

Priorité à la résilience et à la sécurité

Solutions Alcatel-Lucent pour le secteur de l'éducation

Alcatel·Lucent



Sommaire

Présentation

Collaboration TI/TO dans les environnements éducatifs

Solutions réseau résilientes et sécurisées

Solutions de communication résilientes et sécurisées

Protéger les personnes et les actifs

Souveraineté et sécurité des données



Présentation

Face à la multiplication des défis mondiaux, des cyberrisques et des risques physiques, les responsables des campus doivent accorder la priorité à la résilience, à la gestion des risques et à la durabilité. Les menaces cybernétiques et physiques se multiplient, et les établissements d'enseignement sont confrontés à des attentes de plus en plus fortes pour maintenir leurs services opérationnels, protéger les données sensibles et garantir la sécurité des étudiants et du personnel.

Selon l'enquête sur les failles de cybersécurité 2025/26 menée par le gouvernement britannique, 98 % des établissements d'enseignement supérieur ont déclaré avoir subi une faille ou une cyberattaque au cours des 12 derniers mois, et 27 % ont indiqué que de tels incidents se produisaient presque chaque semaine.[1] Dans ce contexte, la protection des infrastructures numériques et physiques n'est pas un luxe, mais une nécessité.

Pourquoi les TIC sont plus essentielles que jamais dans l'enseignement

L'enseignement a connu une profonde transformation numérique, les universités proposant désormais un apprentissage hybride, un accès à distance aux laboratoires et des examens en ligne. Les étudiants s'attendent à des expériences numériques accessibles en tout temps, fluides et sécurisées. Les enseignants et le personnel travaillent et collaborent de plus en plus à distance et depuis différents lieux. Parallèlement, les universités doivent protéger d'énormes volumes d'informations sensibles, des données de recherche aux dossiers personnels.

Alcatel-Lucent accompagne les établissements d'enseignement du monde entier, conscient de l'importance de sécuriser les personnes, les données, les environnements d'apprentissage et les opérations. Nos solutions sont conçues dans un souci de résilience et de confidentialité, des salles de classe aux laboratoires de recherche, en passant par les résidences universitaires et les services de sécurité des campus. Ce livre numérique présente les principales mesures permettant de renforcer la résilience et la sécurité de vos solutions Alcatel-Lucent de communication, de cloud et de réseau.

1 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-education-institutions-findings - Gov.uk, avril 2026

Collaboration entre les technologies de l'information (TI) et les technologies opérationnelles (TO) dans les environnements éducatifs

Avant d'examiner comment Alcatel-Lucent peut renforcer votre résilience et votre sécurité, il est important de comprendre comment la relation entre les technologies de l'information (TI) et les technologies opérationnelles (TO) évolue au sein des campus. Ces deux domaines ne peuvent plus fonctionner en silos. La collaboration est essentielle pour protéger et optimiser les outils numériques qui assurent le bon fonctionnement des campus, des systèmes de chauffage, de ventilation et de climatisation (CVC) et de l'éclairage aux tableaux interactifs et aux équipements de laboratoire connectés à l'Internet des objets (IoT).

Prenons l'exemple de l'Internet des objets (IoT) : si les équipes chargées des installations déploient un éclairage intelligent ou des capteurs de présence sans l'implication du service informatique, ces appareils peuvent rapidement présenter des risques pour la sécurité. Beaucoup d'entre eux disposent de mesures de protection faibles ou incohérentes, et l'informatique fantôme, ou l'utilisation de technologies non autorisées, sur un campus intelligent peut ouvrir la porte à des logiciels malveillants, à des vulnérabilités réseau, voire à des fuites de dossiers académiques sensibles.

En travaillant ensemble, les équipes TI et TO acquièrent la visibilité et le contrôle dont elles ont besoin pour garantir la conformité, renforcer la résilience et créer une base sécurisée pour l'innovation sur l'ensemble du campus.



Des solutions réseau résilientes et sécurisées

Le réseau du campus est l'épine dorsale de tous les services numériques, des examens et cours en ligne à l'accès aux bases de données de recherche, en passant par les systèmes d'alerte d'urgence. Une panne de réseau pourrait perturber la vie de milliers d'étudiants et d'enseignants, nuire à la réputation de l'établissement ou compromettre l'intégrité de la recherche.

