Alcatel-Lucent Enterprise Cybersecurity for Enterprises

Brochure

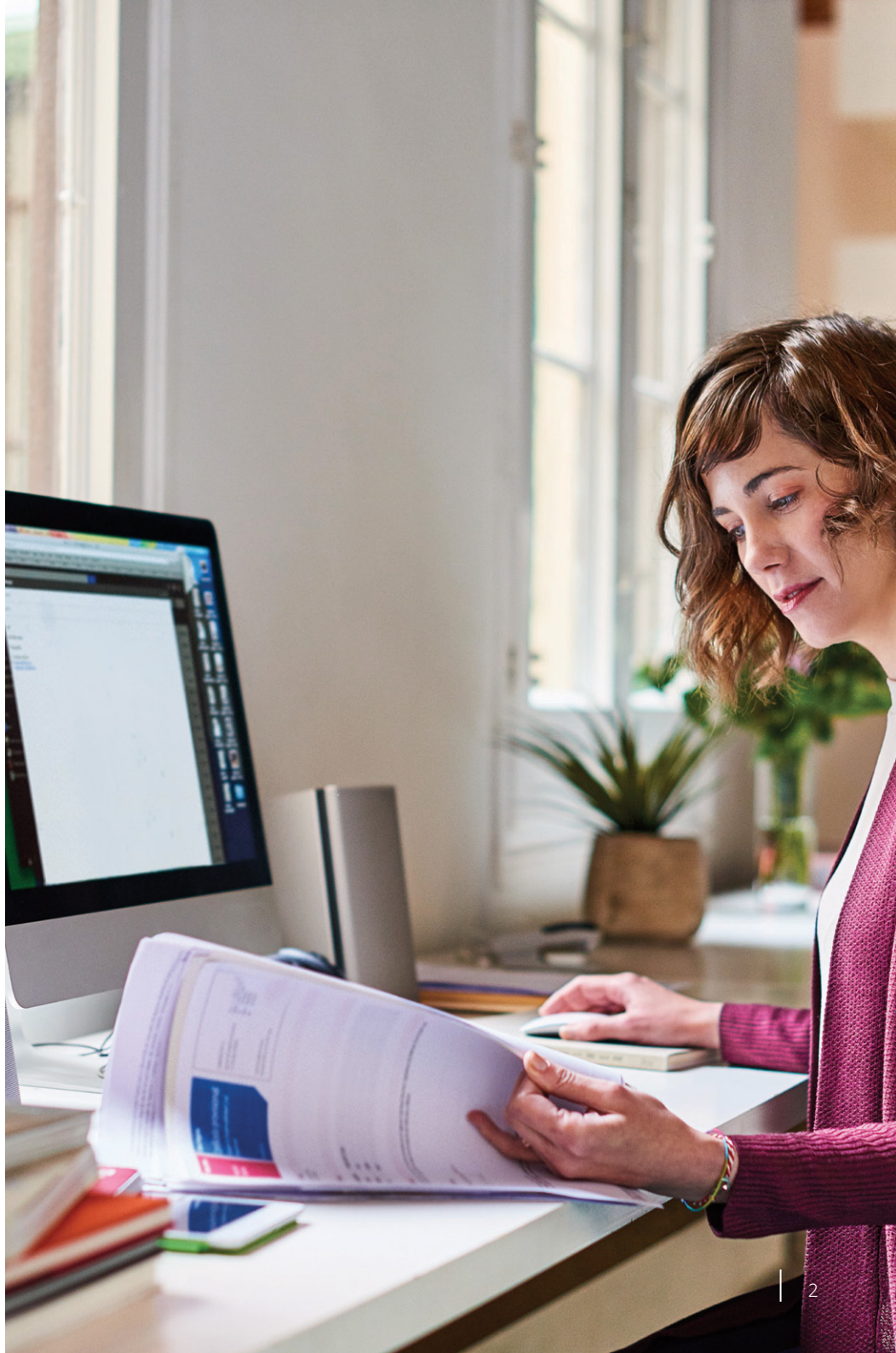
Alcatel·Lucent Enterprise

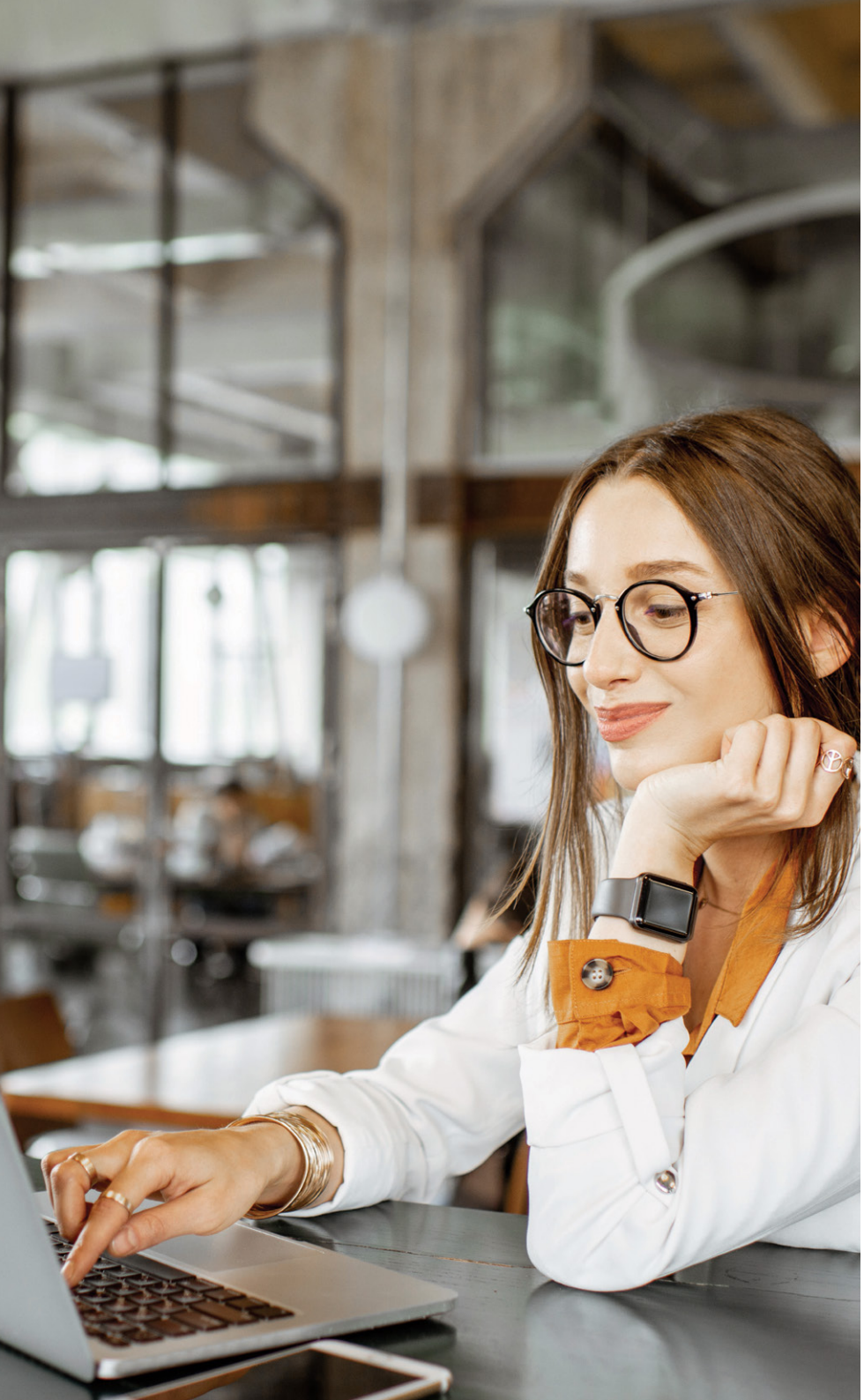
Overview

Cybersecurity has long been a top priority for enterprises. However, cybersecurity demands are changing due to the digital transformation taking place. Digital transformation means organisations use more connected and mobile devices on their networks while employees are increasingly accessing applications and data from beyond the network perimeter.

As change accelerates, the old methods of network security can no longer keep up. This document shares insights on the forces changing today's enterprise cybersecurity requirements and recommends strategies businesses can adopt, and technologies to deploy, to keep data and systems secure in the age of digital transformation.

The Alcatel-Lucent Enterprise cybersecurity solution meets the demands of a digitally transformed enterprise. With a multi-faceted approach to cybersecurity, enterprises can provide policy-based access to connected devices, secure data and software applications, across the enterprise ecosystem.





Changing challenges

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, or of the data held by organisations.

