



How to secure your smart campus in the age of digital transformation

White Paper

Secure your smart campus in the age of digital transformation

Alcatel•Lucent 
Enterprise

Contents

Overview	3
The state of cybersecurity in higher education today	4
Digital Age Networking	6
Flexible connectivity with a Service Defined Network	7
Comprehensive access control with intelligent, automated policies	7
Reduced vulnerability with containerization and segmentation	9
Improved trust with artificial intelligence	10
Secure network equipment reduces vulnerabilities	11
Secure connections for incoming and outgoing traffic	12
Reporting	12
Conclusion	12

Overview

Cybersecurity has long been a top priority for education organizations. However, cybersecurity is changing due to digital transformation. As education institutions adopt smart campus strategies more connected and mobile devices will be added to their networks and Internet of Things (IoT) devices will increasingly access applications and data from beyond the network perimeter. As change accelerates, the old methods of network security become obsolete.

In this whitepaper, we explore how [Digital Age Networking](#) meets the demands of a digitally transformed campus with a multi-faceted approach to cybersecurity that maintains trust with secure, policy-based access to connected IoT devices such as video surveillance cameras, sensors and actuators across the entire smart campus ecosystem.

The state of cybersecurity in higher education today

Higher education institutions are making a significant investment in digital transformation, including new technology like Wi-Fi 6, adopting IoT sensor devices, location-based services and enabling research activities throughout the campus. However, as we extend the reach of technology and connectivity, there will increasingly be cyber-risks to consider. As part of the transformation, a smart campus provides student-centric services, supports business operations, teaching and learning and research. This means the storage and transmission of private student data such as social security numbers, addresses, credit card information, and other sensitive data, needs to be protected. Not to mention sensitive research activities which must be kept secure from threats at all times.

Changing cybersecurity threats

When connectivity and innovation are implemented in large campus infrastructures, they immediately become vulnerable to cyber threats. Today, we are increasingly challenged

in dealing with connected versions of IoT devices that have existed for a long time, such as CCTV cameras, where security was not addressed in the original deployment. Additionally, the sheer volume of data being collected and transmitted across a multi-user network, with numerous locations, can be extremely challenging to protect.

At the same time, the nature of cybersecurity threats is changing. Hackers are using Artificial Intelligence (AI) and Machine Learning (ML) to create more sophisticated, automated attacks. New social engineering techniques enable criminals to connect crumbs of information found across social media to create profiles of individuals and use that information to compromise the network.

Digital transformation in higher education is further altering cybersecurity requirements, resulting in greater complexity, increased use of connected devices, and a disappearing perimeter, all at an accelerating pace.

White Paper

Secure your smart campus in the age of digital transformation





Greater complexity

Universities are adopting new technologies, including mobile, IoT, Big Data, and advanced analytics. These new solutions bring a new level of complexity that requires a new way of looking at security.

Increasing use of connected devices

Smart campuses services include location-based services, geo-fencing, and public safety where the adoption of IoT is significant. Digital transformation is about the synergy of IT and how new services can support student success, attract new students and facilitate unique experiences on campus.

The perimeter is disappearing

Most institutions have, for a long time, clearly demarcated between users

and resources, inside and outside the network. However, as universities embrace digital transformation, digital communications are becoming more complex and need to interact with a broader ecosystem. This includes payment systems, student informations systems, learning management platforms, as well as smart devices like washers, lighting and temperature controls. Users no longer simply access resources from inside the network perimeter—they can be anywhere. For example:

- Students can access IoT device status of their washing machine
- Campus safety can access CCTV feeds and permit external access as needed
- Geo-fencing allows retail to offer incentives to shop/consume at their cafe

IT resources are also no longer confined inside the perimeter. They are on-premises

and in the cloud and connected via APIs. Universities need modern ways to protect resources when the perimeter no longer exists.

Accelerating the rate of change

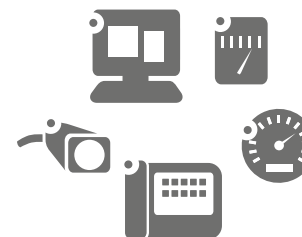
In a digitally transformed campus, everything moves faster. Security tools must handle this speed.

