Introduction à la sécurité dans les écoles primaires et secondaires

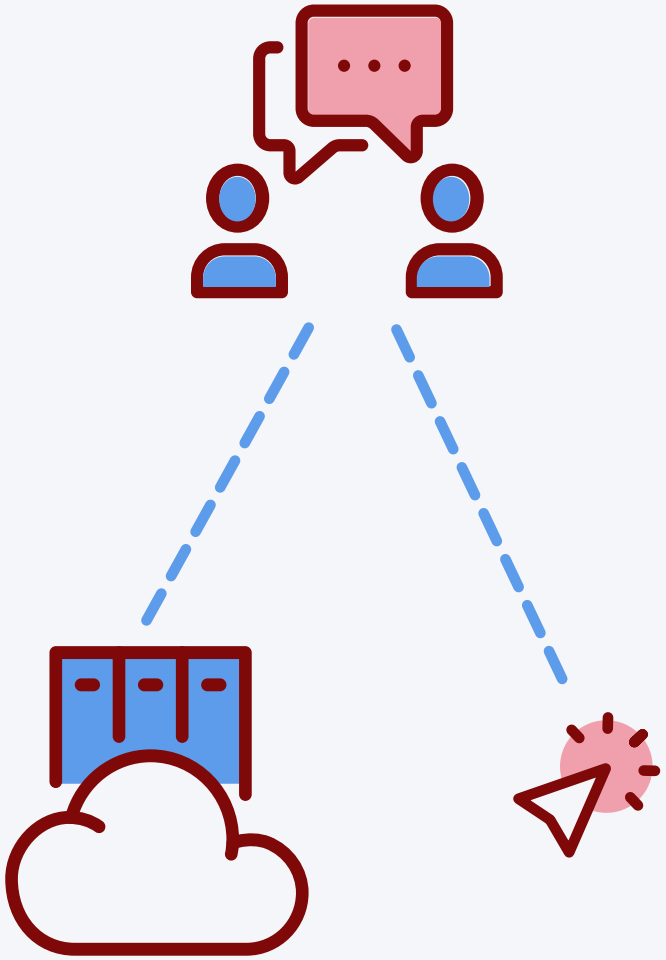
jamf

Peu de secteurs ont autant été affectés par la transformation de la technologie que l'éducation.

Les progrès de l'informatique personnelle et le développement de services basés sur le cloud ont révolutionné certains principes fondamentaux de l'apprentissage :

- Affranchi des limites physiques, l'accès aux livres et aux ressources a connu une croissance exponentielle.
- Des lignes de communication mondiales relient les élèves, les enseignants et les parents.
- Les tests standardisés ont été uniformisés par l'adoption des modèles informatiques.
- Il est possible de répondre aux différents besoins des élèves grâce à un appareil commun doté d'apps spécialisées.
- L'intégration des outils technologiques permet la convergence entre les multiples modalités d'éducation et styles d'enseignement.
- L'apprentissage à distance s'est avéré être une méthode d'éducation viable, capable de surmonter les contraintes d'une pandémie ou d'un autre type de crise.

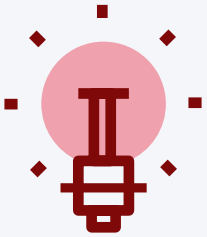
Créer une vision



Une chose est claire : la technologie dans son ensemble a été adoptée par les établissements d'enseignement primaires et secondaires depuis ce jour de 1983 où l'un des premiers ordinateurs d'Apple, l'Apple IIe, a appris à de jeunes esprits à ajouter, lire et taper. Aujourd'hui, ces enfants sont des adultes – et même des enseignants, pour certains – et cultivent cette pratique. Ils utilisent les Macbook air et iPads les plus récents, ainsi qu'un catalogue croissant de près de 2 millions d'applications, pour éduquer les élèves d'aujourd'hui.

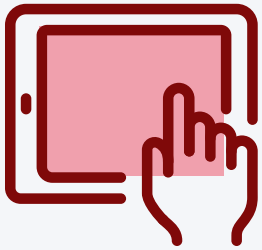
À l'époque, le terme-même cybersécurité existait à peine. Mais quarante ans plus tard, le paysage informatique moderne a considérablement changé. Même en revenant quinze ans en arrière, la situation était très différente : l'environnement de vos appareils n'était pas peuplé d'une myriade de menaces. Des rançongiciels peuvent bloquer l'accès à des données et des services essentiels. Les violations de données peuvent compromettre des dossiers d'élèves et des données sensibles. Les menaces actuelles peuvent même représenter un risque important pour la sécurité des personnes, en capturant des données confidentielles sans autorisation.

Cet e-book n'a pas pour but d'inspirer la peur. Il cherche plutôt à sensibiliser le lecteur aux problèmes de sécurité très réels et parfois effrayants qui touchent le secteur de l'éducation.



