



Making resilience and security a priority

Alcatel-Lucent Enterprise solutions for education

Table of contents

- | Overview
- | IT/OT collaboration in educational environments
- | Resilient and secure network solutions
- | Resilient and secure communications solutions
- | Protecting people and assets
- | Data sovereignty and security



Overview

With growing global challenges and increased cyber and physical risks, campus leaders must prioritize resilience, risk management and sustainability. Cyber and physical threats are rising, and educational institutions face mounting expectations to keep services running, protect sensitive data and ensure student and staff safety. According to EdTech Magazine, cyberattacks against universities jumped 70 percent in 2023.¹ In this context, protecting digital and physical infrastructure is not a luxury—it's a necessity.

Why ICT is more critical than ever in education

Education has undergone a major digital shift, with universities offering hybrid learning, remote access to labs and digital exams. Students expect always-on, seamless and secure digital experiences. Faculty and staff increasingly work and collaborate from multiple locations. Meanwhile,

universities must safeguard massive volumes of sensitive information, from research data to personal records.

Alcatel-Lucent Enterprise supports education institutions globally, understanding the importance of securing people, data, learning environments and operations. Our solutions are built with resilience and privacy in mind—from classrooms to research labs, dorms to campus security offices. This eBook provides insights about resilience and security for your ALE communications, cloud and network solutions.

¹ [Cyberattacks against governments jumped 95% in last half of 2022, CloudSek says](#). CSO United States, January 2023.

² <https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-digital-transformation-strategy.html>.

eBook

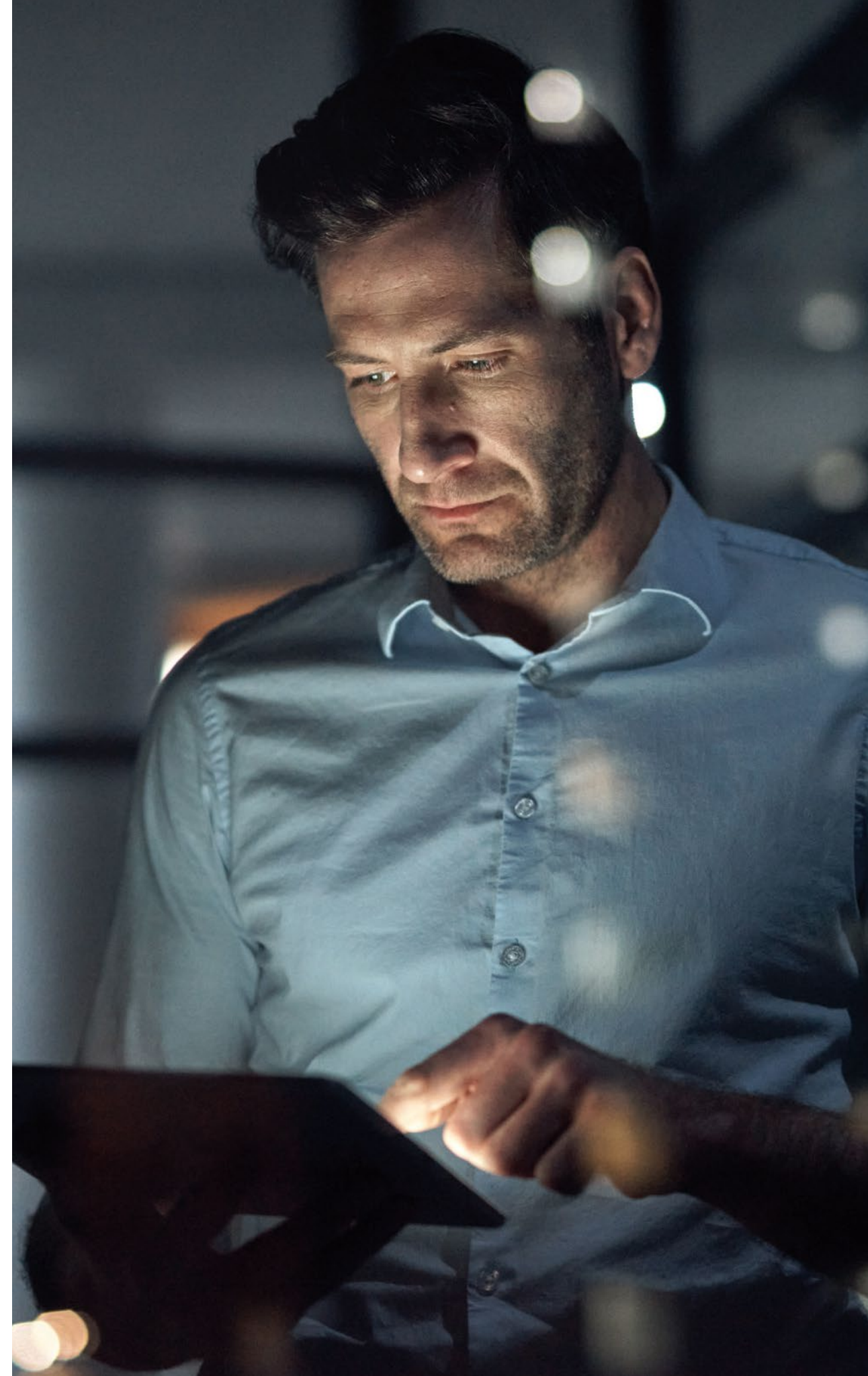
Making resilience and security a priority

