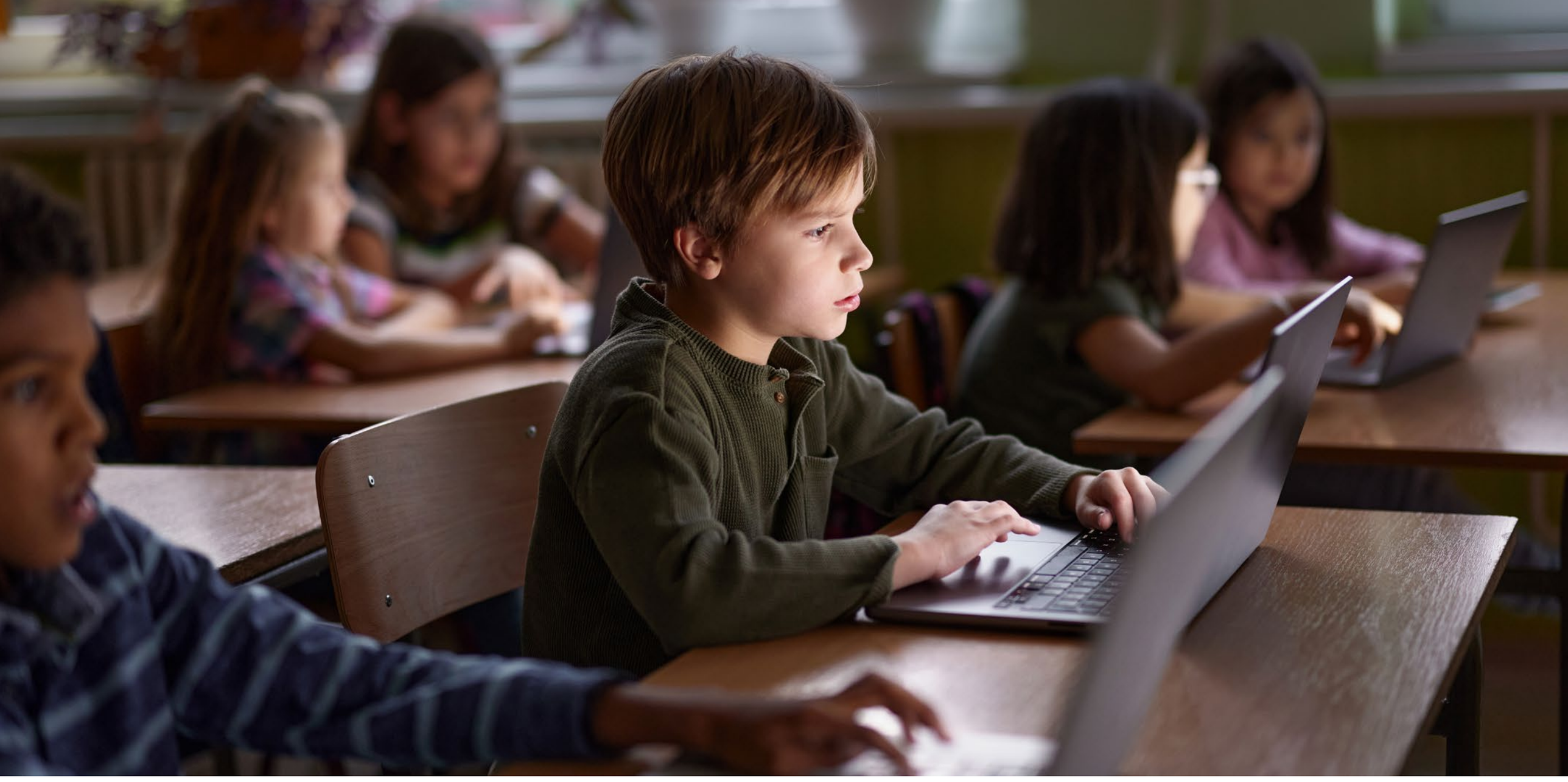


Making resilience and security a priority

Alcatel-Lucent Enterprise solutions for education

Alcatel·Lucent
Enterprise

eBook

Table of contents

Overview

With growing global challenges and increased cyber and physical risks, campuses must prioritize risk management, safeguard critical infrastructure and protect students and faculty. According to EdTech Magazine, cyberattacks against universities jumped 70% in 2023.[1] The expectation is that the business of education continues whatever the situation and that students and staff are kept safe. In today's global climate, it's more important than ever to maintain data security, protect data sovereignty and ensure service availability.