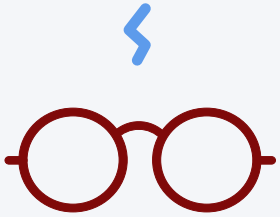
Créer une vision

Éloignons-nous un moment des aspects les plus effrayants. En effet, les menaces prennent le plus souvent la forme d'une perte d'utilisation ou d'accès aux ressources. Et ces retards sont un obstacle à l'apprentissage. D'autre part, certaines réglementations sont mises en place pour empêcher ces situations. Mais elles sont parfois liées à des structures de financement qui, en cas de violation de la conformité, affectent directement la capacité d'une école à apporter le niveau de service attendu par les parties prenantes et la communauté.



Dans cet e-book, nous abordons les menaces de cybersécurité qui visent spécifiquement les établissements primaires et secondaires. Nous allons expliquer pourquoi il est indispensable de s'y préparer, mais aussi :

- **Examiner le rôle crucial que joue la cybersécurité aujourd'hui – et dans l'avenir de l'éducation.**
- **Illustrer les menaces externes et internes qui constituent la majorité des attaques malveillantes contre les établissements primaires et secondaires.**
- **Identifier les pratiques à renforcer pour protéger les appareils, les données confidentielles et les élèves.**
- **Aborder les idées fausses les plus courantes concernant Apple et la sécurité.**
- **Souligner l'importance des programmes de formation des parties prenantes pour la réussite des programmes de cybersécurité.**
- **Expliquer comment les solutions Jamf atténuent les risques tout en sécurisant de manière exhaustive votre flotte de terminaux.**

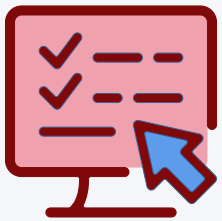


Bienvenue à Poudlard

Dans le monde magique de Harry Potter, le personnage éponyme – un élève au potentiel incroyable – fréquente l'école de Poudlard. Avec ses camarades, il reçoit un enseignement magique selon différentes méthodes. Mais ce que les enseignants leur transmettent ne se résume pas à cela, n'est-ce pas ?

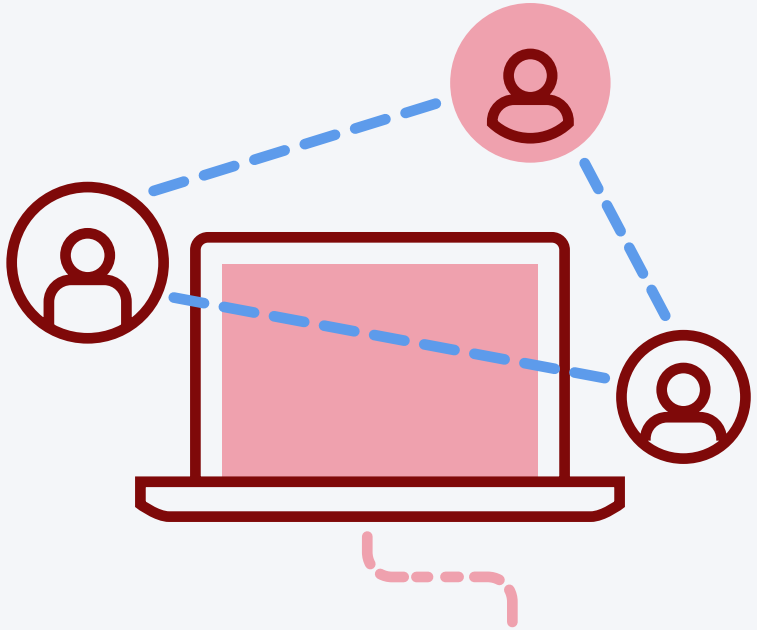
Bien sûr que non. En réalité, les élèves de Poudlard, tout comme leurs homologues des établissements primaires et secondaires du montre réel, embarquent pour un véritable voyage : ils vont acquérir des connaissances dans de nombreuses matières différentes, tout au long de leur scolarité. Certaines sont scolaires, d'autres extrascolaires, mais toutes forment un tissu cohérent qui constitue une éducation complète et équilibrée.

Bien mise en œuvre, la cybersécurité fonctionne à peu près de la même manière, et répond aux besoins et aux exigences uniques du secteur de l'enseignement primaire et secondaire. Mais il n'existe pas de sort, comme Lumos, pour éclairer les secrets de la protection des terminaux. Par contre, une collection d'outils, assortie de bonnes pratiques et d'une formation des utilisateurs finaux, peut maintenir la posture de sécurité de l'infrastructure de votre établissement.



Pourquoi la cybersécurité est-elle aussi importante ?

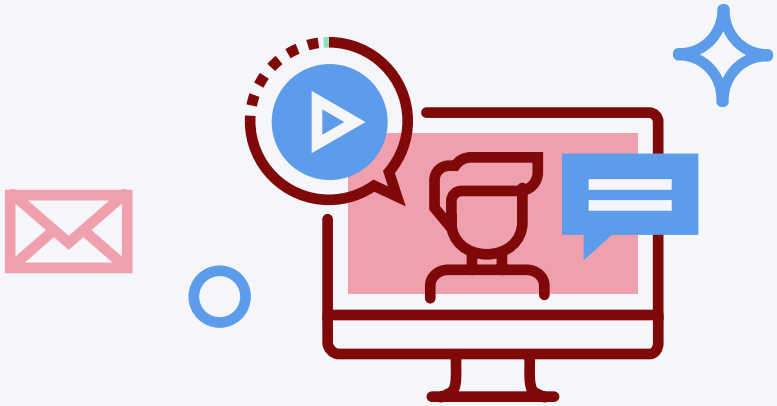
La vocation de la cybersécurité est de garantir la sécurité, la confidentialité et l'intégrité de vos terminaux – élèves, données et appareils. Son importance est accentuée par plusieurs défis spécifiques à l'éducation qui, parfois, empêchent les organisations de mettre en œuvre les solutions nécessaires pour atténuer les menaces malveillantes et combattre les attaques.