Figure 1. Mobility, IoT, and data analytics are key drivers of network transformation

Networks are in perpetual transformation



An always on mobility user experience



A proliferation of connected things to securely onboard and manage



An increase in data analytics to drive IT decisions and student success

Digital Age Networking

Alcatel-Lucent Enterprise [Digital Age Networking](#) (DAN) in education is a multi-faceted approach to network cybersecurity that provides security in depth for connected smart campus devices and applications through multiple layers of security.

Connectivity



Service defined network

Build a network foundation that is based on securely enabling the services that help universities digitally transform, including IoT to connect the campus to new services, location-based services to enable safety and asset management, and improve infrastructure operational efficiency, all while decreasing costs and risk.

IoT



IoT adoption

Simplify campus IoT network setup by easing device onboarding through device fingerprinting, provide more efficient operations for moves/adds or changes, and greatly increase security, with IoT enablement.

Augmented intelligence



Proactive analytics

Minimize the chance of cyber-attacks on the network; aid in managing crisis situations by prioritizing critical communications/resources; and reduce down-time related to maintenance.

Cloud economics



IT as a transformation engine

Confidently adopt cloud-based applications and services to provide operational savings, and anywhere/anytime secure access to information, teaching, and learning.



Flexible connectivity with a Service Defined Network

Our approach starts with a flexible, [Service Defined Network](#) that makes it fast and easy to configure network and cybersecurity policies for the vast number of connected users, devices and applications that fuel digital transformation.

In the past, IT has been a break-it/fix-it operation. IT would install new equipment, get it up and running, and manage the network using tedious manual processes. DAN is a smart, automated network that makes it easy to connect users and devices to their specific applications in a secure manner. Built using the [Intelligent Fabric](#) (iFab) technology, DAN includes our unique iFab combined with industry-standard [Shortest Path Bridging](#) (SPB). Together, these technologies simplify the creation and configuration of

networks while enabling multi-path routing and link aggregation to combine multiple network connections in parallel and thereby increase throughput and provide redundancy.

With the ALE approach, IT defines network services, architecture, access policies and containers, and the network builds itself automatically. Once the network is architected, if anything is moved, changed or added, the network makes the necessary adjustments automatically. For example, if a security camera is redeployed, it is automatically and securely re-enrolled into the network.

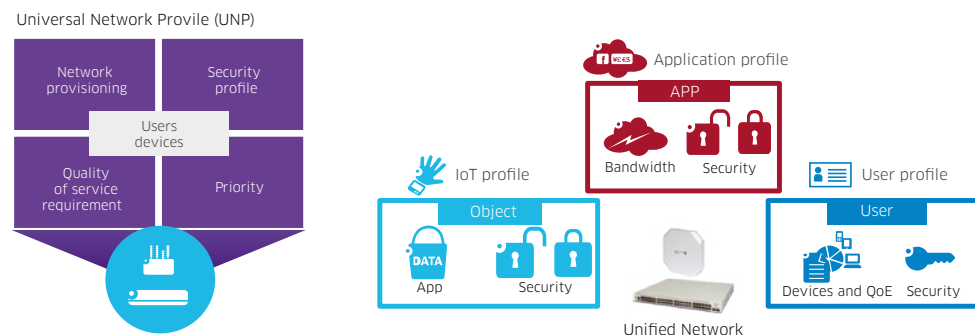
Using a Service Defined Network, universities benefit from automation that reduces manual configuration errors and helps them keep up with the accelerating rate of change within their organization. Because automation eliminates manual work, IT becomes more of a business engine driver.