IT/OT collaboration in educational environments

Before exploring how Alcatel-Lucent Enterprise can strengthen your resilience and security, it's important to recognize how the relationship between information technology (IT) and operational technology (OT) is evolving across campus environments. No longer can these two domains operate in silos. Collaboration is essential to protect and optimize the digital tools that keep campuses running—from HVAC systems and lighting to smart boards and IoT-enabled lab equipment.

Take the internet of things (IoT) as an example: If facility teams deploy smart lighting or occupancy sensors without IT involvement, these devices can quickly become security risks. Many have weak or inconsistent safeguards, and shadow IT on a smart campus can open the door to malware, network vulnerabilities or even breaches of sensitive academic records.

By working together, IT and OT teams gain the visibility and control they need to ensure compliance, enhance resilience and create a secure foundation for innovation across the entire campus.



Resilient and secure network solutions

The campus network is the backbone of every digital service, from online exams and lectures to research database access and emergency alert systems. A network outage could disrupt thousands of students and faculty, damage institutional reputation or compromise research integrity.

ALE's Digital Age Networking solutions are built with resilience at their core. From secure-by-design architecture to embedded segmentation and access control, our networks are hardened to resist disruption. We provide campus-wide visibility, automated onboarding for trusted devices and simplified management, all without hidden costs or add-on licenses.

7 best practices for your network solutions

From online classes and research projects to IoT sensors in smart classrooms, downtime or security breaches directly affect teaching, learning and student trust. Below are seven best practices that universities and schools can adopt to improve resiliency and security in their IT and OT environments.

1. Keep systems current with lifecycle management by regularly reviewing solutions with technology providers to ensure the latest software versions, security patches and enhancements are applied. Use lifecycle management tools like ALE ProActive Lifecycle Management (PALM) to track obsolescence and end-of-life milestones, so hardware replacements can be budgeted and planned for before they become urgent.
2. Strengthen switch security at the code level, protecting your infrastructure by ensuring the network operating system is hardened. ALE's Secure Diversified Code randomizes memory allocation to reduce exploit risks. Independent Verification & Validation (IVV) by third-party experts adds another layer of trust by identifying and eliminating potential vulnerabilities before they reach production.
3. Apply a zero-trust security strategy to your campus network by implementing macro- and micro-segmentation to isolate sensitive systems (such as student records and research labs) from general traffic. Follow a phased approach (monitor, validate, plan, simulate and enforce) to avoid disruptions while improving resilience.
4. Build in redundancy with Shortest Path Bridging to provide fast failover and dynamic rerouting of traffic in case of link or device failures. This creates an efficient, automatically containerized network, reducing the complexity of managing multiple virtual local area networks (VLANs)—an important advantage when scaling across large campuses.
5. Use virtual chassis capabilities to enhance reliability in mission-critical areas. This enables in-service software upgrades (ISSU) without downtime, supports ring or mesh topologies and simplifies management by presenting multiple devices as one logical unit—all while keeping costs predictable.
6. Automate backup and restore with network management tools like Alcatel-Lucent OmniVista® Network Management System. OmniVista Resource Manager simplifies configuration backups, policy enforcement and restore processes. Automating lifecycle tasks ensures faster recovery if outages or misconfigurations occur, reducing pressure on small IT teams in schools and universities.
7. Ensure router redundancy by implementing Virtual Router Redundancy Protocol (VRRP) to provide seamless failover between routers. This avoids single points of failure and ensures continuous access to critical applications such as LMS platforms, collaboration tools or emergency alert systems.