Contraintes budgétaires

Dans un article détaillant comment les écoles américaines luttent pour financer notre avenir, le magazine Forbes relève que « les États qui ont atteint à la fois l'équité et l'adéquation affichent des taux de réussite et de diplômes plus élevés... ». Tous les enseignants ou presque vous le diront. Quand ils ont besoin d'une ampoule de rechange pour leur projecteur LCD ou d'un point d'accès au Wi-Fi plus puissant, on leur répond souvent que c'est impossible, à cause du manque de financement.

Les préoccupations budgétaires sont souvent au cœur des initiatives de modernisation l'infrastructure. Il s'agit de mettre à jour l'équipement de réseau pour offrir une connectivité plus rapide ou prendre en charge davantage d'appareils. C'est notamment le cas dans les districts qui adoptent un modèle d'appareil 1:1, et qui doivent également acquérir des services de sécurité pour détecter et bloquer les logiciels malveillants sur le parc de l'école.



Infrastructure existante

Dans un contexte de restrictions budgétaires, les écoles sont souvent contraintes de « faire plus avec moins ». Autrement dit, continuer à utiliser des équipements obsolètes et dépassés longtemps après que le fournisseur a cessé de les prendre en charge. Certes, ces appareils vétustes fonctionnent encore, techniquement parlant. Mais ils disposent rarement des ressources nécessaires pour être compatibles avec les applications et services modernes, comme les tests informatisés (CBT).

Dans certains cas, les appareils eux-mêmes sont à la limite de l'utilisabilité, ce qui pose divers problèmes aux élèves et aux enseignants. Surtout, ces appareils et applications d'un autre âge ne sont plus pris en charge – et les conséquences sont lourdes. En effet, cela signifie qu'ils ne reçoivent plus les correctifs de sécurité qui résolvent normalement les bugs des logiciels et comblent les vulnérabilités. Or ces vulnérabilités sont exploitées par les acteurs malveillants pour obtenir un accès non autorisé aux données. Le résultat : un trou béant dans la sécurité sans moyen de défense, jusqu'au renouvellement des machines ou des applications.

Informatique de l'ombre

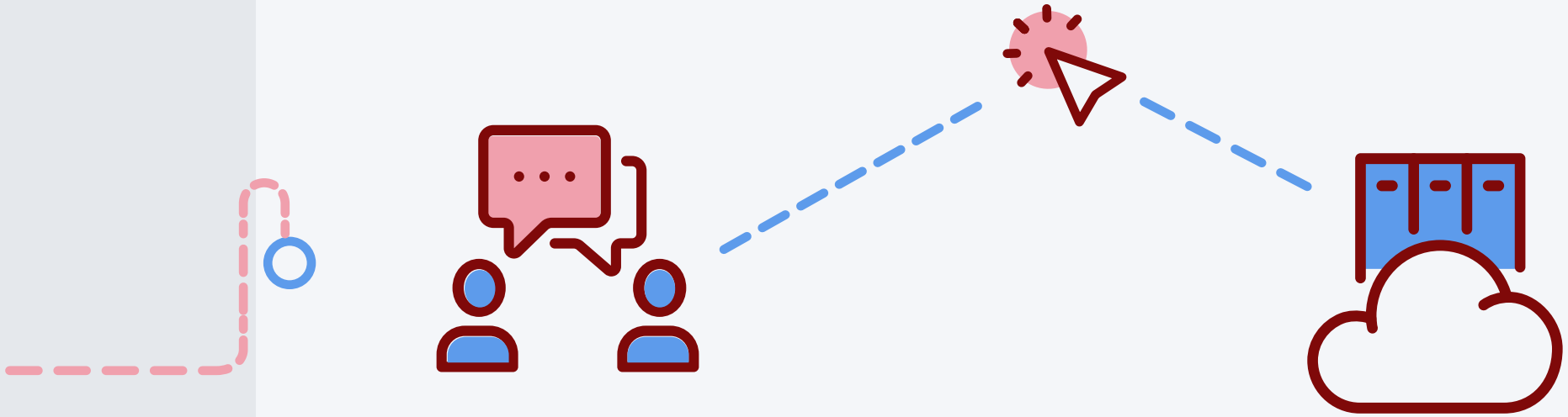
L'informatique de l'ombre désigne l'utilisation d'appareils, d'applications ou de services informatiques non gérés ou approuvés par le service informatique du district. Vous utilisez votre ordinateur personnel, qui contourne les configurations strictes des appareils fournis par l'école ? Vous apportez le routeur Wi-Fi de votre domicile pour « augmenter » la bande passante sans-fil dans votre salle de classe ou votre bureau ? Vous utilisez, dans le cadre de votre travail d'étudiant ou d'enseignant, une Dropbox personnelle, ou toute autre application non approuvée ? Comme vous le voyez, l'informatique de l'ombre prend de nombreuses formes.

