How System Integrators address evolving Government ICT

White Paper

Alcatel·Lucent Enterprise

Table of contents

Overview

The business of providing information and communications technology (ICT) integrations to governments has changed significantly over the past five years. Before the disruptions caused by the pandemic, government ICT requirements were well-understood. Most government departments were in the process of either starting or planning for a cloud-centric digital transformation that would enable more efficient operations and a more effective delivery of services to citizens. However, the onset of the pandemic derailed most of those plans when the key priority shifted to finding ways for government employees to continue to do their jobs remotely.

Today, operational changes introduced to mitigate the impact of the pandemic have created a need for more complex government ICT solutions. New deployments must leverage all the benefits cloud networking offers to address citizens service delivery expectations and support employee hybrid working. This has created significant challenges for system integrators. The scope of government ICT projects continues to expand as departments try to address employee and citizen expectations. And new security, reliability and technical requirements must be met to provide ICT solutions that support continuously evolving distributed network needs.

To be successful in this environment, system integrators must stay well ahead of the ICT requirements curve. While the government continues to be focused on cloud-centric solutions, it's more important than ever for integrators to deliver secure, reliable and flexible networks that provide a vital link to cloud-based applications. With the right network solutions, integrators can offer comprehensive integrations that enable the efficient exchange of information among government employees and with citizens, wherever they are.

However, delivering full-featured networks that address government expectations has become difficult under current market conditions. In today's climate, a stable supply of network hardware and software is difficult to find. Evolving security and compliance requirements complicate integration efforts. And it is taking longer to offset fixed operating costs because of the unavoidable delays in invoicing that are now a fact of life due to supply chain shortages.

To deliver fully integrated network solutions in this environment and remain competitive, integrators can't compromise their business objectives by relying on traditional suppliers and supply chains. They must:

- Choose and source more efficient and intelligent network infrastructure solutions
- Deliver more functionality with every network integration while keeping a close eye on costs
- Leverage network infrastructures that can be configured and delivered quickly and maintained easily

Evolving ICT market conditions

New requirements create new challenges

As presented in a recent Alcatel-Lucent Enterprise white paper, the fundamental objective of a government's digital transformation is to create a digital workplace that will meet employee and citizen expectations. Hybrid work models have become a favoured way of working and government employees want to keep the flexibility these work models offer. Meanwhile, citizens have come to expect that they will be able to access the government services they need online and from anywhere, and that government agencies will be able to deliver those services efficiently.

While cloud-centric ICT solutions and services will be the anchor of the digital workplace, robust and reliable network infrastructures are still needed to provide the critical links to all cloud-based services in departmental offices and branch locations, for remote access, and even to enable more secure communications on defence platforms. The core hardware and software elements needed to enable these networks has not changed, but the task of system integrators has. They must find the right balance of technologies, which may include Gigabit Ethernet, Wi-Fi 6 and Wi-Fi 6E, as well as private, public and hybrid cloud environments. Regardless of which technologies are used, system integrators must now also address more rigorous government requirements to ensure that balance.

Network and data security are paramount

The security of the network itself and the data that it carries has been, and will continue to be, the most significant challenge system integrators must address for any government network. In fact, a review of government data breaches published in 2020 noted that governments at all levels are susceptible to attacks.

Today's government ICT networks are more complex. In addition to the hardware and software needed for communications and computing, these networks now provide the connections for a variety of systems, including Internet of Things (IoT) devices that enable smart building operations, surveillance and security solutions that protect the premises, and heating, ventilation and air conditioning (HVAC) systems that monitor air quality and manage temperatures. These and many more systems connect with a main operations centre either on premises or in the cloud. And every connected device and access point is a potential gateway into the network for a cyberattack that can compromise the entire ICT infrastructure and the data it carries.

Exacerbating the situation is the fact that hybrid and remote working has created more potential attack vectors and organisations are more at risk than ever. According to Deloitte:

> "Not only are people using personal computers and mobile phones to access company information, but the plethora of physical devices in homes—internet-connected thermostats, voice assistants, lights, and blinds—can all be attacked by criminals, who can then worm their way through a home network and into a treasure trove of personal and business-related data."[1]

In response to this reality, government IT teams are constantly looking for ways to upgrade the security posture of their distributed networks, while requiring more robust cyber-protection for their networks with every request for proposal (RFP).