Education sector and why ICT is more critical than ever

In recent years, digital transformation in the education sector has rapidly advanced, with an increasing number of students and staff accessing digital services. Digital transformation has also enabled some employees of educational institutions to adopt a work-from-anywhere work style. There is growing pressure on campuses to accelerate digital transformation further. According to Educause, "Higher education is no longer immune from students' high expectations and preferences for digital service."[2]

Alcatel-Lucent Enterprise works with educational institutions across the globe and recognizes the significance of safeguarding students, staff, operations and buildings against cyber and physical risks. Our solutions consider security and data privacy at every stage of the design process and are built with resilient options to fit every type of organization. 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.

Why IT/OT collaboration is critical

Before we explore how to improve resilience and security with Alcatel-Lucent Enterprise solutions, it is important to acknowledge the changing information technology/operational technology (IT/OT) relationship. In the past, IT and operations teams didn't collaborate closely and each had their own functions and responsibilities. These two worlds are now converging and must work as one. IT and operations teams that aren't aware of each other's activities, or that don't coordinate and collaborate, put the entire organization at risk.

Let's consider, for example, the vast number of internet of things (IoT) devices rapidly being deployed on many campuses. When IT isn't aware of the operations team implementing new IoT devices, they can't ensure the devices comply with the organization's security policies. IoT devices come with highly variable levels of cybersecurity features and may not be equipped with the latest protection mechanisms, or their capabilities may not have been fully implemented. These unauthorized shadow IT devices could run any software and be infected with viruses and malware. Left unchecked, they can easily introduce new vulnerabilities and attack vectors into the network. We are now seeing the emergence of IT/OT collaboration required to ensure network security and resiliency.

Resilient and secure network solutions

The network infrastructure is integral to the functioning of campuses as well as the provisioning of services for students and staff. Due to the sensitive nature of the information contained in campus networks and the critical services educational institutions run, downtime or disruptions in network services can have severe consequences, making resilience and security the priority. Reliable and secure networks are essential for campuses to deliver effective student services, protect sensitive information and ensure smooth operations.