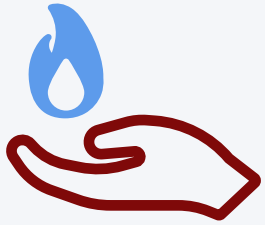
Elles semblent assez inoffensives, surtout lorsque des préoccupations budgétaires limitent l'accès aux technologies du quotidien, mais elles peuvent causer de graves problèmes. Ces apps et services n'ont pas fait l'objet d'un examen approfondi. Le service informatique ne sait pas dans quelle mesure leur utilisation au sein du réseau du district pose des problèmes ou des risques.

Manque de sensibilisation à la sécurité

Qui a le temps de se former à la sécurité, quand il faut déjà préparer la salle de classe, résoudre de petits (et grands) problèmes, prendre soin des élèves, élaborer des plans de cours, corriger les copies et... enseigner ? Nous le savons bien, c'est difficile !

Malheureusement, les acteurs malveillants le savent aussi. Non seulement ils tirent parti de la situation, mais ils profitent également des contraintes de temps et du manque de formation pour cibler le secteur de l'éducation. Pour assurer la cybersécurité, il est essentiel d'apprendre au personnel, aux élèves et aux parents à repérer activement les contenus malveillants des e-mails et les escroqueries par SMS. Il faut les former aux bonnes pratiques d'hygiène et de sécurité, à l'école comme à la maison.





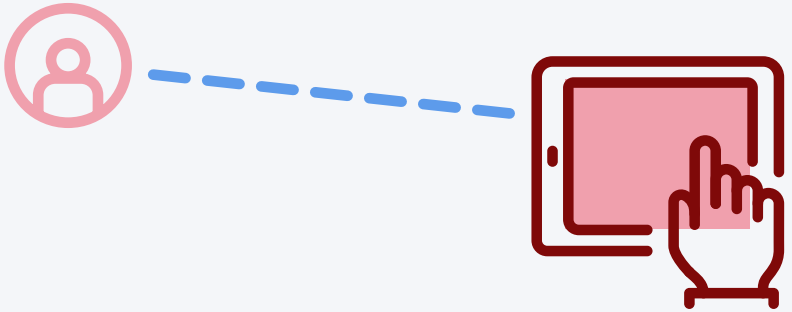
« Celui qui ne doit pas être nommé »

Pour affronter leur peur, les magiciens de la série Harry Potter ont dû franchir une première étape : la reconnaître et l'appeler par son nom, Voldemort. Ce n'est qu'après cela que les protagonistes ont pu se défendre contre le mal qui les menaçait.

De même, l'une des premières étapes pour une cybersécurité robuste consiste à évaluer les risques. Vous devez déterminer quels équipements, apps, services, etc., sont utilisés par le district scolaire, à quelle fréquence et à quel degré, puis les classer en fonction de leur caractère critique. Une fois cette étape franchie, vous pouvez alors « affronter vos peurs », car vous saurez quels types de menaces affectent les éléments de votre évaluation des risques.

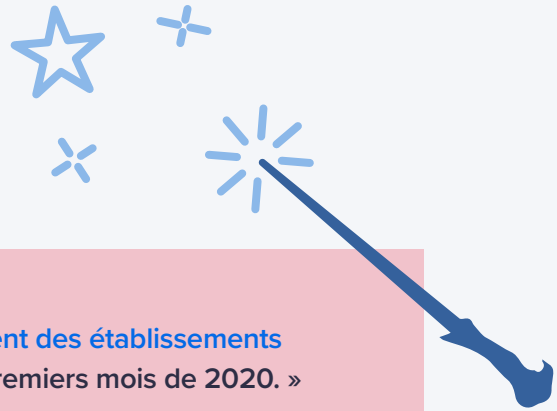
Ces listes peuvent – et vont – changer en fonction des besoins en infrastructure de votre district. Mais on sait que plusieurs menaces ciblent systématiquement l'enseignement primaire et secondaire.

Menaces externes



Parmi les types de menaces provenant de sources externes, les plus perturbatrices sont les logiciels malveillants et les attaques par déni de service (DoS). Ces attaques cherchent à empêcher l'accès aux applications, aux services et aux sites web en envoyant un flot de requêtes au service ciblé. Celui-ci devient alors incapable de répondre à une requête, légitime ou non. De grands districts scolaires ont été visé par des DoS ces dernières années. Pire encore, ces attaques peuvent provenir de plusieurs ordinateurs simultanément : c'est ce qu'on appelle le déni de service distribué (DDoS), contre lequel il est beaucoup plus difficile de se protéger.

Quant à la première menace évoquée, elle repose sur un type de logiciel malveillant appelé rançongiciel ou ransomware. Il chiffre des types de fichiers couramment utilisés, comme DOCX et PDF, à l'aide d'une clé générée de manière aléatoire. Une fois que c'est fait, il envoie un signal à un serveur à distance capable de déchiffrer ou de déverrouiller vos documents en échange d'une rançon – d'où son nom. La rançon demandée peut se compter en milliers de dollars – ou en millions.