Les solutions «Digital Age Networking» d'Alcatel-Lucent sont conçues autour de la résilience. De l'architecture sécurisée dès la conception à la segmentation intégrée et au contrôle d'accès, nos réseaux sont renforcés pour résister aux perturbations. Nous offrons une visibilité à l'échelle du campus, une intégration automatisée des appareils de confiance et une gestion simplifiée, le tout sans coûts cachés ni licences supplémentaires.

7 bonnes pratiques pour vos solutions réseau

Des cours en ligne et projets de recherche aux capteurs IoT dans les salles de classe connectées, les temps d'arrêt ou les failles de sécurité affectent directement l'enseignement, l'apprentissage et la confiance des étudiants. Vous trouverez ci-dessous sept bonnes pratiques que les universités et les établissements scolaires peuvent adopter pour améliorer la résilience et la sécurité de leurs environnements TI et TO.

1. Maintenez vos systèmes à jour grâce à la gestion du cycle de vie en faisant régulièrement le point avec vos fournisseurs de technologies afin de vous assurer que les dernières versions logicielles, les correctifs de sécurité et les améliorations sont bien appliqués. Utilisez des outils de gestion du cycle de vie tels qu'Alcatel-Lucent ProActive Lifecycle Management (PALM) pour suivre l'obsolescence et les étapes de fin de vie, afin de pouvoir budgétiser et planifier le remplacement du matériel avant que cela ne devienne urgent.
2. Renforcez la sécurité des commutateurs au niveau du code, en protégeant votre infrastructure grâce à un système d'exploitation réseau renforcé. La technologie Secure Diversified Code d'Alcatel-Lucent répartit aléatoirement l'allocation de la mémoire afin de réduire les risques d'exploitation de failles. La vérification et la validation indépendantes (IVV) réalisées par des experts tiers ajoutent un niveau de confiance supplémentaire en identifiant et en éliminant les vulnérabilités potentielles avant qu'elles n'atteignent l'environnement de production.
3. Appliquez une stratégie de sécurité fondée sur le principe de confiance zéro (Zero Trust) à votre réseau de campus en mettant en œuvre une macro- et une micro-segmentation afin d'isoler les systèmes sensibles (tels que les dossiers des étudiants et les laboratoires de recherche) du trafic général. Adoptez une approche par étapes (surveillance, validation, planification, simulation et mise en œuvre) pour éviter les perturbations tout en améliorant la résilience.
4. Intégrez une redondance grâce au protocole Shortest Path Bridging afin d'assurer un basculement rapide et un réacheminement dynamique du trafic en cas de défaillance d'une liaison ou d'un périphérique. Cela permet de créer un réseau efficace avec une segmentation automatisée, tout en réduisant la complexité liée à la gestion de multiples réseaux locaux virtuels (VLAN) — un avantage important lors de la mise à l'échelle sur de grands campus.
5. Utilisez les capacités de châssis virtuel pour renforcer la fiabilité dans les zones critiques. Cela permet des mises à jour logicielles à chaud (ISSU) sans temps d'arrêt, prend en charge les topologies en anneau ou en maillage et simplifie la gestion en présentant plusieurs équipements comme une seule unité logique — tout en maintenant des coûts prévisibles.
6. Automatisez la sauvegarde et la restauration à l'aide d'outils de gestion de réseau tels que le système de gestion de réseau OmniVista® d'Alcatel-Lucent. OmniVista Resource Manager simplifie les sauvegardes de configuration, l'application des politiques et les processus de restauration. L'automatisation des tâches liées au cycle de vie garantit une reprise plus rapide en cas de pannes ou d'erreurs de configuration, ce qui allège la charge de travail des petites équipes informatiques dans les établissements scolaires et universitaires.
7. Assurez la redondance des routeurs en mettant en œuvre le protocole VRRP (Virtual Router Redundancy Protocol) afin de garantir un basculement transparent entre les routeurs. Cela permet d'éliminer les points uniques de défaillance et d'assurer un accès continu aux applications essentielles, comme les plateformes de gestion de l'apprentissage, les outils de collaboration et les systèmes d'alerte d'urgence.



