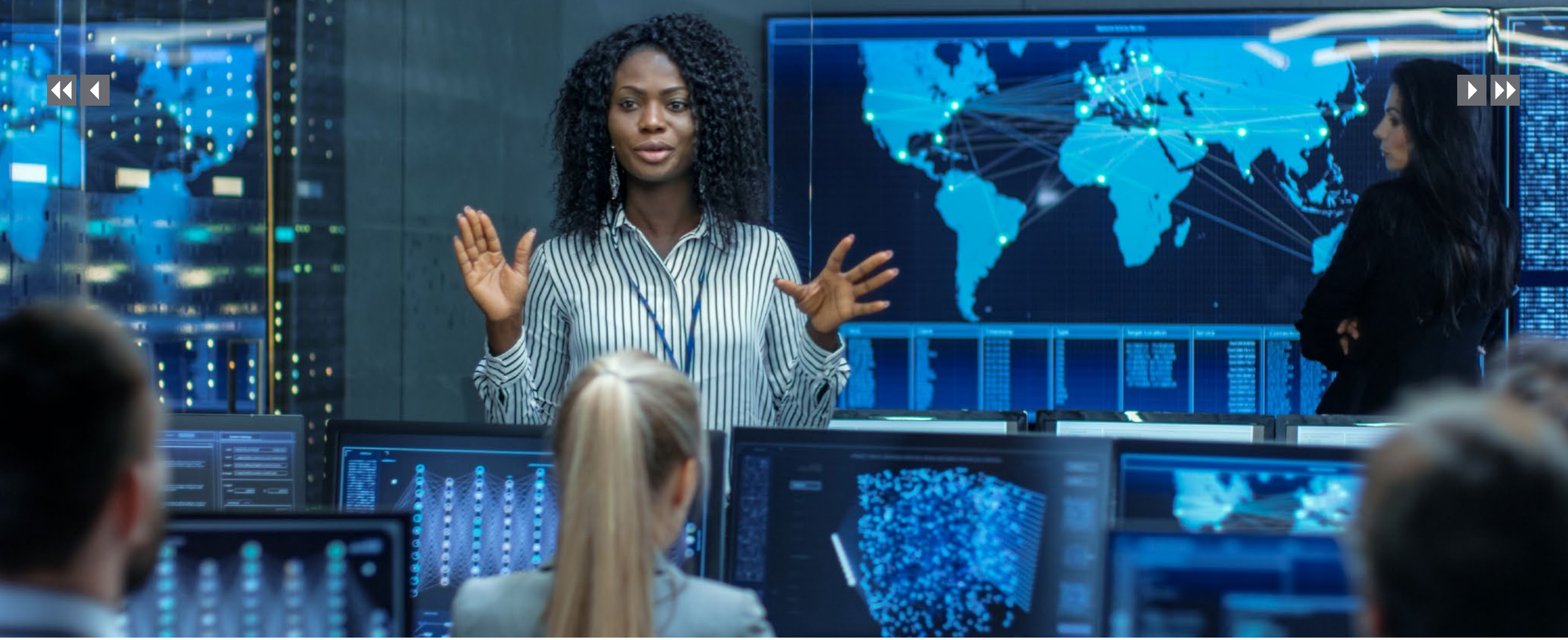
Top security practices for resilient government

Leveraging Information and Communications Technologies

Alcatel·Lucent
Enterprise

eBook

Table of contents



Overview

With growing global challenges and increased cyber and physical risks, governments must prioritise risk management, safeguard critical infrastructure and protect citizens. According to CloudSek cyberattacks against the government jumped 95% in 2022.[1] The expectation is that government business continues whatever the situation and that citizens 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.

Public sector and why Information and Communications Technology (ICT) is more critical than ever

In recent years, digital transformation in the public sector has rapidly advanced, with an increasing number of citizens accessing digital services. Digital transformation has also enabled government employees to adopt a work-from-anywhere workstyle. There is growing pressure on governments to accelerate digital transformation further. According to a Deloitte article, seventy-seven percent of government agencies say that digital transformation initiatives pushed during the pandemic are already having a positive impact on their organisation.[2]

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 you can improve resilience and security, it is important to acknowledge the changing Information Technology, Operational Technology relationship. In the past, IT and Operations teams didn't collaborate closely, 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 organisation at risk.