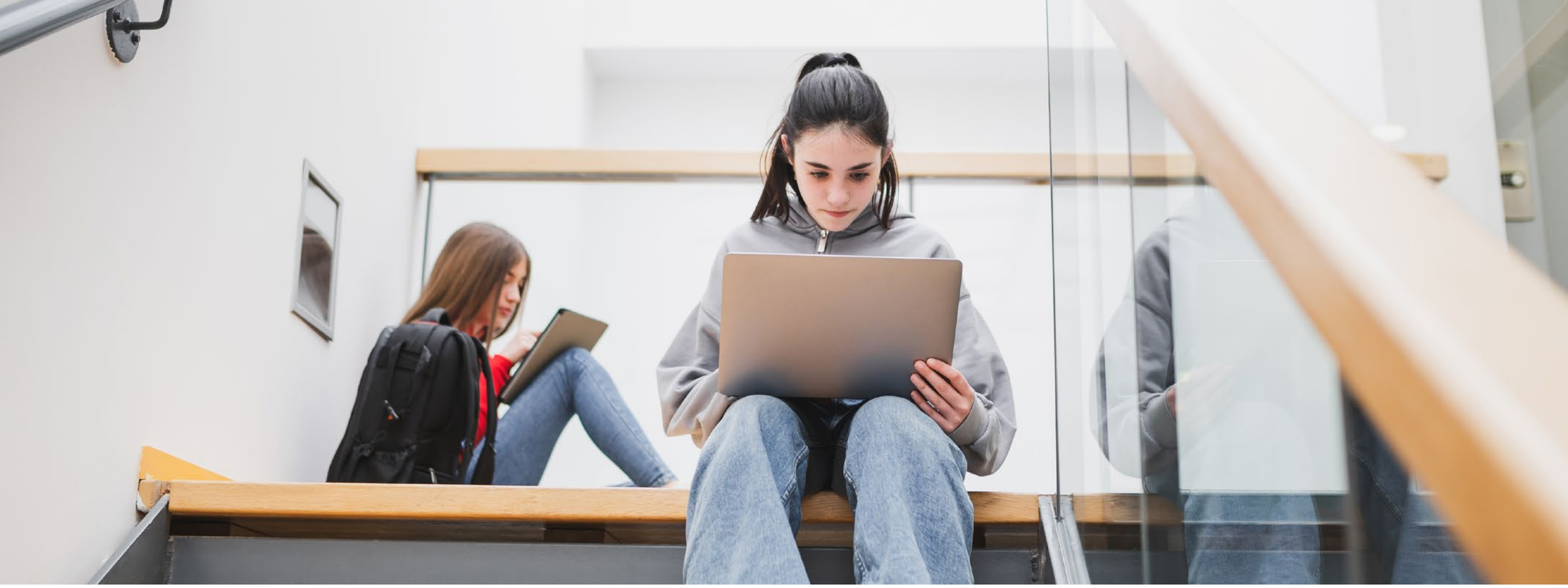
ALE Digital Age Networks are resilient and go beyond what many other technology providers offer. We embed security in our network and solutions from the earliest stages of design, with no additional licensing costs.

7 Best practices for your network solutions

Following are 7 best practices to ensure you fully optimise the resilience and security built into your Alcatel-Lucent Enterprise network solution.

The following are seven best practices to ensure you fully optimize the resilience and security of your Alcatel-Lucent Enterprise network solution.

1. Review your solution with your business partner regularly to ensure the latest version of software, patches and security enhancements are installed. A lifecycle management tool like ALE PALM, which provides information about obsolescence and end-of-life is also an advantage. Campuses can plan in advance for hardware replacement and anticipate deployment.
2. ALE Secure Diversified Code randomizes the location of different segments of code on your switches, dramatically increasing security. In addition, ALE secure diversified code is subject to independent verification and validation (IVV) process, conducted by a third-party cybersecurity expert that analyses and tests the ALE operating system to identify and eliminate any potential vulnerabilities, backdoors, malware or system exploits in all new releases.
3. Adopt a zero trust security strategy and implement zero trust network access. Macro- and micro-segmentation of your network is crucial for maintaining a resilient infrastructure. Follow the ALE phased approach for micro-segmentation to ensure the proper implementation so as not to cause disruptive consequences. Monitor, validate, plan, simulate and enforce.
4. Make use of Shortest Path Bridging (SPB) to achieve redundancy through the ability to dynamically reroute traffic using multiple paths in the event of a path failure. It also creates an efficient and automatically containerized network.
5. Consider leveraging virtual chassis capabilities to enhance reliability in critical areas, as this enables redundancy and resiliency for your network, supporting in-service software upgrades (ISSU) and allowing for or ring interconnections. The virtual chassis presents a cost-effective solution to simplify network management while ensuring high availability.
6. Use Alcatel-Lucent OmniVista® Network Management System capabilities. OmniVista Resource Manager ensures that you have all the configuration backups from network switches, and will be able to restore them should the worst case happen or when the need arises. This powerful tool handles the complete backup and restoration lifecycle.
7. Implement Virtual Router Redundancy Protocol (VRRP). VRRP enhances network resiliency by providing a backup virtual router that can seamlessly take over if the primary router fails.