Enterprise digital transformation is also impacting cybersecurity requirements, resulting in greater complexity, increased use of connected devices, a perimeter that is disappearing, and all at an accelerating pace.

More devices, more complexity

Enterprises are adopting new technologies, including cloud, mobile, IoT, Big Data and advanced analytics. These new solutions introduce a new level of complexity that requires a new way of looking at security. Additionally, as the number of connected devices increases so too do the vulnerabilities and opportunities for breaches.

For example, in many cases the first generation of connected devices did not require passwords. Because the devices connected to the network, hackers could use them as a gateway onto the network. Today, security features such as hardcoded passwords are often mandated into devices, however, breaches remain inevitable and when they occur, hackers can still gain access to the network.

The vanishing perimeter

Most organisations have, for a long time, clearly demarcated between users and resources inside and outside the network. However, as organisations embrace digital transformation, they become more open to exchanges with the broader ecosystem, including other partners and providers in an integrated collaborative environment. Users no longer simply access resources from inside the network perimeter — they can be anywhere. Information can be exchanged with contacts in a different network. IT resources are also no longer confined within the enterprise perimeter. They can be on premises and in the cloud and connected using APIs. Enterprises need modern ways to protect resources when the perimeter no longer exists.

Macro- and micro-segmentation in a zero trust world

There are two kinds of segmentation, macro and micro. In macro-segmentation, the physical network is partitioned into different logical segments. All enterprises use segmentation, but not always for security reasons. Often, macro-segmentation is used for scalability, administrative, or organisational purposes. These segments can be a VLAN, a combination of VLAN + VRF, it could also be a VPN when talking about Shortest Path Bridging, MPLS, or even VXLAN or GRE tunnels. Traffic between users or devices on different segments is controlled by a physical firewall. If two devices are mapped to different VLANs and can communicate without going through a firewall, they are on the same macro-segment. For example, cameras and door locks might fall under the control of the access security group whereas thermostats might fall under the control of the building maintenance group.

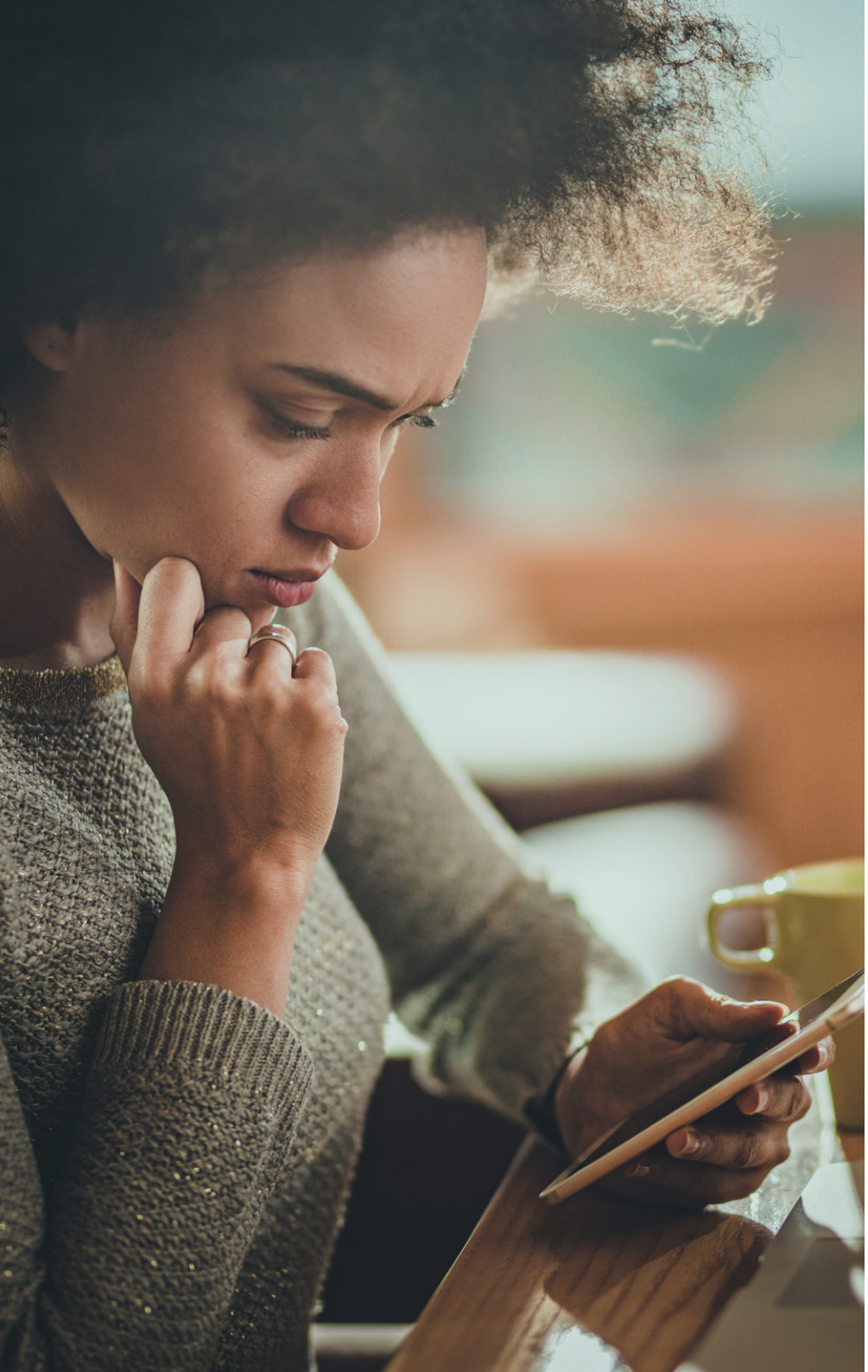
Micro-segmentation takes things one step further. Not all users are the same and not all users have a legitimate need to access all resources. The same profile that maps users to a segment also includes a set of policies which add granular control over user/device privileges that are different for different roles such as HR or Finance. This is known as 'role-based access', and is directly related to the 'principle of least privilege'. And so, even though cameras and door locks are both on the same segment, they do not need to use the same resources. The camera needs to communicate with the video recorder and the door lock with its server. There is no need for a camera to communicate with a door lock just like there is no need for a door lock to communicate with another door lock. These granular permissions are implemented through policies which are part of the profile and dynamically applied to the device after authentication.