> « **57 % des attaques de rançongiciels signalées concernaient des établissements primaires et secondes , c'est deux fois plus que dans les premiers mois de 2020.** »
>
> – Avis conjoint de cybersécurité, coécrit par le Bureau fédéral d'investigation (FBI), l'Agence de cybersécurité et de sécurité des infrastructures (CISA) et le Centre multi-états d'analyse et de partage des informations (MS-ISAC)

Mais les systèmes d'enseignement primaire et secondaire sont également ciblés par d'autres menaces et attaques externes :

Logiciels malveillants : cette catégorie générale englobe tous les codes malveillants. Les virus, par exemple, s'exécutent sur un appareil pour obtenir un accès non autorisé au matériel ou aux données, ainsi qu'à ceux qui y sont connectés au même réseau.

Les logiciels espions : ces logiciels malveillants fonctionnent en toute discrétion pour recueillir des informations sur l'utilisateur. Il acquiert des données (documents, photos, etc.) et recherche souvent des informations personnelles identifiables (IPI) : numéros de sécurité sociale, dossiers d'étudiants, enregistrements réalisés à partir de caméras et de microphones intégrés, données de localisation, cartes de crédit et identifiants financiers. Les auteurs de l'attaque cherchent ensuite à les vendre.

Man-in-the-Middle (MitM) : lorsque vous vous connectez au réseau Wi-Fi de votre école, savez-vous s'il s'agit réellement du bon service ? L'objectif des attaques MitM est d'inciter les utilisateurs à se connecter au site web ou au service d'un adversaire qui se fait passer pour un site légitime. Il peut ainsi récolter des identifiants qui permettront ensuite d'accéder aux ressources du district.

Hameçonnage : comme l'attaque MitM, l'hameçonnage repose sur l'ingénierie sociale pour tromper l'utilisateur. Par contre, il n'exploite pas nécessairement la technologie. Souvent, ces attaques se font par e-mail, par SMS ou par téléphone. L'adversaire persuade l'utilisateur (ou le menace de sanctions) pour l'amener à divulguer des informations sensibles. Celles-ci serviront ensuite à compromettre davantage les systèmes et accéder à des données.

Analyse des vulnérabilités : basée sur un processus informatique légitime, l'analyse des problèmes aide les équipes à identifier les problèmes existants afin de les résoudre avant qu'ils ne provoquent un incident de sécurité. Les acteurs malveillants ont accès aux mêmes outils et les emploient pour repérer les appareils vulnérables, puis attaquer leur point faible.

Détournement de communications : les logiciels de visioconférence et de communication populaires, tels que Teams et Zoom, peuvent être la cible d'attaques. Profitant de défauts de configuration dans les salles, des attaquants extérieurs perturbent les communications, compromettent le secret des conversations, mettent en danger le bien-être des étudiants et peuvent même exposer des informations sensibles.

Menaces internes

Soyons clairs, toutes les menaces externes énumérées ci-dessus peuvent aussi venir de l'intérieur. Les deux ne s'excluent pas mutuellement, mais le facteur décisif est l'origine de la menace : un utilisateur interne ou une entité externe inconnue. Cela dit, voici une liste de menaces internes affectant couramment les établissements primaires et secondaires :

Ingénierie sociale : nous l'avons abordée dans la section consacrée à l'hameçonnage, mais elle mérite une mention supplémentaire car elle ouvre souvent la voie à des attaques fructueuses. Pensez-y par exemple quand vous tenez la porte à quelqu'un dans une entrée sécurisée. Le geste est gentil mais peut permettre à des personnes non autorisées d'entrer dans des zones réservées.

Mots de passe faibles : plus un mot de passe est facile à retenir, plus il est facile à deviner. Ce phénomène, avec le vol d'identifiants ci-dessous, constituent deux scénarios de menace totalement évitables.

Vol d'identifiants : les mots de passe sont de plus en plus complexes et nous en utilisons un nombre impressionnant tant dans la vie personnelle que professionnelle. On peut avoir envie de les noter, par exemple sur un post-it collé derrière le clavier ou l'écran. Cela peut sembler ridicule, mais c'est une menace sérieuse pour la sécurité des utilisateurs et de leurs données.

Appareils non mis à jour : tous les appareils et applications nécessitent des mises à jour fréquentes pour corriger les bugs et les vulnérabilités. Sans ces correctifs, les appareils sont exposés aux menaces internes et externes. Les vulnérabilités facilitent en effet le contournement des protections intégrées, la collecte de données sensibles et la découverte des ressources connectées.

Vol/exfiltration de données : la clé USB permet de stocker et de déplacer des données d'un appareil à l'autre, ce qui est utile lorsque vous emportez du travail à la maison. Mais cet objet anodin peut servir un objectif plus néfaste : déplacer des données d'un emplacement sécurisé vers un autre potentiellement non sécurisé, ou extraire des documents confidentiels.