[1] Stealing Physical Data in a Digital World, Deloitte, 2022.

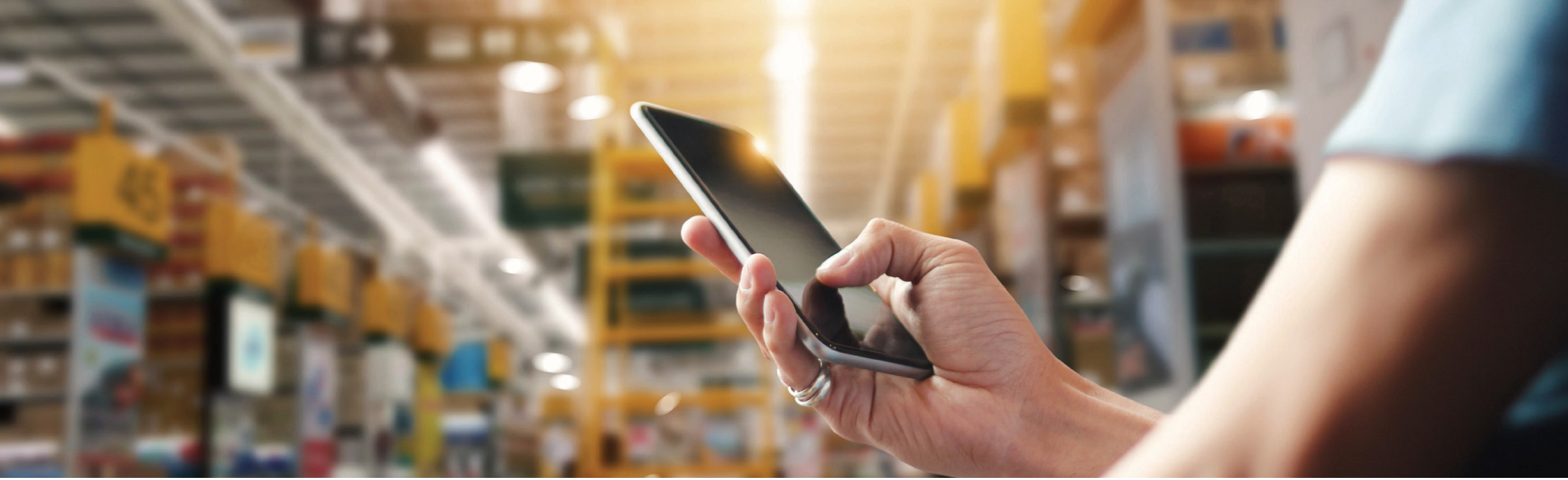
Securing the supply chain

In addition to more robust cyber-protection for network infrastructures and data, government departments must now ensure that the suppliers who provide the hardware and software for those networks are delivering critical ICT elements through secure supply chains. All these efforts focus on reducing the potential for backdoor gateways into critical ICT infrastructures. System integrators in many cases, must now ensure that any solution they propose meets a variety of secure supply chain requirements in order to respond to an RFP.

More stringent certifications are mandatory

While secure supply chain requirements may be new, system integrators must also continue to ensure the products they offer are certified to address government standards.

Although not all government RFPs require certification to meet specific standards, system integrators who work with suppliers who can provide products that meet certifications are in a much better position to propose solutions for government departments and agencies.



Reliable supply is critical

Ultimately, while integrators may find suppliers who can meet most or all the requirements, the biggest challenge continues to be finding a reliable and ongoing supply of hardware and software.

The impact of the pandemic on global supply chains has affected every industry. In the ICT space, workforce disruptions have resulted in slowdowns in everything from design to manufacturing. The shortage of semiconductors has further exacerbated already stressed supply chains, and some analysts predict shortages will continue to affect most industries until 2024 or later.[2]

What this means for integrators is that lead times for many ICT orders will get longer. Orders that may have previously been filled in 15 to 25 days, can now stretch from 15 to 24 months. And if the semiconductor shortage continues, as analysts predict, lead times may be even longer.

It's worth noting that finding a reliable supplier is only half the battle. The real value of the supplier to a government system integrator will be realised when the supplier's offerings meet the business objectives of the integrator, as well as the technical requirements of government ICT networks.