Invest in resilient and secure network solutions

Investing to ensure your network is resilient and secure always makes sense. However, understanding where best to invest can be complex and take time — planning is key. Before you get started, here are some key areas to consider to ensure you get the security and resiliency your organization requires:

- Together with your business partner, review and update network design to ensure your organization's requirements are reflected in the network, including the appropriate level of resiliency for sensitive and critical areas that impact essential campus services. For critical areas, consider adding backup servers and multiple connections where possible and applicable.
- Improve incident response using artificial intelligence (AI) and machine learning (ML) capabilities with the [Alcatel-Lucent OmniVista Network Advisor](#). This tool ensures problems are resolved before they impact end users by proactively identifying and addressing network or security issues. It expedites troubleshooting and improves network security through configuration audits and administering alerts in real-time about any sudden changes in network behavior.
- Consider [hardened switches](#) for harsh environments. The Alcatel-Lucent Enterprise family of ruggedized Ethernet switches is specifically designed to excel in challenging environments and extreme temperatures. These switches are built with ruggedized components and housed in sturdy enclosures, ensuring durability and reliability, and have the same operating system as other ALE switches. To enhance security and protect sensitive information, some models are equipped with intrusion alerts and alarm relays that enable the connection of external alarm systems. Some models even support MACsec (media access control and security) for secure data communications. With virtual chassis capability in ruggedized switches, you can gain improved redundancy, resiliency and scalability.
- Provide [ALE technical training](#) for the network operational team to help them detect and react quickly to issues

Resilient and secure communications solutions

Communications are crucial for educational institutions to interact with students, staff and other institutions, as well as for the dissemination of important information. Communications systems must be available in times of crisis, when students and staff need campus assistance most. Resilience and security are evolving, and regular reviews will help keep your Alcatel-Lucent Enterprise communications solution safe and available.

ALE communications solutions are secure by design. That means we consider security during every step of product definition, development and delivery. All hardware and operating systems are hardened, and denial of service (DoS) protection is built-in. We comply with recognized certifications and accreditations for global security and privacy standards (ISO 27001, ISO 27017 and ISO 27018). We also adhere to industry-specific security and privacy standards, such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and Hébergeurs de Données de Santé (HDS) for health data hosting in France, as well as regional security and privacy standards, such as the General Data Protection Regulation (GDPR) in the E.U.

7 Best practices for your communications solutions

The following are seven best practices to ensure you fully optimize the resilience and security of your ALE communications solutions.

1. Review system status with your business partner regularly to ensure the latest version of software, patches and security enhancements are installed and that your SPS contract is up to date
2. Regularly review security and service continuity components in your [Alcatel-Lucent OmniVista 8770 Network Management System](#), which includes valuable resilience and security information and features for your communications solution
 - Consider automated remote system backup to avoid configuration data loss
 - Configure alarm monitoring and ensure it is regularly updated with the right thresholds. Additionally, verify that notifications for communication system failures or quality alerts are sent to the appropriate individuals.
3. Review and enforce a strong password policy, preferably using external authentication (RADIUS server) and set in place user reminders to help prevent toll fraud, which is still a threat in many countries
4. Train employees and ensure they are aware of risks and prevention measures
5. Review business-critical application servers for condition, suitability and serviceability
6. Consider a specific VLAN for voice. Separating voice data from other traffic reduces the chance of contamination, which could disrupt operations and potentially campus services.
7. Make sure your Session Border Controllers (SBCs) are set up correctly. Requirements may have changed over time.