Réglages mal configurés : les réglages informatiques ressemblent beaucoup aux préférences, nous en avons tous et ils peuvent différer d'une personne à l'autre. Mais certains d'entre eux doivent être définis d'une façon précise pour sécuriser les appareils et éviter des problèmes potentiels. On peut, par exemple, désactiver la fonction de stockage des identifiants d'un navigateur web, pour empêcher qu'une personne accède à vos données sensibles simplement en utilisant votre ordinateur.

Suppression de la protection des terminaux : cette opération est devenue de plus en plus délicate au fil des ans, mais elle reste possible. Les utilisateurs invoquent souvent une baisse des performances pour justifier la suppression du logiciel chargé de protéger leur appareil contre les menaces.

Informatique de l'ombre : comme nous l'avons vu précédemment, l'informatique de l'ombre vise à résoudre un problème mais en laisse souvent d'autres dans son sillage.

Vous vous demandez peut-être en quoi c'est essentiel à la réussite des élèves, en quoi cela affecte leurs performances ? La cybersécurité a un impact à la fois direct et indirect sur la capacité des parties prenantes à apprendre et à travailler.

La fracture numérique

Selon la démographie de la région concernée, le nombre d'élèves sans accès haut-débit fiable à Internet à domicile peut varier par rapport à la moyenne de 40 %, comme l'indique une enquête de l'Institut des politiques publiques de Californie (PPIC). Un certain nombre d'initiatives locales, étatiques et fédérales ont été lancées ces dernières années pour confier davantage d'appareils aux enseignants et aux élèves. Pourtant, la fracture numérique reste une préoccupation bien réelle pour de nombreux districts scolaires. C'est d'autant plus crucial si ces appareils et l'accès à Internet par les points d'accès mobiles sont les seuls moyens dont ils disposent pour bénéficier de l'apprentissage à distance ou faire leurs devoirs à la maison.

Absence d'accès aux appareils ou aux ressources.

En d'autres termes, si un appareil est inaccessible en raison d'un problème technique, s'il est au service informatique en cours de triage ou s'il attend l'intervention d'un prestataire tiers, un enseignant ou un élève est privé de son outil. Il en va de même pour les logiciels ou les services indisponibles. Ils représentent en effet autant d'occasions perdues d'apprendre et d'enseigner.

Financement lié aux progrès et aux résultats des élèves

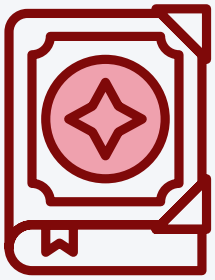
À l'instar de la fracture numérique mentionnée plus haut, la question de l'influence des résultats des examens et des progrès des élèves sur le montant des fonds reçus peut varier d'un district à l'autre. Elle peut d'ailleurs dépendre largement des caractéristiques démographiques de votre région.

- Primes et promotions pour les enseignants et les administrateurs
- Primes ponctuelles pour les enseignants
- Augmentation du financement des écoles ou des programmes scolaires
- Accès à certaines subventions ou autres formes de financement
- Les écoles peu performantes peuvent être tenues de proposer un tutorat
- Les enseignants et les administrateurs des écoles peu performantes peuvent être remplacés

Sécurité en ligne des élèves

Nous sommes tous d'accord pour dire que la sécurité des élèves et du personnel est d'une importance capitale dans les établissements d'enseignement primaire et secondaire. La technologie occupe une part croissante dans notre vie quotidienne, les menaces de sécurité se font plus pressantes, et les attaques de cybersécurité cible de plus en plus le secteur de l'éducation. Soyons clairs : l'époque où il suffisait d'installer un logiciel antivirus sur un appareil est révolue.

On connaît les menaces des logiciels malveillants et les attaques visant les apps et les services. Mais les acteurs malveillants cherchent également à infiltrer les réseaux pour obtenir des dossiers d'étudiants et les vendre sur le Dark Web. Pire encore, l'absence de contrôles de sécurité appropriés peut mettre en danger le bien-être des parties prenantes, qui peuvent être espionnées à leur insu : capture du flux des caméras, écoute des micros et suivi de la localisation. Des malfaiteurs peuvent même usurper l'identité d'un proche pour commettre des crimes plus graves. Sensibiliser les élèves à l'importance de la sécurité en ligne, tout en les guidant dans l'apprentissage des compétences nécessaires pour identifier eux-mêmes les menaces, est la clé d'un cursus robuste de sécurité informatique.



Adressez-vous au ministère

Dans le monde magique de Harry Potter, le ministère de la Magie est le gardien de l'information et de tout ce qui touche à la magie. Dans l'enseignement primaire et secondaire, vous pouvez compter sur Jamf. Nous sommes là pour faire la lumière sur les informations erronées et vous aider à établir les pratiques de sécurité les mieux adaptées à vos besoins. Bien entendu, nous vous accompagnons tout au long de la mise en œuvre de ces pratiques.

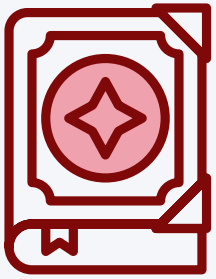
Avant de poursuivre, prenons un moment pour aborder certaines des idées fausses les plus répandues au sujet de la sécurité Apple, mais aussi du rôle de la cybersécurité dans l'enseignement primaire et secondaire.

