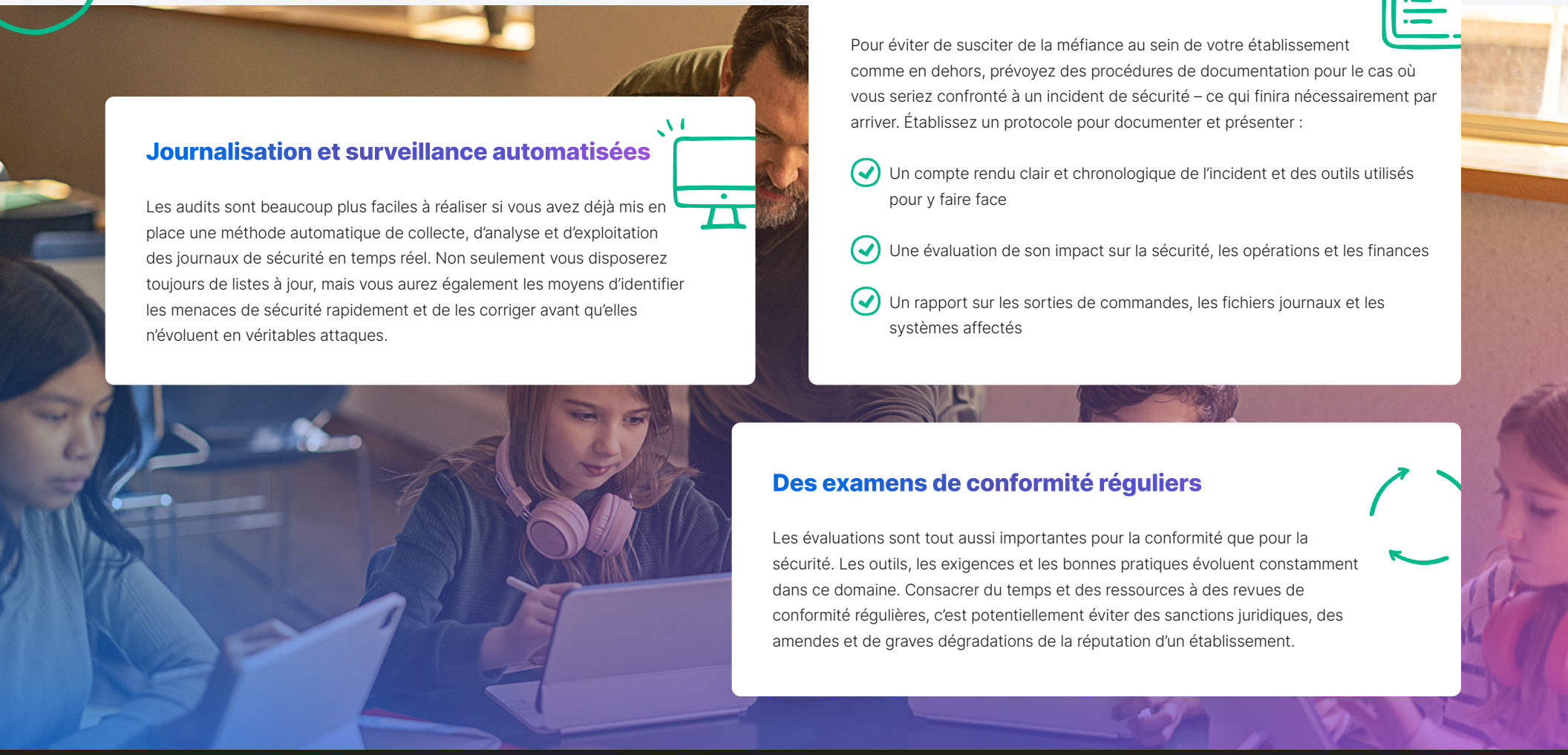
Gérer l'inventaire du matériel et des logiciels

Numériser les documents lorsque cela s'avère nécessaire

Suite ...

Les quatre piliers de la conformité dans l'enseignement primaire et secondaire

4. Documentation et préparation aux audits



Journalisation et surveillance automatisées

Les audits sont beaucoup plus faciles à réaliser si vous avez déjà mis en place une méthode automatique de collecte, d'analyse et d'exploitation des journaux de sécurité en temps réel. Non seulement vous disposerez toujours de listes à jour, mais vous aurez également les moyens d'identifier les menaces de sécurité rapidement et de les corriger avant qu'elles n'évoluent en véritables attaques.

Procédures de documentation des incidents

Pour éviter de susciter de la méfiance au sein de votre établissement comme en dehors, prévoyez des procédures de documentation pour le cas où vous seriez confronté à un incident de sécurité – ce qui finira nécessairement par arriver. Établissez un protocole pour documenter et présenter :

- Un compte rendu clair et chronologique de l'incident et des outils utilisés pour y faire face
- Une évaluation de son impact sur la sécurité, les opérations et les finances
- Un rapport sur les sorties de commandes, les fichiers journaux et les systèmes affectés

Des examens de conformité réguliers

Les évaluations sont tout aussi importantes pour la conformité que pour la sécurité. Les outils, les exigences et les bonnes pratiques évoluent constamment dans ce domaine. Consacrer du temps et des ressources à des revues de conformité régulières, c'est potentiellement éviter des sanctions juridiques, des amendes et de graves dégradations de la réputation d'un établissement.