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 your 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 behaviour.
- 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

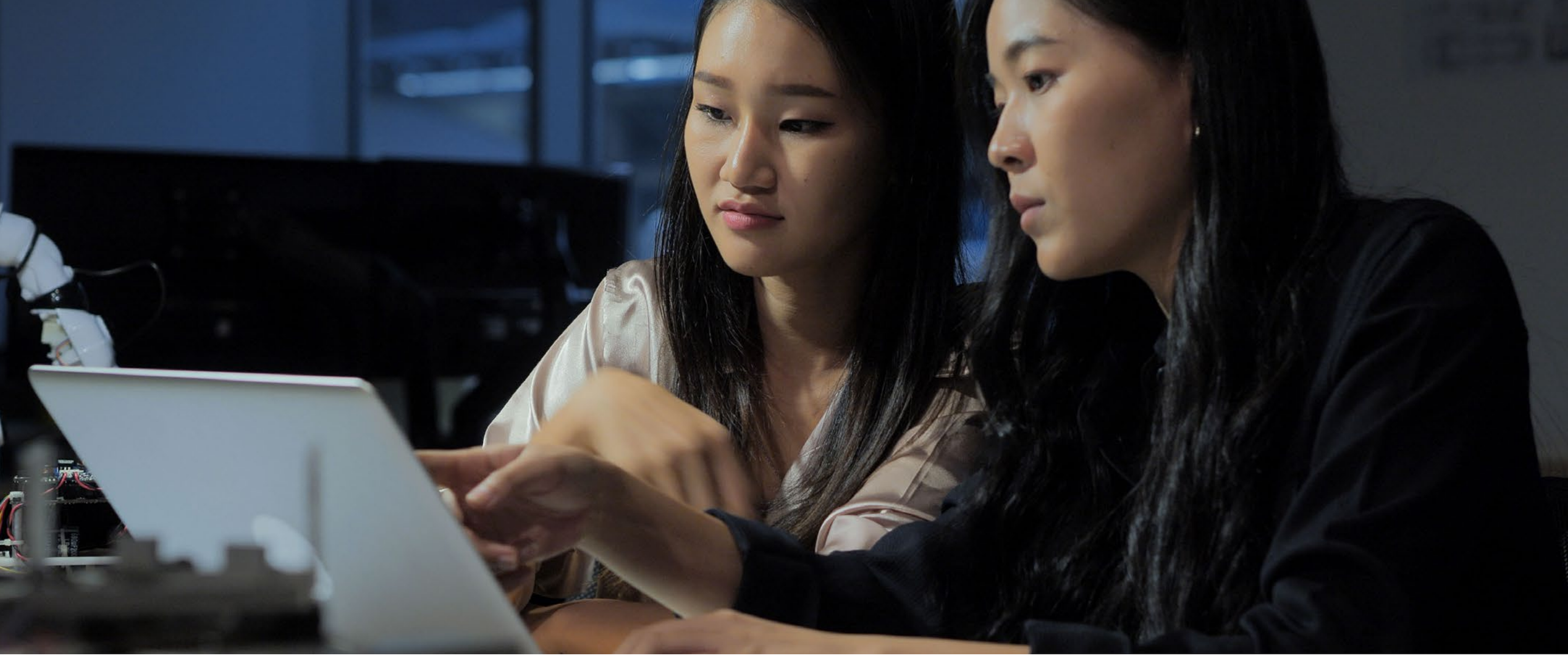
Communications are crucial for educational institutions to interact with students, staff and other institutions, as well as for the dissemination of important information. Communications systems must be available in times of crisis, when students and staff need campus assistance most. Resilience and 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. 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

Over the last few years, the educational environment has shone a light on the importance of communications with students, faculty and other staff. The following are some key areas to consider for campuses planning to invest in a communications solution to enhance resiliency and security.