Apple n'est pas touché par les virus : cela n'a jamais été tout à fait vrai, mais les Mac n'étaient tout simplement pas aussi populaires. Les acteurs malveillants se sont donc concentrés sur Windows, dont la part de marché était plus importante. Ces dernières années, la situation a radicalement changé et la croissance fulgurante d'Apple a fait de ses machines des cibles de choix.

L'éducation est très ciblée : vrai. En fait, selon un rapport de Bitdefender, les établissements d'enseignement primaire et secondaire représentent la deuxième cible la plus importante des rançongiciels, juste derrière le commerce de détail. Les logiciels malveillants ne représentent qu'un seul type de menace, mais ils comptent parmi les plus dangereux.

L'éducation est faible sur le plan de la sécurité : c'est en tout cas la perception qu'en ont les analyses et les rapports sur les menaces, comme celui de Security Scorecard, qui révèle que « sur 17 secteurs aux États-Unis, l'éducation arrive en dernière position en termes de cybersécurité totale ». Plus précisément, le rapport indique que la fréquence des correctifs et la sécurité des applications et des réseaux figurent parmi les points sensibles les plus préoccupants.

La sécurité est difficile et coûteuse : il y a une pénurie de professionnels de la cybersécurité, c'est bien connu. Cela s'explique en partie par la difficulté de la tâche. Cela dit, il est primordial de connaître votre environnement, d'évaluer vos besoins et de travailler avec des partenaires fiables pour répondre à ces préoccupations et réussir un programme de cybersécurité. Écouter le battage médiatique sans explorer les solutions ne peut conduire qu'au désastre. Il est donc difficile de trouver la voie à suivre, et cela peut coûter cher. Pour autant, il ne faut pas baisser les bras. Vous exposeriez en effet votre district à des menaces, et gérer les conséquences d'une violation de données et les pénalités de conformité a un impact financier élevé.



Adressez-vous au ministère

> « Les pirates n'ont besoin de réussir qu'une fois ; nous devons réussir à chaque fois. »
>
> – Chris Triolo, professionnel de la sécurité chez HP.

Solutions « taille unique » : le mythe de la solution « taille unique » va de pair avec celui de la difficulté et du coût. Bien sûr, un même fournisseur peut développer plusieurs solutions qui fonctionnent ensemble pour faire face à de nombreuses malveillances. Nous parlons ici d'un produit unique qui prétend traiter tous les aspects de la menace. Historiquement, les produits de ce type ont failli à plusieurs de leurs missions – et la cybersécurité ne peut se le permettre.

C'est un problème d'informatique : ce point de vue générique est partagé par beaucoup, mais il est important pour le débat sur l'enseignement primaire et secondaire. Cernés par les problèmes de budget et de temps, les parties prenantes ont souvent l'impression que les fonctions de chaque rôle sont clairement délimitées. En vérité, la sécurité – comme la pollution – est l'affaire de tous, et il faut les efforts de toutes les parties prenantes pour la maintenir. Pensez à l'analogie classique de la chaîne, dont la solidité dépend de son maillon le plus faible.

Ne vous préoccupez pas de sécurité tant qu'on ne vous pirate pas : cette politique de l'autruche est déconnectée de la réalité. Toutes les institutions, à un moment de leur histoire, peuvent se vanter de n'avoir connu aucune faille de sécurité. Jusqu'à la première. En étant proactif plutôt que réactif, les districts peuvent surveiller les menaces, détecter les points préoccupants et y remédier afin d'éviter que les menaces ne se concrétisent de façon dramatique.

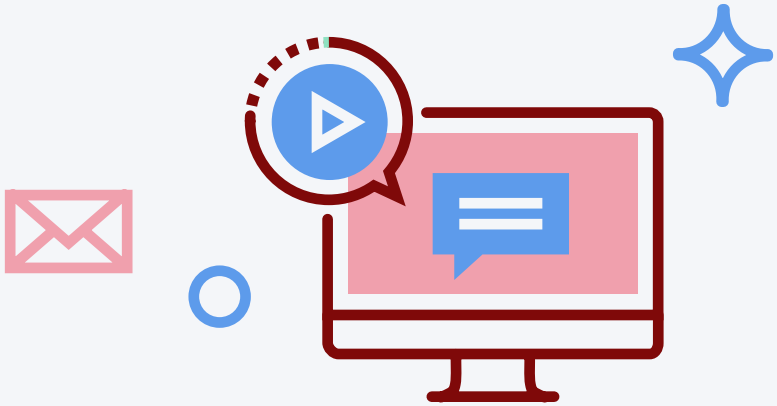
Jamf + Apple

Élaborée en étroite collaboration avec Apple, chaque solution est conçue non seulement pour protéger vos appareils, vos utilisateurs et vos données, mais aussi pour utiliser le moins de ressources possible. L'objectif : assurer un fonctionnement transparent dans le cadre de l'expérience utilisateur qui fait la réputation des produits Apple.