[2] When Will the Chip Shortage End?, Anne Hoecker, Peter Hanbury, Hans Joachim Heider, and Sophia Zou, Bain & Company, September 2022.

New challenges require focused solutions

Since the network is the foundation of any government digital transformation effort, the right combination of network technologies is needed to enable integrators to respond to RFPs with tailored integrations. With the right technologies and solutions, integrators can propose ICT infrastructures that address the government's distributed networking requirements.

As integrators search for ideal networking solutions, here are seven key elements that should be top-of-mind.

1. Open standards

Networking solutions built on open standards and open architectures are essential to efficient integrations. Hardware and software based on proprietary protocols and customised implementations of standards are typically more difficult to integrate with products from other suppliers. Additionally, IoTs are exploding across all industries. It is anticipated that by 2025, 20 billion objects will be connected globally.[1] Those IoTs will come from different vendors with different protocols so to integrate all the objects the network infrastructure must be open and standards-based. This creates challenges and inefficiencies during the initial integration process, which can increase integration costs and cut into already thin margins. It also complicates future updates and upgrades that may be needed to ensure the network is always operating at peak efficiency from the edge to the core, and that the most cutting-edge technologies are always protecting critical points in the network, such as intrusion detection systems.

The more open a solution is the easier it will be to integrate it into a standards-based network architecture. And the easier it will be to add, enhance and upgrade the network architecture with advanced technologies as they become available throughout its lifecycle.

[3] Networked World: Risks and opportunities in the Internet of Things

2. Flexibility of design

Every ICT solution should also offer the flexibility to scale the network up or down as needed to meet evolving requirements. With flexible, standards-based options, integrators can meet the immediate needs of government departments for coverage, capacity and functionality across a distributed network today, and easily adapt and add to the network to accommodate more users with access and services, wherever they may be tomorrow.

3. Secure hardware and software

To meet government ICT purchasing requirements, integrators must ensure the hardware and software solutions they are proposing meet all secure supply chain guidelines. This includes verification of the country of origin for hardware and software, as well as the security compliance of all operational software.