Investissez dans des solutions réseau résilientes et sécurisées

Investir dans la résilience et la sécurité de votre réseau est essentiel. Cependant, déterminer où investir au mieux peut s'avérer complexe et prendre du temps : la planification est donc essentielle. Avant de vous lancer, voici quelques points clés à prendre en compte pour vous assurer d'obtenir le niveau de sécurité et de résilience dont votre organisation a besoin :

- En collaboration avec votre partenaire d'affaires, passez en revue et mettez à jour la conception de votre réseau afin de vous assurer que les besoins de votre établissement y sont pris en compte, notamment en termes de niveau de résilience adapté aux zones sensibles et critiques qui ont un impact sur les services essentiels du campus. Pour les zones critiques, envisagez d'ajouter des serveurs de secours et des connexions multiples lorsque cela est possible et pertinent.
- Améliorez la réponse aux incidents grâce aux capacités d'intelligence artificielle (IA) et d'apprentissage automatique (ML) offertes par Alcatel-Lucent OmniVista Network Advisor. Cet outil aide à détecter et à résoudre les problèmes avant qu'ils n'affectent les utilisateurs finaux, en identifiant et en traitant de manière proactive les problèmes de réseau ou de sécurité. Il accélère le dépannage et renforce la sécurité du réseau grâce à des audits de configuration et à la gestion en temps réel des alertes concernant tout changement soudain dans le comportement du réseau.
- Envisagez l'utilisation de commutateurs renforcés pour les environnements difficiles. La gamme de commutateurs Ethernet renforcés d'Alcatel-Lucent est spécialement conçue pour exceller dans des environnements exigeants et à des températures extrêmes.

  Ces commutateurs sont construits à partir de composants renforcés et logés dans des boîtiers robustes, garantissant ainsi durabilité et fiabilité, et disposent du même système d'exploitation que les autres commutateurs Alcatel-Lucent. Pour renforcer la sécurité et protéger les informations sensibles, certains modèles sont équipés d'alertes d'intrusion et de relais d'alarme permettant la connexion de systèmes d'alarme externes. Certains modèles prennent même en charge le protocole MACsec (Media Access Control and Security) pour des communications de données sécurisées. Grâce à la fonctionnalité de châssis virtuel intégrée aux commutateurs renforcés, vous bénéficiez d'une redondance, d'une résilience et d'une évolutivité accrues.
- Proposez une formation technique Alcatel-Lucent à l'équipe d'exploitation du réseau afin de l'aider à détecter les problèmes et à y réagir rapidement

Solutions de communication résilientes et sécurisées

Les communications sont essentielles pour permettre aux établissements d'enseignement d'interagir avec les étudiants, le personnel et d'autres institutions, ainsi que pour diffuser des informations importantes. Les systèmes de communication doivent rester disponibles en cas de crise, lorsque les étudiants et le personnel ont le plus besoin de l'aide du campus. La résilience et la sécurité sont des domaines en constante évolution, et des révisions régulières contribueront à garantir la sécurité et la disponibilité de votre solution de communication Alcatel-Lucent.

Les solutions de communication Alcatel-Lucent sont sécurisées dès leur conception. Cela signifie que nous prenons en compte la sécurité à chaque étape de la définition, du développement et de la livraison des produits. L'ensemble du matériel et des systèmes d'exploitation est renforcé, et une protection contre les attaques par déni de service (DoS) est intégrée. Nous respectons les certifications et accréditations reconnues en matière de normes mondiales de sécurité et de confidentialité (ISO 27001, ISO 27017 et ISO 27018). Nous respectons également les normes de sécurité et de confidentialité spécifiques à certains secteurs, telles que la loi HIPAA (Health Insurance Portability and Accountability Act) aux États-Unis et la norme HDS (Hébergeurs de Données de Santé) pour l'hébergement des données de santé en France, ainsi que les normes régionales en matière de sécurité et de confidentialité, comme le Règlement général sur la protection des données (RGPD) dans l'Union européenne.

7 bonnes pratiques pour vos solutions de communication

Voici sept bonnes pratiques pour vous assurer d'optimiser pleinement la résilience et la sécurité de vos solutions de communication Alcatel-Lucent.