The question is, do we really need both? The challenge with having a macro-segmentation only approach is that the firewall becomes a bottleneck because all VLANs have to be terminated at the firewall, and then performance issues are created. Alternatively more firewalls can be deployed at the distribution layer, however, that would be quite costly and still not good from a performance perspective. As well, more firewalls means there are multiple policy enforcement points, and multiple places to keep policies up-to-date.

Micro-segmentation alone can also be problematic. If the only policy enforcement is done through Network Access Control (NAC) policies, then policy lists become long and complex, and may exhaust the device capacity limits. A balance between these two types of segmentation lets the firewall control traffic between different segments (vertical), and the NAC policies control traffic within a given segment (lateral). By combining macro- and micro-segmentation, security threats that spill over from one security segment to another can be acted on, as well as ones that move laterally across the same segment.

In terms of a zero trust approach to network security, the guiding principle is 'act as if attackers are already present'. That means authenticating all connections. No asset and no user is inherently trusted. Whether they are on premises or off premises, they go through the same checks. There's no such thing as trusting internal users. Every access is authenticated.

If we consider a traditional approach to security where the network was viewed as a fortress built around the enterprise. The fortress represents the firewall, so that anything outside is untrusted and scrutinized, while anything inside is implicitly trusted and allowed. However, micro-segmentation, software-defined micro-segmentation specifically, takes it a step further. In addition to the fortress, and the security around the building, there are also security guards requiring authentication. This trust boundary is fuzzy, is distributed and is mobile. It's not tied to a particular location, switch port, or VLAN. It depends on the identity, the device, the situation and time of day. It's software-defined and it's adjusted on the fly. The key to this approach is that the components are managed and should be able to react and reconfigure as needed to respond to threats or changes in the workflow.



A solution for the evolving enterprise

Alcatel-Lucent Enterprise delivers a multi-faceted approach to enterprise cybersecurity that provides security in depth for connected devices and applications through multiple layers of protection.

Flexible connectivity

Our approach starts with a flexible, autonomous 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. Alcatel-Lucent Enterprise Digital Age Networking offers a smart, automated network that makes it easy to connect users and devices to their specific applications in a secure manner. Built using ALE Intelligent Fabric (iFab) technology, Digital Age Networking combines iFab with the industry-standard, Shortest Path Bridging (SPB). Together, these technologies simplify the creation and configuration of networks while enabling fast multipath routing and link aggregation to combine multiple network connections in parallel to increase throughput and provide redundancy.

