RENFORCER LA SÉCURITÉ DANS LES ENVIRONNEMENTS D'APPRENTISSAGE ACTIF

Dossier Intel® pour l'éducation

Alors que la troisième décennie du 21e siècle se profile à l'horizon, il semble évident que les élèves apprennent mieux lorsqu'ils s'engagent activement dans l'apprentissage. Si cet engagement prend diverses formes selon le niveau scolaire, la matière, les compétences de l'enseignant et les objectifs pédagogiques, on observe dans la majorité des classes que la technologie est de plus en plus utilisée quand l'élève est indépendant et n'a plus besoin de la surveillance directe de l'enseignant.

Les risques pour la sécurité des élèves augmentent à chaque étape menant à l'indépendance vis-à-vis de la salle de classe. En septembre 2018, le FBI mettait en garde : « L'utilisation malveillante de ces données sensibles pourrait mener à des attaques d'ingénierie sociale, au harcèlement, à l'usurpation d'identité ou à d'autres moyens permettant de cibler les enfants. »

Bien entendu, l'absence de surveillance seule n'explique pas les problèmes de sécurité. Quand les élèves apprennent et collaborent en dehors de la classe, ils utilisent des ordinateurs et des serveurs qui ne sont peut-être pas suffisamment protégés contre les chevaux de Troie, les virus, les rançongiciels et d'autres types de logiciels malveillants, ainsi que des appareils publics sur lesquels leurs informations peuvent être récupérées par des intrus à proximité.

Enfin, plus le nombre d'élèves devant collaborer avec d'autres élèves et membres de la communauté augmente, plus le risque de cyberharcèlement (c'est-à-dire l'envoi ou la publication de textes ou d'images dans l'intention de blesser ou d'embarrasser une autre personne) est important. Comme les sites sur lesquels les élèves collaborent ne sont pas nécessairement sûrs, le harcèlement peut provenir d'une personne qui se fait passer pour un collaborateur.

Certaines menaces pour la sécurité sont atténuées quand les élèves utilisent les ordinateurs à l'école. Les sites malveillants et non protégés sont généralement filtrés par les serveurs de l'école et de nombreux établissements consignent les sites visités.

« L'utilisation malveillante de ces données sensibles pourrait mener à des attaques d'ingénierie sociale, au harcèlement, à l'usurpation d'identité ou à d'autres moyens permettant de cibler les enfants. »

U.S. FEDERAL BUREAU OF INVESTIGATION, 2018

OFFRIR UN EXPÉRIENCE PÉDAGOGIQUE PLUS SÛRE

Avantages pour les administrateurs

- Puissants PC avec processeur Intel® Core™ pour protéger l'investissement dans les années à venir.
- Enseignement et apprentissage de compétences et de pratiques du monde réel dans un environnement sûr et administré.

Avantages pour les enseignants

- Engagement plus sûr des élèves dans un apprentissage actif sur Internet.
- Chaque élève accède aux mêmes ressources pour les projets.

Avantages pour les élèves

- Utilisation de ressources Internet sans crainte d'usurpation d'identité, de cyberharcèlement, etc.
- Collaboration avec d' autres élèves et leurs enseignants.
- Accès aux ressources adaptées aux projets.

SOLUTION ADAPTÉE À L'ENSEIGNEMENT ET À L'APPRENTISSAGE

Qu'il s'agisse d'un déploiement à grande échelle ou d'un modèle impliquant des appareils partagés, chaque élève a besoin d'un ordinateur équipé d'un matériel et de logiciels qui le protègent quand il est connecté à Internet, qu'il passe ou pas par le serveur de l'école. Comme les pédagogies d'apprentissage actif impliquent diverses ressources en ligne, les ordinateurs doivent disposer de plusieurs outils pour protéger les élèves.

Authentification matérielle à deux facteurs

L'utilisation sûre d'Internet commence par s'assurer que seuls les élèves et le personnel autorisé ont accès aux comptes des élèves. Cette stratégie protège contre l'usurpation d'identité.

Protection antivirus

Une deuxième défense inclut l'installation d'un logiciel antivirus qui utilise la technologie Intel® Threat Detection. En plus des appareils des élèves, cette solution protège le système informatique de l'école.

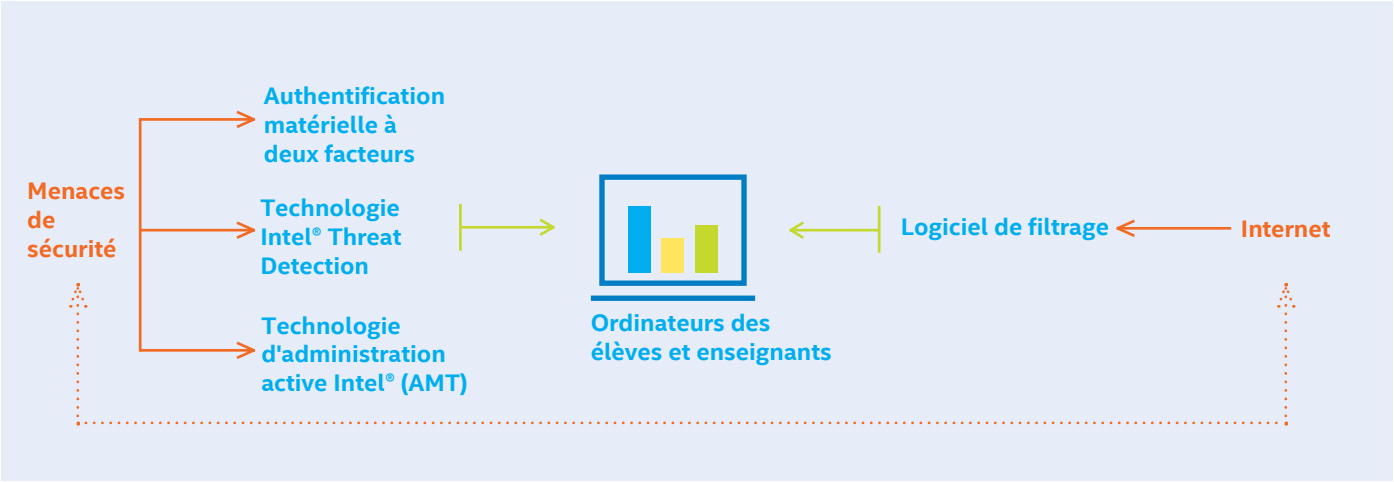
Filtrage Internet

Le trafic Internet est filtré pour que seuls les sites approuvés par l'établissement soient accessibles.

EXEMPLES DE CAS D'USAGE

- Dans une classe inversée, l'enseignement direct a le plus souvent lieu en dehors de la classe à l'aide de vidéos, de sites Web et d'autres sources en ligne.
- Dans l'apprentissage par projet, les élèves effectuent généralement des recherches indépendantes à l'aide de moteurs de recherche et travaillent avec les membres de leur équipe en collaboration sur des rapports, des plans et des tâches.
- Quand un élève crée un support, il utilise des outils en ligne et publie ses réalisations dans des collections en ligne.

FONCTIONNEMENT DE LA SÉCURITÉ MATÉRIELLE



« La protection des données des élèves commence avec les enseignants et les administrateurs... elle dépend aussi de pratiques, stratégies et technologies robustes. »

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES DE L'UE

Pour en savoir plus sur la nouvelle génération d'appareils pour l'éducation, prenez contact avec votre responsable de compte Intel ou rendez-vous sur www.intel.fr/education.