- Redundant and resilient architecture. Duplicating call servers in critical areas, implementing remote site redundancy and duplicating critical application servers can provide additional protection.
- Customers who use TDM DECT should consider extending the coverage to critical areas to provide resilience in the event of an IP system failure
- Create a workflow using Rainbow and/or Alcatel-Lucent Visual Notification Assistant (VNA) with automatic triggers (trigger being human, IoT or system) to notify key people of system issues so they can act quickly and speed up the recovery process
- Deploy strong encryption. Encryption is based on industry standards designed natively into the solution, without any impact on voice quality and performance.

- Implement Rainbow™ by Alcatel-Lucent Enterprise, the ideal collaborative tool to complement ALE communications solutions. Rainbow offers a comprehensive set of features including voice, video and instant messaging, empowering seamless communications and efficient collaboration. With Rainbow, you can exchange images, videos and video surveillance feeds, enhancing contextual awareness and enabling better decision-making. Rainbow also provides hybrid communications with secure connectivity between on premises and cloud environments. It ensures resilient communications, keeping you connected to colleagues and customers and providing uninterrupted connectivity even in challenging situations. Hybrid communications also have the advantage of cloud and on premises operations being run from different locations, for the ultimate in resiliency and open communications. .
- For campuses with more stringent security requirements, Rainbow Edge offers an on premises alternative with a private cloud instance. The instance can be hosted in any data centre, providing complete control over servers, storage and networks, empowering educational institutions to customize and configure the infrastructure according to their requirements. Personalized security policies can be implemented, and resources can be managed autonomously. This level of control provides complete visibility and authority over your infrastructure, enabling campuses to make informed decisions and optimize performance in alignment with their objectives.
- Define a secure distributed workforce communication strategy. ALE provides multiple options for communications and collaboration for distributed, mobile and work-from-home employees, including:
  - Rainbow
  - IP Desktop softphone
  - ALE Softphone
  - Deskphone with embedded VPN and can be mass deployed with embedded security (VPN)

Protecting people and assets

ALE offers flexible, secure and highly available real-time communications and notification systems. These solutions can integrate with campus control centre operations, streamlining call dispatching and prioritization, facilitating contextual information exchange with IoT data, and enhancing collaborative efforts among various stakeholders, enabling improved decision-making and coordination.

The ability to interconnect IoT devices within buildings, combined with analytics and AI, is fundamentally transforming the communications landscape. Through the integration of sensors, video surveillance, Rainbow and AI, the shift from a reactive to proactive approach enhances time and cost efficiency. This integration facilitates a comprehensive contextual understanding, supports decision-making processes and subsequently reduces request response times.