With the ALE approach, IT defines network services, architecture, access policies and containers and the network builds itself out automatically. Once the network is architected, if anything is moved, changed or added, the network makes the necessary adjustments automatically and undetectably. For example, if a switch goes out of service, the network will automatically reroute around that switch.

Using an autonomous network, enterprises benefit from automation that reduces manual configuration errors and helps them keep up with the accelerating rate of change within their organisations. Because automation eliminates manual work, IT becomes more of a business engine driver.

Access control through intelligent, automated policies

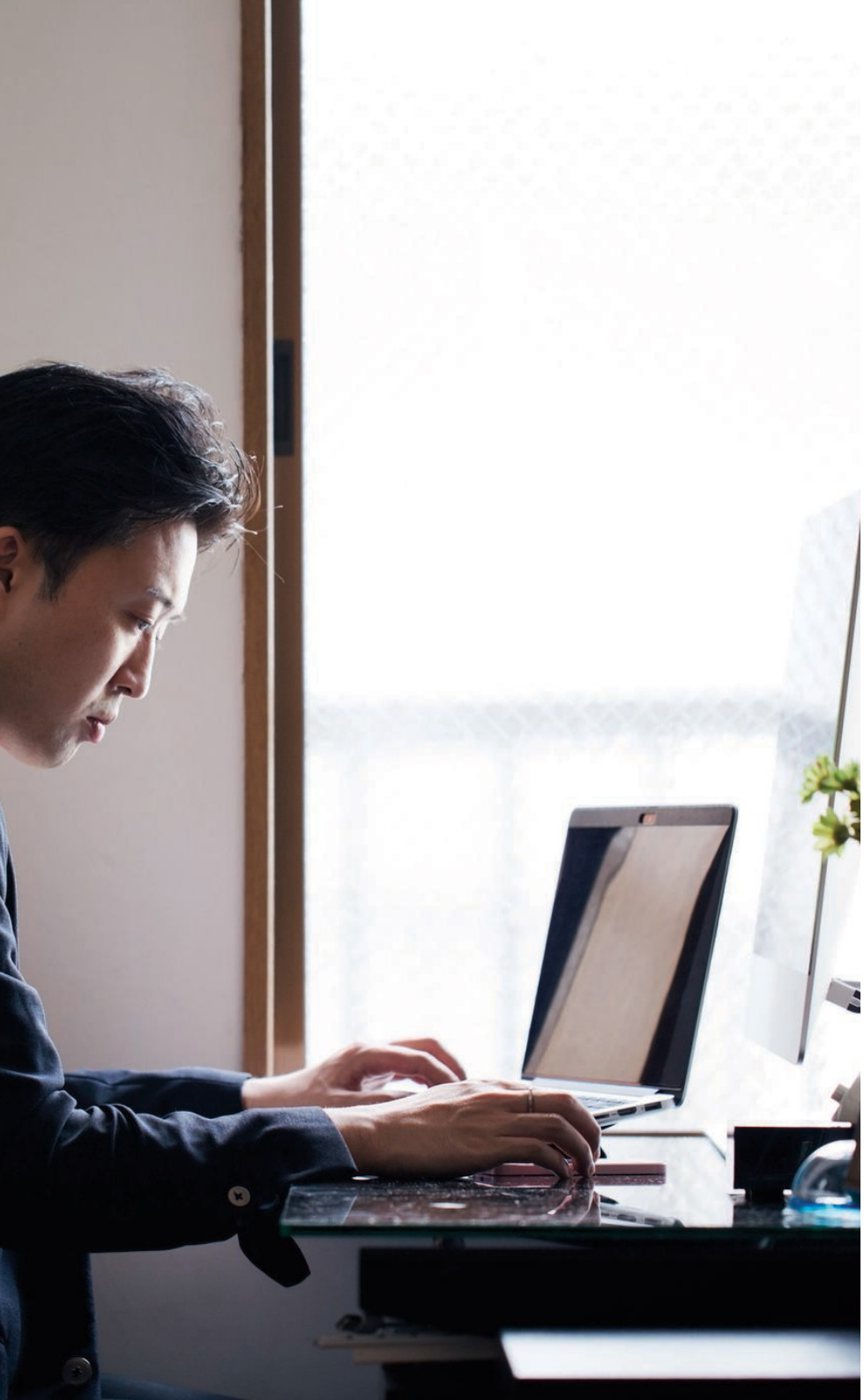
Businesses can use Digital Age Networking to define user access rules and policies that govern which applications and devices users can access and use — and follow users wherever they go. For example, they can set up policies that enable access to:

- Specific systems
- Internet services
- Other partners on a contractor-based policy

ALE also offers location-based services, such as indoor wayfinding navigation, asset and people tracking that enables organisations to set up policies that take user location into account.