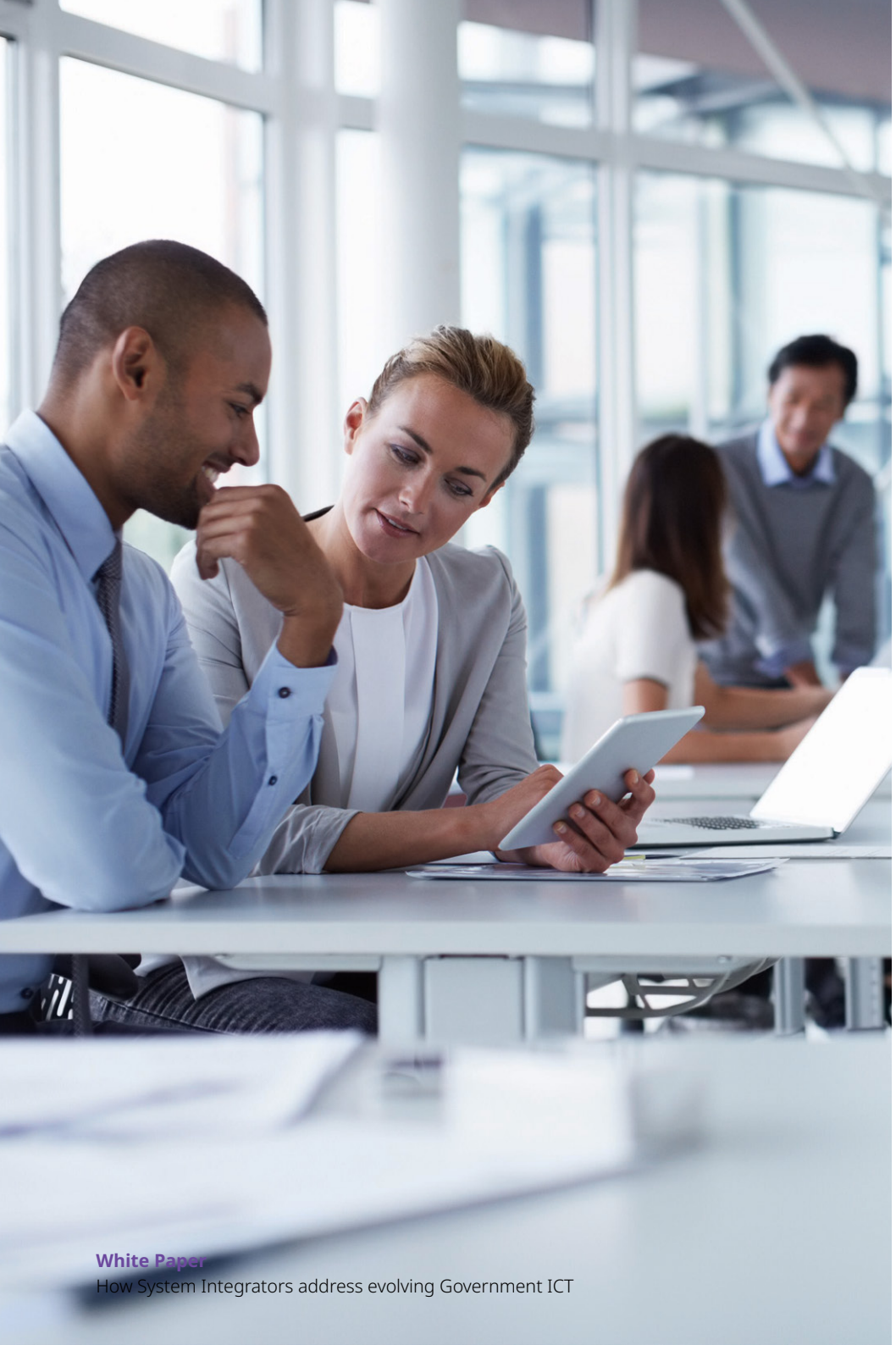
4. Zero trust security capabilities

Given the evolving cyberthreat landscape, traditional approaches to cybersecurity protection are no longer enough. Network architectures based on zero trust security principles are essential for any government network integration. Those architectures must be built with hardware and software products that can be configured through micro- and macro-segmentation to operate in a “Never Trust-Always Verify” mode. This will enable system integrators to deliver architectures that provide more granular control of user and device access to reduce the risk of potential attacks on the network.

5. Zero-touch provisioning

Ideally, network hardware and software should be engineered to streamline integration and deployment. Manual configuration of hardware elements can add significant time and cost to large-scale network deployments. Products and solutions that offer zero-touch provisioning can be integrated faster, with fewer errors, more efficiently.

Networking solutions that support zero-touch provisioning through automatic configuration can save integrators time and money during initial deployments, as well as future upgrades, enhancements and additions needed to accommodate more users, more office connections, and more coverage and capacity requirements.



6. Ease of management

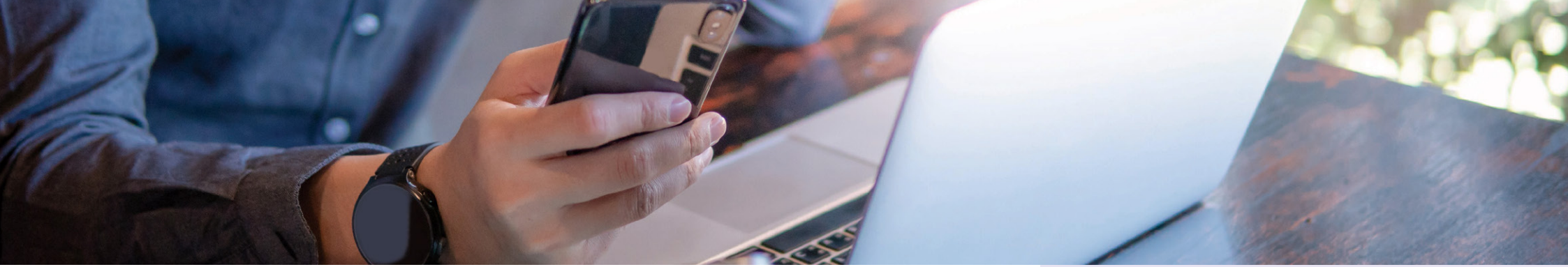
Of course, once a network is deployed it must be managed. In addition to zero-touch provisioning, integrators should select solutions that eliminate the need for multiple management systems for network resources in favour of a single system that provides a cohesive view across all network resources. With a single management system, integrators can provide government departments with rationalised and standardised visibility and control over all network elements, wherever they are deployed.