ÉVALUER L'ÉTAT DE PRÉPARATION À LA CONFORMITÉ

Est-ce que votre environnement est prêt ?

Check-list d'auto-évaluation

Ce processus rigoureux, complexe et dynamique peut sembler insurmontable. Heureusement, les check-lists peuvent aider votre équipe à s'assurer qu'elle n'a rien oublié.

PRÉPARATION DE L'INFRASTRUCTURE TECHNOLOGIQUE

Avez-vous mis en place les éléments suivants ?

- [ ] Système d'inventaire et de gestion des appareils
- [ ] Gestion centralisée des identités et des accès
- [ ] Segmentation du réseau pour séparer les systèmes étudiants et administratifs
- [ ] Protection des points de terminaison déployée sur tous les appareils
- [ ] Chiffrement des données au repos et en transit
- [ ] Procédures automatisées de sauvegarde et de récupération
- [ ] Capacités de surveillance de sécurité et d'alerte

PRÉPARATION EN TERMES DE RÈGLES ET DE GOUVERNANCE

Avez-vous documenté ou établi :

- [ ] Des règles globales d'utilisation acceptable
- [ ] Des règles de conservation et d'élimination des données
- [ ] Des procédures de réponse aux incidents
- [ ] Des programmes de formation du personnel
- [ ] Des processus de gestion des fournisseurs et de diligence raisonnable
- [ ] Un calendrier régulier de révision et de mise à jour des règles

PRÉPARATION OPÉRATIONNELLE

Avez-vous :

- [ ] Désigné un responsable ou une équipe en charge de la conformité
- [ ] Réalisé des évaluations régulières de la sécurité
- [ ] Mis en place des fonctions de suivi d'audit
- [ ] Établi des procédures de notification des violations
- [ ] Défini des protocoles de communication avec les parents et les élèves
- [ ] Créé des systèmes de documentation et de tenue des registres

PRÉPARATION DES FOURNISSEURS ET DES TIERS

Avez-vous mis en place :

- [ ] Des accords sur le traitement des données avec tous les fournisseurs
- [ ] Un processus de vérification des certifications de sécurité
- [ ] Des évaluations régulières de la sécurité des fournisseurs
- [ ] Des contrôles clairs en matière de partage des données et d'accès
- [ ] Des exigences de notification des incidents pour les fournisseurs

Jamf for K-12, votre allié pour la conformité

Si Jamf for K-12 n'a pas directement pour fonction d'automatiser et de garantir la conformité de votre établissement, il fournit une infrastructure essentielle qui soutient votre stratégie globale de conformité :

Gestion et sécurité des appareils

- Inscription et configuration centralisées des appareils
- Application automatisée des règles de sécurité
- Gestion et protection des appareils à distance
- Inventaire et rapports complets sur les appareils

Contrôle d'accès et authentification :

- Intégration avec les fournisseurs d'identité pour l'authentification SSO
- Gestion des accès basée sur le rôle
- Restrictions de contenu et d'applications basées sur le rôle
- Authentification sécurisée sur l'ensemble des appareils et des plateformes

Gestion évolutive :

- Application homogène des règles sur tous les appareils
- Gestion efficace des grands déploiements d'appareils
- Déploiement des règles à l'échelle de vastes parcs d'appareils
- Prise en charge de différents environnements d'apprentissage (1:1, appareils partagés, BYOD)

Possibilités d'intégration

- Compatible avec les systèmes informatiques scolaires existants
- Prise en charge des applications éducatives tierces
- Intégration à l'infrastructure du réseau
- Connexion aux solutions de gestion des identités et des accès

La plateforme Jamf offre aux administrations scolaires un socle pour créer l'environnement technologique fiable, sécurisé et gérable que réclament les cadres de conformité.

Grâce à nos automatisations et à nos fonctionnalités, votre équipe est libérée des défis quotidiens de la gestion des appareils et peut se concentrer sur les règles, la formation et les initiatives stratégiques de conformité.

Dans l'enseignement primaire et secondaire, la conformité est un processus continu.

Cette pratique évolue en même temps que votre technologie, votre population d'élèves et le paysage réglementaire.

La bonne nouvelle, c'est que vous n'avez pas à construire ce socle tout seul.

Jamf for K-12 donne à votre équipe les outils dont elle a besoin pour gérer les appareils, appliquer des règles et maintenir un environnement sécurisé, vérifiable et conforme. Le résultat : moins de temps passé à gérer l'infrastructure, et plus d'énergie pour les tâches qui comptent vraiment.

Demandez un essai gratuit

jamf