Unified Policy Access Management (UPAM) 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 device and their credentials are validated, they don't need to re-authenticate. They stay connected if the device is on and the system automatically enforces the policy for that user.

Policies ensure all users, inside or outside the organisation, have access only to permitted areas and that the access controls are enforced consistently. They also simplify enterprise workflows while enforcing cybersecurity. Users can quickly access the systems and information they need without onerous security login procedures.



Reduce device vulnerability

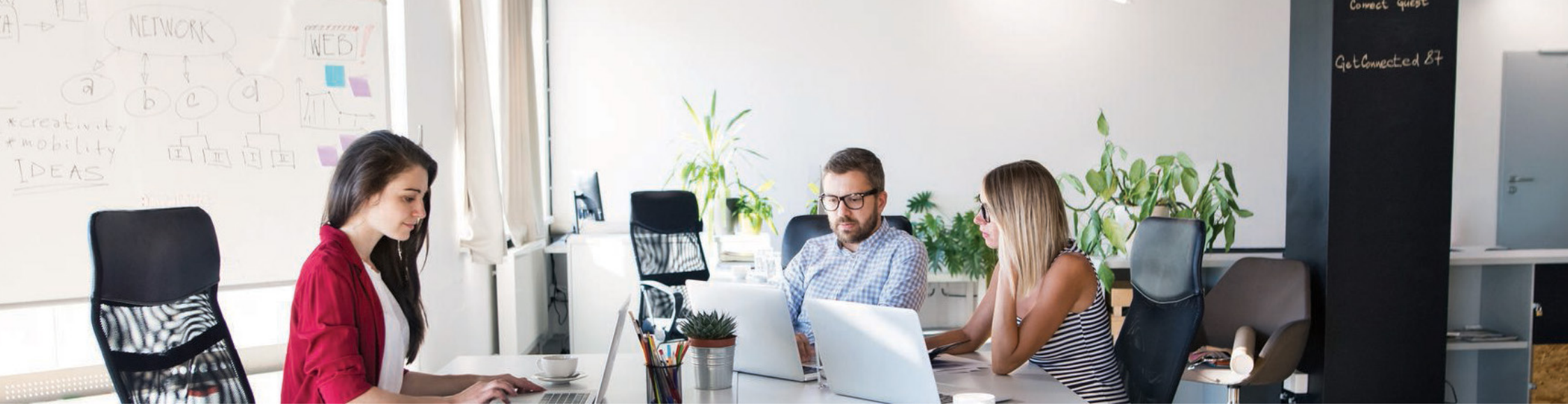
Enterprises connect to many IoT devices. The Alcatel-Lucent Enterprise Digital Age Networking solution allows organisations to containerise each device, creating a virtual network segment for it to prevent any device from becoming a point of attack. Containerisation within Digital Age Networking makes multiple virtual networks out of a single physical network, is simple for IT to implement and is managed by a single management system. This solution automatically discovers each device on the network. When a device is plugged into the network, the Alcatel-Lucent OmniVista® Network Management System, available on premises or in the cloud, attempts to identify the device. If the management system doesn't have the device in its database, it will consult a cloud-based database of 29 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 solution is then set up in a virtual container for the 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.

Artificial intelligence for a trusted environment

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. The behavior of applications at the edge of the network can be monitored to decide whether to connect to the application as well as detect any 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 show that 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.



Secure the network

While organisations today are aware of the need to secure IoT devices on the network, they may fail to consider devices that form the foundation of the network, such as switches and access points. Alcatel-Lucent Enterprise employs many technologies to reduce the threat from these devices. ALE solutions:

- Harden the OS software to provide secure, diversified code
- 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 an ALE switch, they would be unable to access another switch the same way.
- Provide built-in denial of service (DoS) protection. The CPU can detect unusual amounts of network traffic and automatically shut down the CPU if necessary.
- Multiple security certifications such as JDIC and FIPS
- Perform continual software upgrades

Secure connections for incoming and outgoing traffic

For incoming traffic, our VPN capabilities provide an encrypted connection to the local network while end-to-end traffic is protected using the MACsec encryption (also known as IEEE 802.1AE) to protect information as it traverses the network, and with the ability to reload services, such as TLS and HTTPS with no reboot required, the network isn't interrupted.