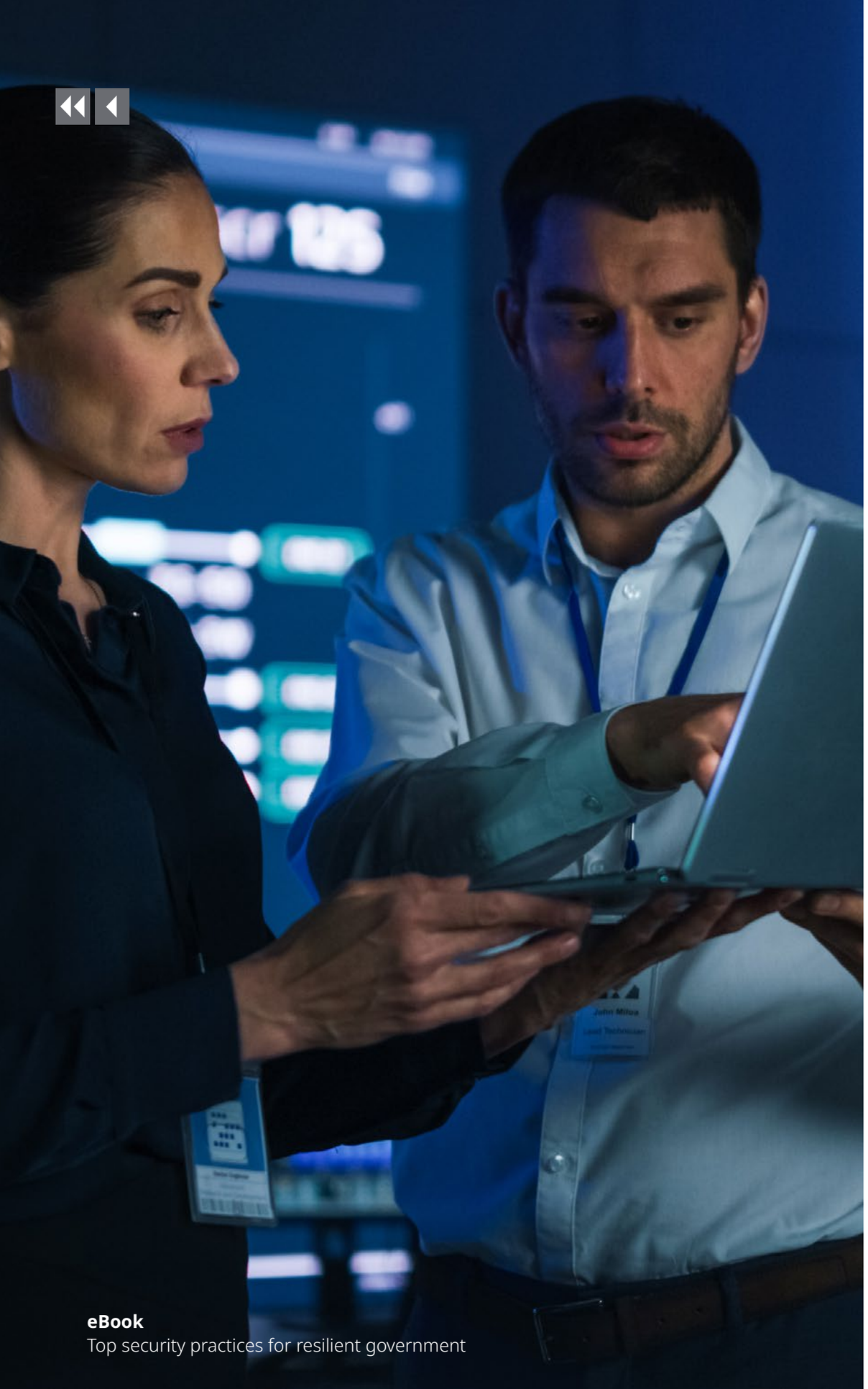
Let's consider, for example, the vast number of Internet of Things (IoT) devices that are rapidly being deployed in many government agencies and smart cities. When IT isn't aware of the operations team implementing new IoT devices, they can't ensure the devices comply with the organisation's security 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 unauthorised "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 government organisations as well as the provisioning of services for citizens. Due to the sensitive nature of the information contained in government networks and the critical services governments run, downtime or disruptions in network services can have severe consequences, making resilience and security the priority. Reliable and secure networks are essential for governments to deliver effective public services, protect sensitive information and ensure smooth operations.Resilient networks that embed security in the earliest stages of design with no additional licenses are an important requirement.