Invest in resilient and secure communications solutions

Modern campuses need communication systems that are always available, whether for teaching, research or emergency alerts. As institutions plan next-generation solutions, here are key areas to prioritize:

- Deploy duplicate call servers and application services in mission-critical locations such as health clinics, dormitories and research centers. Redundancy ensures that communication remains available even if one system fails, safeguarding student well-being and operational continuity.
- Ensure Digital Enhanced Cordless Telecommunications (DECT) or Wi-Fi coverage includes not only classrooms but also sensitive and hard-to-reach areas such as laboratories, data centers and outdoor zones. Comprehensive coverage supports both daily learning and emergency communications.
- Use tools such as [Alcatel-Lucent Visual Notification Assistant](#) or Rainbow™ to create workflows with automatic triggers, whether from people, IoT devices or systems. This ensures that key personnel are notified immediately of issues, enabling faster response and recovery.
- Implement [Rainbow™ by Alcatel-Lucent Enterprise](#), the ideal collaborative tool to complement ALE communications solutions. Rainbow offers secure voice, video, messaging and file sharing, supporting hybrid teaching, mobile faculty and remote collaboration. Its hybrid architecture (cloud and on premises) ensures resilience by running from different locations, keeping communications open even during local disruptions. Features such as image and video sharing, including surveillance feeds, enhance situational awareness for both academic and safety use cases.
- For institutions with strict data governance requirements, Rainbow Edge can be deployed in a private or regional cloud, ensuring compliance with academic or national data policies while still delivering modern collaboration features
- ALE offers flexible solutions for remote teaching, mobile faculty and hybrid staff setups to support secure voice, video and collaboration from anywhere, including:
 - Rainbow for cloud-based collaboration
 - [IP Desktop SoftPhone/SoftPhone](#) for remote or hybrid staff
 - [DeskPhone with embedded VPN can be mass deployed](#) for secure, large-scale deployments

eBook

Making resilience and security a priority



Protecting people and assets

A smart campus is more than fast internet – it is a connected environment where technology actively protects students, staff and critical resources. By integrating communications, IoT and analytics, universities and schools can move beyond a reactive approach and create a proactive safety culture.

Real-time information plays a central role. Fire alarms, motion detectors, access control systems or AI-based video analytics can automatically trigger alerts to security teams or facilities managers, reducing response times and preventing small incidents from escalating. Instead of waiting for problems to be reported, institutions can anticipate risks and act immediately, whether locking down a building, directing maintenance to a failed HVAC system or responding to suspicious activity.

The true value emerges when data, workflows and communications come together. Tools such as Rainbow and Visual Notification Assistant can connect people, systems and IoT devices into automated workflows, ensuring the right information reaches the right individuals at the right time. This context-

aware approach improves decision-making, enhances situational awareness and ultimately strengthens both safety and operational resilience.

Protecting assets is almost as important as protecting people. With features like asset tracking, campuses can locate valuable research equipment on interactive maps, improving utilization while reducing the risk of loss or theft. Recorded communications and action logs also simplify post-event analysis, helping institutions strengthen their security processes and meet compliance requirements.

To enable these capabilities, a solid foundation is essential. Ubiquitous Wi-Fi coverage, secure IoT onboarding and resilient communication systems provide the backbone that supports everything from lecture halls and dormitories to research labs and outdoor facilities. In this way, resilience and security become a natural part of daily campus operations, turning technology into a trusted ally for safety, efficiency and innovation.



Data sovereignty and security

Protecting sensitive information such as student records, research data and health information requires strict compliance and strong cybersecurity practices. At ALE we:

- Follow National Institute of Science and Technology (NIST) best practices for risk assessments on new features and when implementing cybersecurity features, such as native encryption, in our solutions
- Have Common Criteria EAL2+ certification
- Apply ISO 27001 standards to all our cloud-based solutions
- Support ZTNA, granular network segmentation and highly specific security policies to reduce the risk of unauthorized activities
- Execute highly specialized, security-specific tests, such as penetration tests, on our products

- Ensure our products achieve key industry certifications, such as HDS, HIPAA and the Family Educational Rights and Privacy Act (FERPA)

As recognized cybersecurity experts, we contribute to E.U. proposals for cybersecurity directives. We also leverage our cybersecurity expertise to help customers choose and implement the right mix of secure unified communications and collaboration solutions to meet their needs, along with training their employees in cybersecurity best practices.

By combining certified solutions, proactive risk management and staff awareness, universities and schools can ensure data sovereignty while maintaining compliance and trust.