Reporting

ALE reporting enables different personas to access information about the status, health and performance of the network, how applications are running, and user satisfaction. For example, IT can see data about network performance and operations.

Line of business units can ensure that equipment such as sensors or telemetry systems, are transmitting data to servers and tablets seamlessly. The IT department can determine whether the network is delivering services that allow employees to spend more time doing their jobs and whether they're getting the most out of the network.

Cybersecurity in Industries

Education

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 connectivity and innovation are implemented in large campus infrastructures, they immediately become vulnerable to cyber threats. Alcatel-Lucent Enterprise Digital Age Networking for smart campuses keep IT assets and data secure in today's digital transformation age. With this solution, institutions can closely manage user access, reduce vulnerabilities created by IoT, mobile and network devices, keep the inevitable breach from providing a point of attack, all while enabling the services and applications your students and staff require.

Transportation

The advancements in transportation systems resulting from the technological innovations will require transformation of the existing foundation upon which they are built. Integrating the devices and systems that enable any transportation ecosystem to function demands fast, reliable and secure connections. Transportation data networks must be IoT-aware to seamlessly connect sensors, cameras, signage and traffic control systems together. Network security is also vitally important to protect data and the integrity of the network.

ALE uses secure diversified code to improve network integrity and provide added security against network cyber-attacks. Secure diversified code protects networks from intrinsic vulnerabilities, code exploits, malware and potential back doors that could compromise mission-critical operations. ALE also provides finger printing for IoT to identify each device, including vehicles, sensors and cameras to ensure they do not pose a security threat to the network. The ALE in-depth security strategy has received the highest levels of certification from governmental agencies, including Common Criteria (EAL2 and NDcPP), JITC, FIPS 140-2 and NIST.

Healthcare

Healthcare has long been, and remains, one of the industries targeted most by hackers. And, the problem continues to grow. In 2018, the healthcare sector saw 15 million patient records compromised in 503 breaches, three times the count in 2017, according to Protenus Breach Barometer.[1]

Breaches occur because healthcare data is extremely valuable. Individual patient records contain everything including name, current and previous addresses, work history, names and ages of an individual's relatives and financial information such as credit cards and bank numbers.[2]

ALE Digital Age Networking provides a multi-faceted approach to cybersecurity that maintains trust with secure, policy-based access to connected medical devices, patient data and software applications across the healthcare ecosystem.

Government

The expanded role of digital at both the central government and city levels has blurred the line protecting digital assets that support transportation, infrastructure maintenance and environment monitoring. Government cybersecurity policies for data security, vulnerability, and trust management need to be revised.

The ALE approach to cybersecurity provides an end-to-end, service-centric approach to security to protect all layers of the service, from the network to the software.

On the device side, public sector organisations can use containerisation, to create a virtual network segment to prevent devices from becoming a point of attack.

Hospitality

The growth of IoT in the hospitality industry brings an explosion of cybersecurity threats, as the proliferation of sensors and connected devices greatly expands the network attack surface. IoT is especially susceptible because many IoT devices are manufactured without security in mind, or built by companies that don't understand current security requirements. Consequently, IoT systems are increasingly the weak link in network security for hospitality businesses.

Protecting IoT traffic and devices requires a strategic approach that takes advantage of multiple security safeguards. To help hotels, casinos, resorts and other hospitality businesses take advantage of the benefits and mitigate the risks of IoT deployment, ALE provides a multi-level security strategy that delivers protection at every layer of the infrastructure, from the individual user and device to the network layer. It also provides an IoT containment strategy to simplify and secure device onboarding and deliver the right network resources to run the system properly and efficiently, all in a secure environment to safeguard hospitality businesses from cyberattacks.

1 https://healthitsecurity.com/news/the-10-biggesthealthcare-data-breaches-of-2019-so-far
2 https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-tohackers/#2bb1f96b50cf

Summary

Digital transformation has profoundly changed enterprise cybersecurity requirements as the number of connected devices increases, the network perimeter disappears, and change continues to accelerate. Alcatel-Lucent Enterprise Digital Age Networking keeps your IT assets and data secure in today's digital transformation age. 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 point of attack and provide a trusted enterprise ecosystem.