6 Best practices for choosing your network solutions

1. 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. Following a phased approach for micro-segmentation to ensure the proper implementation is needed to avoid disruptive organisational consequences.
2. Consider adopting a solution that leverages Shortest Path Bridging 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 containerised network.
3. 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 dedicated mesh, or ring interconnections. The virtual chassis presents a cost-effective solution to simplify network management while ensuring high availability.
4. A solution that 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 is a critical requirement.
5. Implementing 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 should be considered.
6. An enhanced security step is Secure Diversified Code that randomises the location of different segments of code on your switches, dramatically increasing security. In addition, an independent verification and validation (IVV) process, conducted by a third-party cybersecurity expert that analyses and tests the Operating System to identify and eliminate any potential vulnerabilities, backdoors, malware, or system exploits increases security further.



eBook
Top security practices for resilient government

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 ensuring you get the security and resiliency your organisation requires:

- Prior to investing, ensure your network design is consistent with your organisational requirements, and identify any critical and sensitive areas which may have changed from previous network designs. For critical areas, consider adding backup servers and multiple connections where possible and applicable.
- Consider the increasing importance of incident response time, for example we use Artificial Intelligence (AI) and Machine Learning (ML) capabilities for our 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. Ruggedised Ethernet switches are specifically designed to excel in challenging environments and extreme temperatures. These switches are built with ruggedised components and housed in sturdy enclosures, ensuring durability and reliability with a common Operating System, reducing the TCO of managing multiple operating systems. To enhance security and protect sensitive information, some models of switches are equipped with intrusion alerts and alarm relays that enable the connection of external alarm systems. Some models even support MACsec for secure data communications between the two ends. With Virtual Chassis capability in ruggedised switches, you can gain improved redundancy, resiliency and scalability.

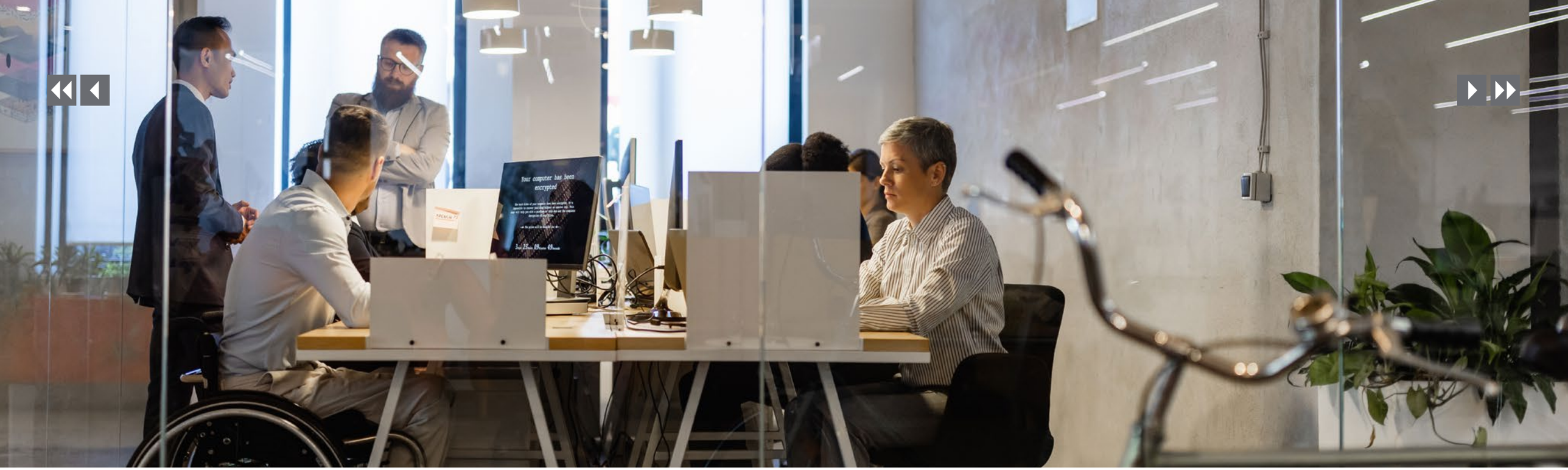
Resilient and secure communications solutions

Communications are crucial for governments to interact with citizens, stakeholders and other government agencies, as well as for the dissemination of important information. Communications systems must be available in times of crisis, when citizens need government assistance most. Resilience and security are constantly evolving, and it is important to keep up to date with emerging cyber security practices.