Ensemble, nous fusionnons les services et les équipements fournis par Apple avec les solutions Jamf qui répondent aux besoins spécifiques du secteur de l'enseignement primaire et secondaire. Les élèves et les enseignants sont autonomisés, ce qui favorise une utilisation innovante et créative de la technologie. Les équipes informatiques et de sécurité, quant à elles, savent que les risques et les menaces sont atténué par des solutions spécialisées dans la gestion des appareils, le provisionnement des identités et l'authentification, ainsi que la protection des terminaux en arrière-plan.

Apple School Manager (ASM)

Initiez le processus de gestion des terminaux à l'aide de cette console cloud centralisée, aussi puissante que facile à utiliser. Fourni gratuitement par Apple, ce service synchronise les achats effectués avec la console en ligne et permet à l'informatique d'établir une connectivité avec le logiciel de gestion des appareils mobiles (MDM) du district, ce qui facilite l'enrôlement automatique des appareils .



Jamf School

La solution EDU phare, conçue pour gérer tous les appareils de l'écosystème Apple, est exclusivement destinée aux enseignants, aux techniciens pédagogiques et aux administrateurs Mac du secteur de l'éducation. La solution MDM de Jamf School autonomise plus de 36 millions d'élèves dans le monde. Grâce à elle, les enseignants bénéficient d'une fonctionnalité de gestion de classe, sélectionnent des applications, des contenus de cours et des restrictions, et déploient facilement des identifiants Apple gérés sans avoir besoin d'être expert – technique ou autre. De plus, le système intégré de gestion des incidents permet de suivre les problèmes signalés, comme les appareils hors garantie : un atout de poids pour la réussite de la stratégie de cybersécurité.

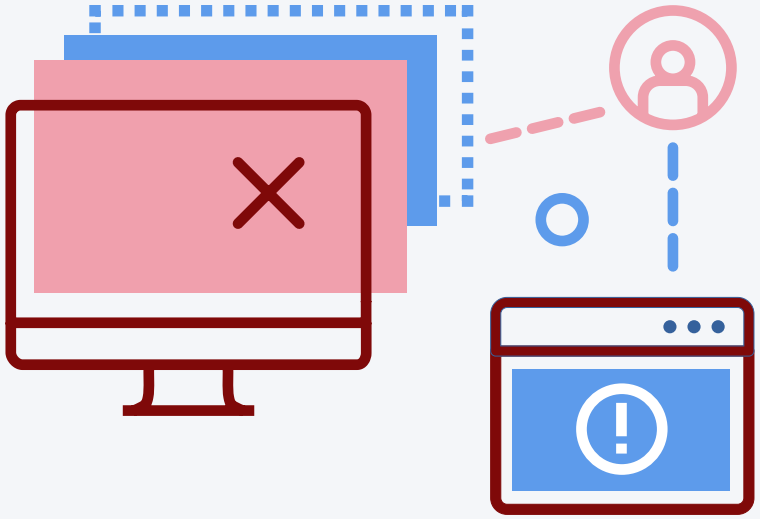
En savoir plus

Jamf Pro

La solution MDM de référence pour les organisations qui ont besoin d'une plateforme MDM avec des fonctionnalités et des modèles de prise en charge avancés. Aux fonctionnalités de Jamf School, Jamf Pro ajoute l'automatisation et une intégration robuste avec d'autres produits de votre pile de gestion de réseau et de systèmes. Son accès par API, notamment, permet de sécuriser les communications entre les applications et les services.
Des fonctionnalités très techniques fournissent par ailleurs aux équipes informatiques dédiées la puissance supplémentaire requise pour gérer plusieurs écoles ou un district scolaire entier.

En savoir plus

Jamf Connect



Reposant sur une gestion des comptes centralisée et basée sur le cloud, Jamf Connect est le pivot qui permet d'approvisionner des comptes pour que les utilisateurs puissent s'authentifier sur leur Mac. Jamf Connect leur permet de le faire avec un seul compte : plus besoin de mémoriser plusieurs mots de passe. La solution met en effet en place une véritable authentification unique (SSO) pour accéder à l'ensemble des applications et services assignés, et peut accueillir l'authentification multifacteur (MFA) qui ajoute une deuxième couche de protection.

En savoir plus

Jamf Protect

Jamf Protect met exclusivement l'accent sur la sécurité Apple. Cet outil aide les équipes de sécurité à bloquer les logiciels malveillants connus, à détecter les menaces et à utiliser l'analyse comportementale pour identifier les risques pesant sur la santé de vos appareils. En outre, Jamf Protect est doté d'alertes et d'une journalisation en temps réel offrant une visibilité granulaire sur les terminaux. Pour vous, c'est l'assurance d'atteindre vos objectifs de conformité réglementaire. Et pour l'informatique, la possibilité de corriger les problèmes et d'aider les utilisateurs sans les gêner.

En savoir plus

Faites passer votre technologie éducative au niveau supérieur

jamf

Vous souhaitez plus d'informations sur les atouts de Jamf ou vous avez des questions sur le déploiement de ces outils dans votre propre établissement ? Commencez un essai gratuit pour vous lancer.

Demander une version d'essai

Ou contactez votre revendeur habituel de matériel Apple.