7. Supply diversity

Ultimately, more demanding RFP requirements and tighter government procurement budgets mean that integrators must deliver more functionality with every network integration while keeping a close eye on costs. To win government contracts and deploy optimal network architectures, integrators need products and solutions that can be configured and delivered quickly and maintained easily.

Given the variety of criteria that must be taken into consideration, integrators can't afford to limit their options when it comes to suppliers they partner with. The biggest supplier may not always be the best option and integrators should not settle for any networking option just because it's familiar. To win bids, integrators should offer the full potential of next-generation networks with highly secure, rugged and flexible networking solutions engineered to support the most complex requirements and deliver a higher return on investment.

Diversification is the shortest path to success. Through diversification, integrators can go beyond the obvious and leverage the significant benefits of best-of-breed networking infrastructure solutions that will optimise all ICT integrations. A supplier who offers the right balance of all the elements is the ideal choice. And the right supplier will offer the next-generation, fully customisable and hardened networking solutions needed for any government ICT requirement.



Streamline integrations

Government integration programs can be demanding on time, resources and budgets as these networks require more efficient and intelligent network infrastructures to support an ever-increasing number of users, complex applications and the tsunami of data they generate.

Alcatel-Lucent Enterprise simplifies government network integrations with standards-based communications, network and cloud offerings engineered to support any digital transformation and digital workplace initiative. Our completely customisable and easily managed network solutions go beyond proprietary, complex and costly networking options by providing more integrated and cost-effective offerings optimised to move data faster and more efficiently. And all our products provide enhanced security, reliability, and operational efficiency for every network integration without requiring integrators and their customers to get locked into complex, disintegrated, restrictive and costly hardware and software road maps.

Integrate flexible network solutions

With ALE, system integrators get maximum flexibility through open architecture solutions and open Restful APIs. This simplifies the integration of all elements into existing government infrastructures and ensures backwards and forwards compatibility with no additional fees, right out of the box.

Our networking products and solutions go beyond supply chain and network security standards with:

- **Integrated security features** that go above and beyond current security practices and standards to ensure the security of all hardware and software verified by third-party validation of the underlying code
- **Security with privacy by design** built on a zero trust framework with all relevant data privacy certifications

The ALE portfolio of networking solutions includes:

- Alcatel-Lucent OmniSwitch 9900 Modular LAN Chassis B, a high-density, multi-terabit, resilient, SDN-ready platform for connectivity needs from the edge to the core
- Alcatel-Lucent OmniSwitch 6900 Core and Data Center Network Switch for top-of-rack LAN and data center deployment in a compact and high-density form factor with 10 Gigabit Ethernet (GigE), 25 GigE, 40 GigE and 100 GigE options
- Alcatel-Lucent OmniSwitch 6860 Stackable LAN Switch, a high-density, unified access communications switch with Smart Analytics
- Alcatel-Lucent OmniSwitch® 6865 Hardened Ethernet Switch for superior performance in mission-critical applications running in harsh environments or extreme temperatures

Choose an experienced solutions provider

ALE networking solutions go beyond basic speeds and feeds technology specifications to provide quantifiable business benefits for ICT network integrations:

- **Move from design to deployment and revenue faster** with network hardware and software that is easily deployed, field-upgradeable and fully scalable
- **Reduce network integration and deployment costs** with zero-touch provisioning that enables automated setup and configuration for any platform
- **Increase short- and long-term margins** with network integration and deployment models structured to eliminate vendor lock-in and enable full customisation for any platform
- **Simplify network management** with a single management system that manages the entire network right out of the box
- **Reduce integration time** with the only hardened switches available with shortest path bridging (SPB) technology
- **Do more with less** by leveraging multicast capabilities, SPB, and wire-rate speeds that provide a network infrastructure optimised for any deployment
- **Eliminate costly legacy network switches** with more efficient and cost-effective hardware that meets and exceeds existing capabilities

Our partnership approach, exceptional professional services and track record delivering ICT solutions for local, national and federal government departments has made us a trusted partner for system integrators around the world.

Learn more

Contact us to find out how we can help with your next government network integration.

https://www.al-enterprise.com/en/industries/government

Alcatel·Lucent
Enterprise