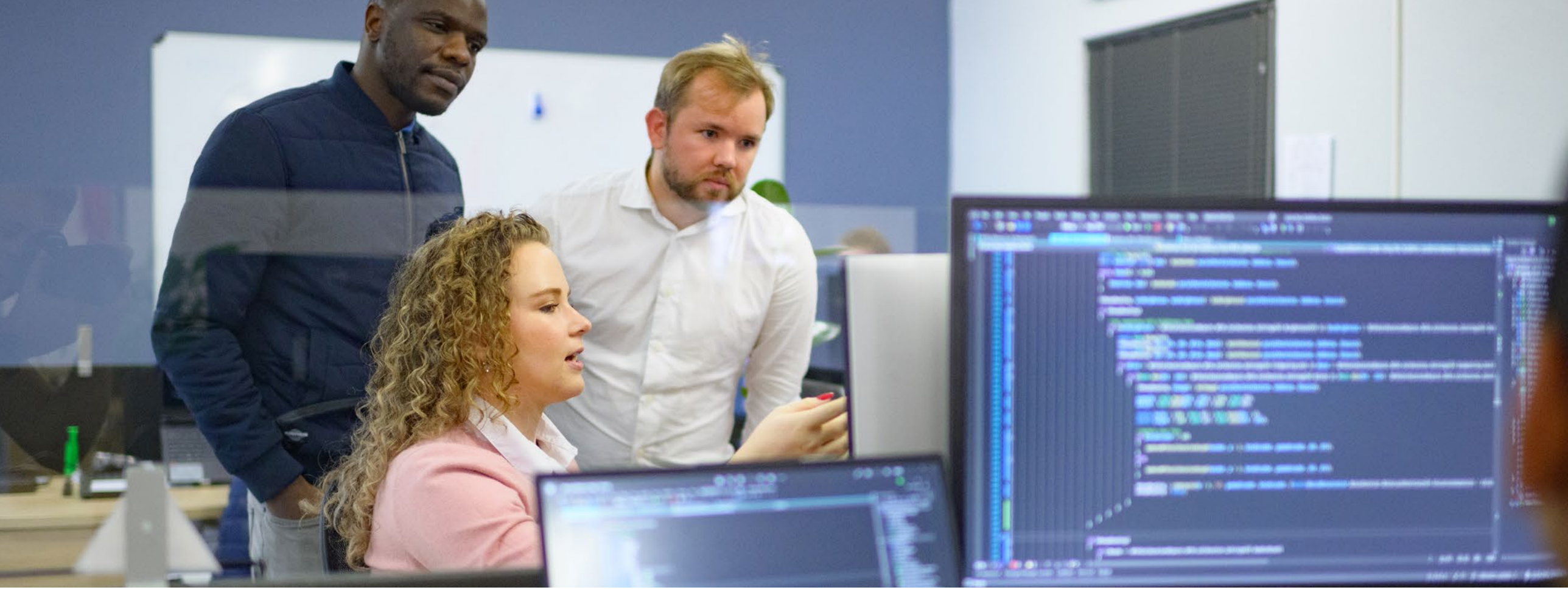
Functionalities like asset tracking and control of smart locks and lights streamlines operations. And the ability to record communications and log actions simplifies post-event analysis, enhancing security processes and mitigating potential liabilities. To achieve these advancements, a connected environment with ubiquitous Wi-Fi access and effortless IoT onboarding is crucial.

For time-sensitive, secure and highly available real-time communication platforms, a robust infrastructure is vital to ensure seamless operations. Your technology infrastructure should encompass appropriate software, high availability networking protocols and the flexibility to incorporate rugged network switches, which can seamlessly integrate with your ecosystem and withstand harsh environmental conditions such as limited airflow, shocks and extreme weather temperatures. Rugged equipment ensures longevity in such challenging locations.

When it comes to physical security systems, the stakes are high. Each minute and every piece of video footage could be crucial to identify wrongdoing, pinpoint the source of an incident, or understand the cause of campus disturbance. A robust video surveillance infrastructure is essential.

Networking infrastructure should not only provide sufficient bandwidth and power over ethernet (PoE) for surveillance cameras, but also seamlessly integrate with video surveillance management systems. This integration ensures an efficient and reliable surveillance network with smooth operation and easy troubleshooting. This enables the operations team to promptly resolve any video issues, particularly in environments or situations where every video frame is critical. Alcatel-Lucent OmniSwitch® solution integrations, accomplished through plugins with major video management systems, help you achieve this vital objective.

For times when asset tracking or locating individuals or equipment within your organization becomes necessary, an effective asset tracking solution can easily and accurately locate people and assets. Such a system also enhances safety and security by enabling the quick dispatch of assistance when the location of individuals is known. With the Alcatel-Lucent OmniAccess® Asset Tracking solution, staff and equipment can be located quickly and shown on a floor plan. Asset tracking also provides information about usage patterns, helping campuses assess whether assets are over utilized or underutilized.



Data sovereignty and security

Alcatel-Lucent Enterprise surpasses other technology providers in implementing best practices required for end-to-end cybersecurity. At ALE, we:

- Follow the National Institute of Science and Technology (NIST) best practices and recommendations when performing 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) compliance

As recognised cybersecurity experts, we contribute to European Union 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 and we train their employees in cybersecurity best practices.

Alcatel·Lucent
Enterprise