1. Vérifiez régulièrement l'état du système avec votre partenaire d'affaires afin de vous assurer que la dernière version des logiciels, des correctifs et des mises à jour de sécurité est installée et que votre contrat SPS est à jour.
2. Vérifiez régulièrement les composants liés à la sécurité et à la continuité de service dans votre système de gestion de réseau Alcatel-Lucent OmniVista 8770, qui comprend des informations et des fonctionnalités précieuses en matière de résilience et de sécurité pour votre solution de communication
   - Envisagez la sauvegarde automatisée à distance du système pour éviter toute perte de données de configuration
   - Configurez la surveillance des alarmes et assurez-vous qu'elle est régulièrement mise à jour avec les seuils appropriés. De plus, vérifiez que les notifications en cas de défaillance du système de communication ou les alertes de qualité sont bien transmises aux personnes concernées.
3. Passez en revue et appliquez une politique de mots de passe rigoureuse, de préférence au moyen d'une authentification externe, comme un serveur RADIUS, et mettez en place des rappels à l'intention des utilisateurs afin de prévenir la fraude téléphonique, qui demeure une menace dans de nombreux pays.
4. Formez les employés et assurez-vous qu'ils connaissent les risques et les mesures de prévention.
5. Vérifiez l'état, la pertinence et la facilité de maintenance des serveurs hébergeant des applications essentielles aux activités.
6. Envisagez la mise en place d'un VLAN dédié à la voix. La séparation du trafic vocal des autres types de trafic réduit le risque de contamination, susceptible de perturber les opérations et, potentiellement, les services du campus.
7. Assurez-vous que vos contrôleurs de frontière de session (SBC) sont correctement configurés. Les exigences ont pu évoluer au fil du temps.



Investissez dans des solutions de communication résilientes et sécurisées

Les campus modernes ont besoin de systèmes de communication disponibles en permanence, que ce soit pour l'enseignement, la recherche ou les alertes d'urgence. Alors que les établissements planifient des solutions de nouvelle génération, voici les domaines clés à privilégier :

- Déployez des serveurs d'appels et des services applicatifs redondants dans les lieux critiques tels que les infirmeries, les résidences universitaires et les centres de recherche. La redondance garantit la disponibilité des communications même en cas de défaillance d'un système, préservant ainsi le bien-être des étudiants et la continuité des opérations.
- Veillez à ce que la couverture DECT (Digital Enhanced Cordless Telecommunications) ou Wi-Fi couvre non seulement les salles de classe, mais aussi les zones sensibles et difficiles d'accès telles que les laboratoires, les centres de données et les espaces extérieurs. Une couverture complète facilite à la fois l'apprentissage quotidien et les communications d'urgence.
- Utilisez des outils tels que Visual Notification Assistant d'Alcatel-Lucent ou Rainbow™ pour créer des flux de travail avec des déclencheurs automatiques, qu'ils proviennent de personnes, d'appareils IoT ou de systèmes. Cela garantit que le personnel clé est immédiatement averti en cas de problème, ce qui permet une intervention et une reprise plus rapides.
- Déployez Rainbow™ d'Alcatel-Lucent, l'outil collaboratif idéal pour compléter les solutions de communication d'Alcatel-Lucent. Rainbow offre des fonctionnalités sécurisées de voix, de vidéo, de messagerie et de partage de fichiers, prenant en charge l'enseignement hybride, la mobilité du corps enseignant et la collaboration à distance. Son architecture hybride, dans le cloud et sur site, contribue à la résilience en permettant aux communications de rester disponibles à partir de différents emplacements, même en cas de perturbation locale. Des fonctionnalités telles que le partage d'images et de vidéos, y compris les flux de vidéo-surveillance, améliorent la connaissance de la situation tant pour les besoins académiques que pour les questions de sécurité.
- Pour les établissements soumis à des exigences strictes en matière de gouvernance des données, Rainbow Edge peut être déployé dans un cloud privé ou régional, garantissant ainsi le respect des politiques académiques ou nationales en matière de données tout en offrant des fonctionnalités de collaboration modernes.
- Alcatel-Lucent propose des solutions flexibles pour l'enseignement à distance, la mobilité des enseignants et les configurations hybrides du personnel, afin de prendre en charge la voix, la vidéo et la collaboration en toute sécurité, où que l'on se trouve, notamment :
  - Rainbow pour la collaboration dans le cloud
  - Softphone IP de bureau / Softphone pour le personnel à distance ou en mode hybride
  - DeskPhone avec VPN intégré pouvant être déployé en masse pour des déploiements sécurisés à grande échelle.



Protéger les personnes et les actifs

Un campus intelligent ne se résume pas à une connexion Internet haut débit : il s'agit d'un environnement connecté où la technologie protège activement les étudiants, le personnel et les ressources essentielles. En intégrant les communications, l'Internet des objets (IoT) et l'analyse de données, les universités et les établissements scolaires peuvent aller au-delà d'une approche réactive et instaurer une culture de la sécurité proactive.