Comprehensive access control with intelligent, automated policies

Universities can use DAN to define user access rules and policies that govern which applications and devices users can access and use - and they follow users wherever they go. For example, policies can be set up that provide:

- Security personnel exclusive access to security devices and systems
- Students access to academic applications
- Guests access to the internet only, and nothing else

Figure 2. Mobility and IoT Unified Access: authentication, authorization, classification



A coherent Quality of Experience all across the network for users, devices and applications

White Paper

Secure your smart campus in the age of digital transformation



ALE also offers location-based services, such as indoor wayfinding navigation and, asset and people tracking that enables universities to manage their campus while taking user location into account.

Unified Policy Management capabilities enforce policies automatically every time a user connects, ensuring users have only the permitted access privileges. Once users log into the network with a PC/laptop/mobile device and their credentials are validated, they don't need to keep authenticating. They stay connected if the device is on and the system automatically enforces the policy for that user.

Policies ensure that all users, inside or outside of the campus, have access only to permitted resources and that these access controls are enforced consistently. They also simplify smart campus workflows while enforcing cybersecurity. Policy driven authorization enables full campus mobility.

Figure 3. ALE Location-based services - Wayfinding

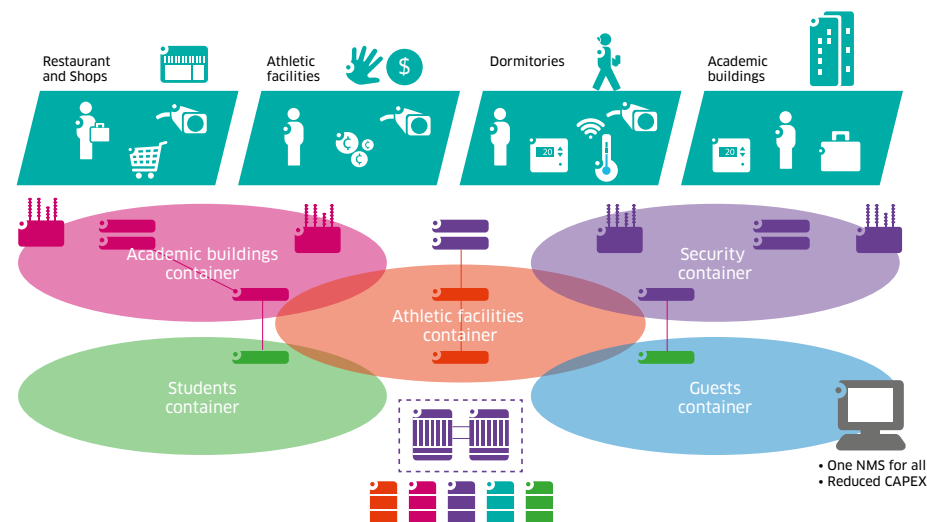




Reduced vulnerability with containerization and segmentation

In the drive to digitally transform, smart campus systems use many IoT devices, including sensors and actuators, smart lighting, smart appliances, as well as video cameras, HVAC systems, sprinkler systems, intrusion detection systems, and many others. The ALE DAN solution allows universities to containerize each device, creating a virtual network segment to prevent any device from becoming a vector for attack. Containerization within Digital Age Networking makes multiple virtual networks out of a single physical network, which is managed by a single management system.

Figure 4. Multiple virtual private networks over one physical IoT network



Containerization is simple for IT to implement. The DAN solution automatically discovers each device on the network. When a device is plugged into the network, the [Alcatel-Lucent OmniVista® 2500 Network Management System](#) - available on-premises or in the cloud - attempts to identify that device through device fingerprinting. If the management system doesn't have the device in its database it will consult a cloud-based database of 17 million plus devices.

Once the device is identified the system will classify it, for example, as a security camera. If that device is on the approved vendor list for security cameras it will be connected to the network. If not, then it won't be connected. The camera is then set up in a virtual container for that type of device, segmenting it from the rest of the network. If someone hacks into any networked device, that attacker will be unable to use that device to access the rest of the network.

Improved trust with artificial intelligence

Once devices are connected they must be continuously monitored to identify any threats and maintain trust. ALE analytics and application visibility allow network administrators to see what's going on in the network by device. Analytics identify patterns for normal, expected network behavior as well as any unusual patterns when they occur. We can look at the behavior of

applications at the edge of the network to decide whether to connect to that application as well as unusual behavior in allowed applications, such as a video camera that's producing more data than it should.