Best practice is secure-by-design. That means considering security during every step of product definition, development and delivery. All hardware and operating systems should be hardened, with Denial of Service (DoS) protection built in. When choosing your communications solution, ensure that they comply with recognised certifications and accreditations for global security and privacy standards (ISO 27001, ISO 27017 and ISO 27018). As well we 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 European Union.

6 Best practices for your communications solutions

1. Ensure that you have automated remote system backup to avoid configuration data loss.
2. Consider a solution that includes alarm monitoring but remember to ensure it is regularly updated with the right thresholds. Additionally, verify that notifications for communication system failures or quality alerts are being 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, the voice from other traffic reduces the chance of contamination which could disrupt operations and potentially government services.



Invest in resilient and secure communications solutions

Over the last few years, the global environment has shone a light on the importance of government-citizen communications. Following are some key areas to consider for government agencies planning to invest in communications solution to ensure resiliency and security.

- Redundant and resilient architecture. Your architecture should be fully redundant and resilient. Duplicating call servers in critical areas, implementing remote site redundancy and duplicating critical application servers can provide additional protection.
- Create a workflow with automatic triggers (trigger being human, IoT or system) to notify key people of system issues so they act quickly and speed up the recovery process
- Deploy strong encryption based on industry standards, that is native to the solution, and does not have any impact on voice quality and performance
- Implement a collaborative tool to complement your communications solution with a comprehensive set of features including voice, video and instant messaging, empowering seamless communications and efficient collaboration. The tool should be capable of exchanging images, videos and video surveillance feeds, enhancing contextual awareness and enabling better decision-making. Ideally, the tool should provide hybrid communications with secure connectivity between on premises and cloud. It ensures resilient communications, keeping you connected to colleagues and customers, 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 ultimate resiliency to keep communications open.
- For agencies with more stringent security requirements. An on premises alternative with a private cloud instance should be considered. It is important that the instance can be hosted in any data centre, providing complete control over servers, storage and networks, empowering agencies to customise and configure the infrastructure according to their requirements. It is a critical requirement that personalised security policies can be implemented, and resources can be managed autonomously. This level of control provides complete visibility and authority over the infrastructure, enabling agencies to make informed decisions and optimise performance in alignment with their objectives.

Protecting people and assets

Governments also need to consider safety of people and assets, the availability of flexible, secure and highly available real-time communications and notification systems is an important requirement. These solutions can integrate with public safety or smart city control centre operations, streamlining call dispatching and prioritisation, facilitating contextual information exchange with IoT data, and enhancing collaborative efforts among first responders and various stakeholders enabling improved decision-making and coordination.

The ability to interconnect IoT devices within buildings, venues and cities, combined with analytics and AI, is fundamentally transforming the communications landscape. Through the integration of sensors, video surveillance, workflow and AI, the shift from a reactive to proactive approach is possible, enhancing process efficiency in terms of time and cost. This integration facilitates a comprehensive understanding of the context, supports decision-making processes, and subsequently reduces emergency response times. Additionally, functionalities like Asset Tracking and control of smart locks and lights streamlines operations. Furthermore, 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 ruggedized network switches which can seamlessly integrate into your ecosystem and withstand harsh environmental conditions, including limited airflow, shocks and extreme weather temperatures. Opting for ruggedized equipment ensures longevity in such challenging locations where non-rugged equipment would be less durable.

In the field of physical security systems, the stakes are high. Each minute and every piece of video footage could be crucial for authorities in identifying wrongdoing, pinpointing the source of an incident, or understanding the cause of a disaster. A robust video surveillance infrastructure is essential. The 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. The operations team should be capable of promptly resolving any video issues, particularly in environments where every video frame is critical. Alcatel-Lucent OmniSwitch® solution integrations, accomplished through plugins with major video management systems, enable you to achieve this vital objective.

Furthermore, there are situations where asset tracking or locating individuals or equipment within your organisation becomes necessary. An effective asset tracking solution relies on its ability to 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 an asset tracking solution, staff and equipment can be located quickly and shown on a floor plan map. Asset tracking also provides information about usage patterns, knowing if assets are over utilised or underutilised can provide valuable information.

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 unauthorised activities
- Execute highly specialised, security-specific tests, such as penetration tests, on our products
- Ensure our products achieve key industry certifications, such as HDS (securing personal health data), HIPAA, and the Family Educational Rights and Privacy Act (FERPA)

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.

ALE certifications

ONGOING CERTIFICATION

UNDER RENEWAL

DID23091202EN (October 2023)