Les informations en temps réel jouent un rôle central. Les alarmes incendie, les détecteurs de mouvement, les systèmes de contrôle d'accès ou l'analyse vidéo basée sur l'IA peuvent déclencher automatiquement des alertes destinées aux équipes de sécurité ou aux responsables des installations, ce qui réduit les délais d'intervention et empêche les incidents mineurs de s'aggraver. Au lieu d'attendre que les problèmes soient signalés, les établissements peuvent anticiper les risques et agir immédiatement, qu'il s'agisse de verrouiller un bâtiment, d'envoyer une équipe de maintenance réparer un système de chauffage, de ventilation et de climatisation défaillant ou d'intervenir en cas d'activité suspecte.

La véritable valeur ajoutée se révèle lorsque les données, les flux de travail et les communications sont intégrés. Des outils tels que Rainbow et Visual Notification Assistant permettent de relier les personnes, les systèmes et les appareils IoT au sein de flux de travail automatisés, garantissant ainsi que les bonnes informations parviennent aux bonnes personnes au bon moment. Cette approche contextuelle améliore la prise de décision, renforce la connaissance de la situation et, en définitive, renforce à la fois la sécurité et la résilience opérationnelle.

La protection des biens constitue également un enjeu important. Grâce à des fonctionnalités telles que le suivi des biens, les campus peuvent localiser les équipements de recherche de grande valeur sur des cartes interactives, ce qui permet d'optimiser leur utilisation tout en réduisant le risque de perte ou de vol. L'enregistrement des communications et les journaux d'actions simplifient également l'analyse a posteriori, aidant ainsi les établissements à renforcer leurs processus de sécurité et à respecter les exigences de conformité.

Pour mettre en œuvre ces fonctionnalités, une base solide est indispensable. Une couverture Wi-Fi omniprésente, une intégration sécurisée de l'IoT et des systèmes de communication résilients constituent l'infrastructure qui prend en charge l'ensemble des installations, des amphithéâtres et résidences universitaires aux laboratoires de recherche et installations extérieures. Ainsi, la résilience et la sécurité s'intègrent naturellement au fonctionnement quotidien du campus, faisant de la technologie un allié de confiance pour la sécurité, l'efficacité et l'innovation.



Souveraineté et sécurité des données

La protection des informations sensibles, telles que les dossiers des étudiants, les données de recherche et les informations de santé, nécessite une conformité stricte et des pratiques rigoureuses en matière de cybersécurité. Chez Alcatel-Lucent, nous :

- suivons les pratiques exemplaires du National Institute of Standards and Technology (NIST) des États-Unis pour évaluer les risques associés aux nouvelles fonctionnalités et mettre en œuvre des fonctions de cybersécurité, comme le chiffrement natif;
- détenons une certification Critères communs de niveau EAL2+;
- appliquons la norme ISO 27001 à toutes nos solutions infonuagiques;
- prenons en charge le ZTNA, la segmentation granulaire du réseau et des politiques de sécurité très précises afin de réduire le risque d'activités non autorisées;
- réalisons sur nos produits des essais spécialisés en sécurité, notamment des tests d'intrusion;
- veillons à ce que nos produits répondent aux principales certifications et exigences sectorielles, notamment HDS, HIPAA et FERPA.

En tant qu'experts reconnus en cybersécurité, nous contribuons aux propositions de l'Union européenne relatives aux directives sur la cybersécurité. Nous mettons également à profit notre expertise en matière de cybersécurité pour aider nos clients à choisir et à mettre en œuvre la combinaison adéquate de solutions sécurisées de communications unifiées et de collaboration afin de répondre à leurs besoins, tout en formant leurs collaborateurs aux meilleures pratiques en matière de cybersécurité.

En combinant des solutions certifiées, une gestion proactive des risques et la sensibilisation du personnel, les universités et les établissements scolaires peuvent renforcer la souveraineté des données tout en favorisant la conformité et la confiance.

www.al-enterprise.com
© 2026 ALE International, ALE USA Inc. Tous droits réservés pour tous pays. Le nom et le logo d'Alcatel-Lucent sont des marques commerciales de Nokia utilisées sous licence par ALE. Pour voir la liste des marques de commerce d'ALE, veuillez consulter : www.al-enterprise.com/fr-fr/documentation-juridique/marques-copyright. Certaines images contenues dans ce document peuvent avoir été générées à l'aide d'une intelligence artificielle et sont fournies à titre indicatif uniquement. DID25060501FR (octobre 2026)

Alcatel·Lucent