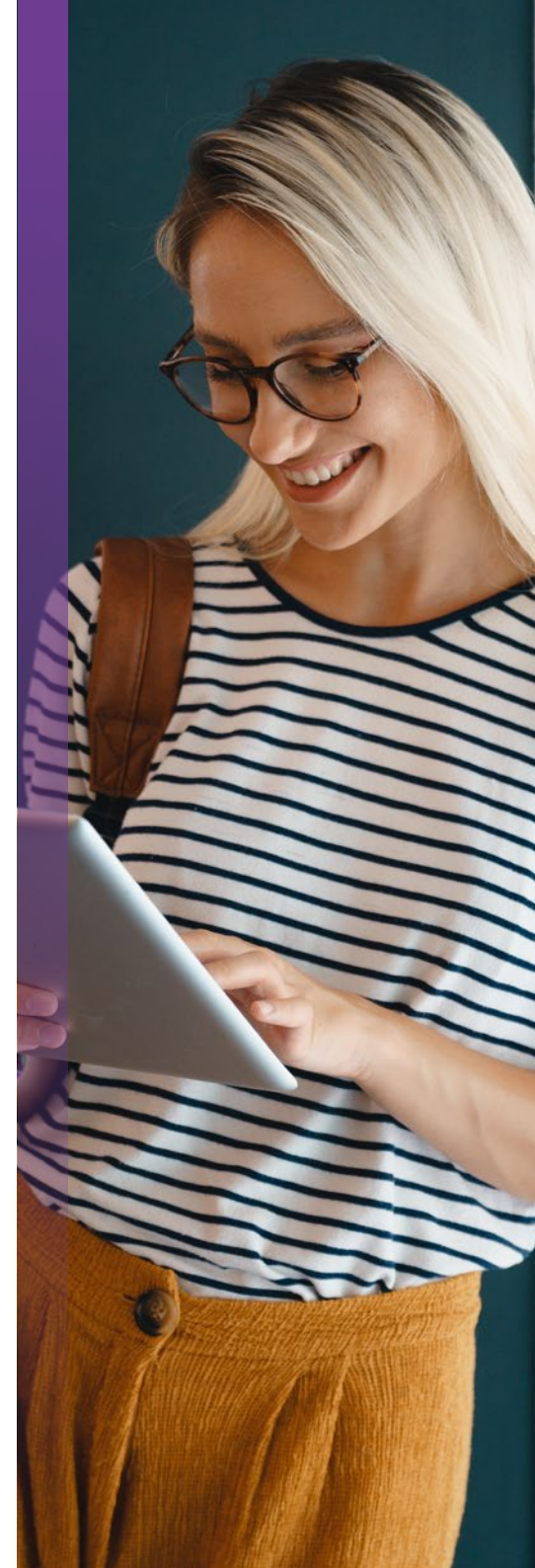
If an anomaly or unusual behavior occurs on the device, the analytics will alert so the network security manager can intervene. Today the investigation must be performed manually, but ALE is working on automating the response using AI and ML.

Figure 5. OmniVista 2500 Network Management System - Analytics dashboards



White Paper

Secure your smart campus in the age of digital transformation





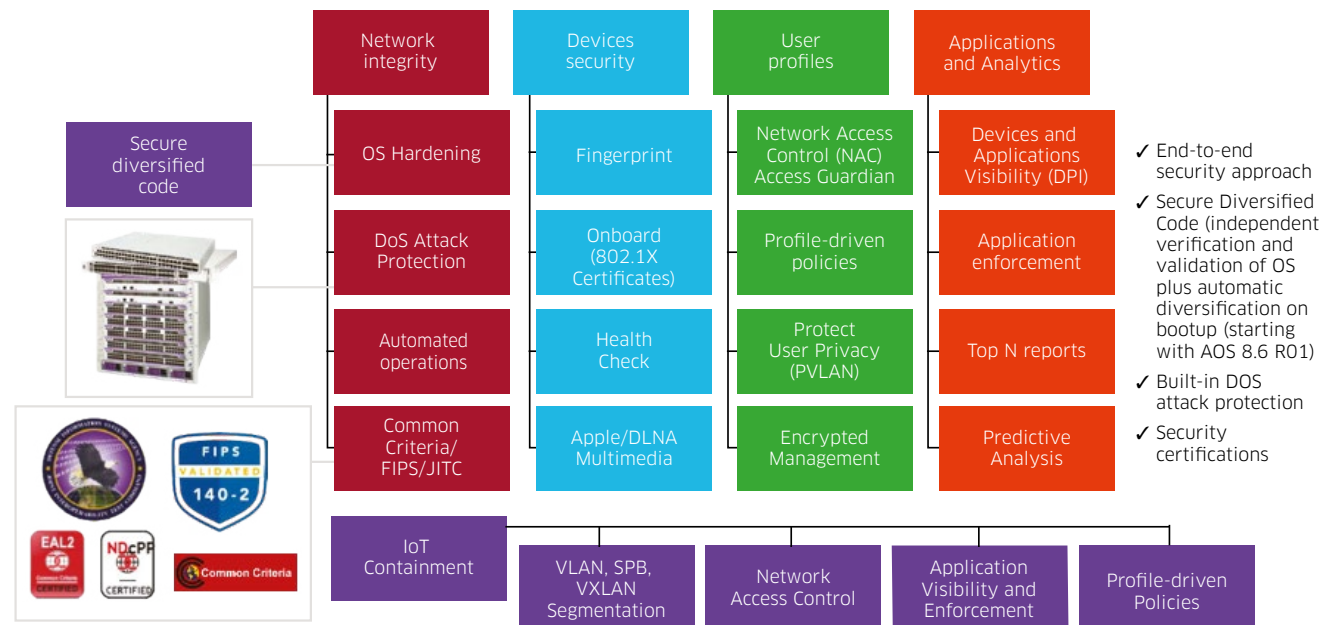
Secure network equipment reduces vulnerabilities

Cybersecurity is a top priority for higher education and they are aware of the need to secure IoT devices on the network. However, they may fail to consider devices that form the foundation of the network, such as switches and access points.

ALE employs many technologies to reduce the threat from these devices. Our approach includes:

- Send the OS software for third-party verification and validation to ensure it has no easy entry points or backdoors
 - Ensure every time a switch is booted up, the memory is compiled and brought up in a different manner. Although switches function identically, no two have the same memory configuration internally. If someone were to break into one of our switches, they would be unable to access another switch the same way.
 - Provide built-in denial of service (DoS) protection and quarantine.
- Our OS can detect and discard DoS traffic and automatically quarantine misbehaving devices.
 - Security certifications such as Common Criteria, FIPS, and JITC
 - Provide microservices architecture – critical software updates such as TLS, HTTPS and SSH without rebooting the switch ensuring continuous network operation
 - Harden the OS software to provide secure, diversified code

Figure 6. ALE Network in-depth security layered approach



Secure connections for incoming and outgoing traffic

For incoming traffic, ALE VPN capabilities provide an encrypted connection to the local network while end-to-end traffic is protected using MACsec encryption (also known as IEEE 802.1AE) to ensure information remains private as it traverses the network.

Reporting

ALE reporting enables access to information about the status, health and performance of the network, how applications are running, and the overall user experience. In addition, network analytics data can be exported to be consumed by student success applications, as well as to make informed decisions on improving network performance.

Conclusion

Digital transformation has profoundly changed university cybersecurity requirements as the number of connected devices increases, the network perimeter disappears, and change continues to accelerate. Alcatel-Lucent Enterprise Digital Age Networking for smart campuses keeps your IT assets and data secure in today's age of digital transformation. With this solution you can closely manage user access, reduce vulnerabilities created by IoT, mobile and network devices, keep the inevitable breach from providing a vector for attack, all while enabling the services and applications your institution requires.

