Security and resilience practices for modern organizations

Leveraging information and communications technologies

Alcatel·Lucent Enterprise

eBook

Table of contents

Overview

With growing global challenges and increased cyber and physical risks, organizations must prioritize risk management and safeguard critical infrastructure. The expectation is that business continues whatever the situation. In today's global climate, it's more important than ever to maintain data security, protect data sovereignty and ensure service availability.

eBook
Security and resilience practices for modern organizations

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 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.

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. However, we are now seeing the emergence of IT/OT collaboration to ensure network security and resiliency.

Resilient and secure network solutions

A resilient and secure network infrastructure is integral to the functioning of organizations. Downtime or disruptions in network services can have severe consequences, making resilience and security the priority. 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 organizational consequences.
2. Consider adopting a solution that leverages Shortest Path Bridging to achieve redundancy by dynamically rerouting traffic using multiple paths in the event of a path failure. It also creates an efficient and automatically containerized network.
3. Consider leveraging virtual chassis capabilities to enhance reliability in critical areas, as this enables redundancy and resiliency for your network, supports in-service software upgrades (ISSU) and allows 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 you have all configuration backups from network switch, 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.
6. An enhanced security step is secure diversified code that randomizes the location of different segments of code on your switches, dramatically increasing security. An independent verification and validation (IVV) process, conducted by a third-party cybersecurity expert that analyzes and tests the operating system to identify and eliminate any potential vulnerabilities, backdoors, malware or system exploits increases security further.

eBook
Security and resilience practices for modern organizations

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 time-consuming. Before you get started, here are some key areas to consider to ensure you get the security and resiliency your organization requires:

- Prior to investing, ensure network design is consistent with your organizational 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 iincident response time. For example, ALE uses 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 by identifying sudden changes in network behavior.
- Consider hardened switches for harsh environments. Ruggedized Ethernet switches are 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 with a common operating system and reducing the TCO of managing multiple operating systems. To enhance security and protect sensitive information, some 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 ruggedized switches, you can gain improved redundancy, resiliency and scalability.

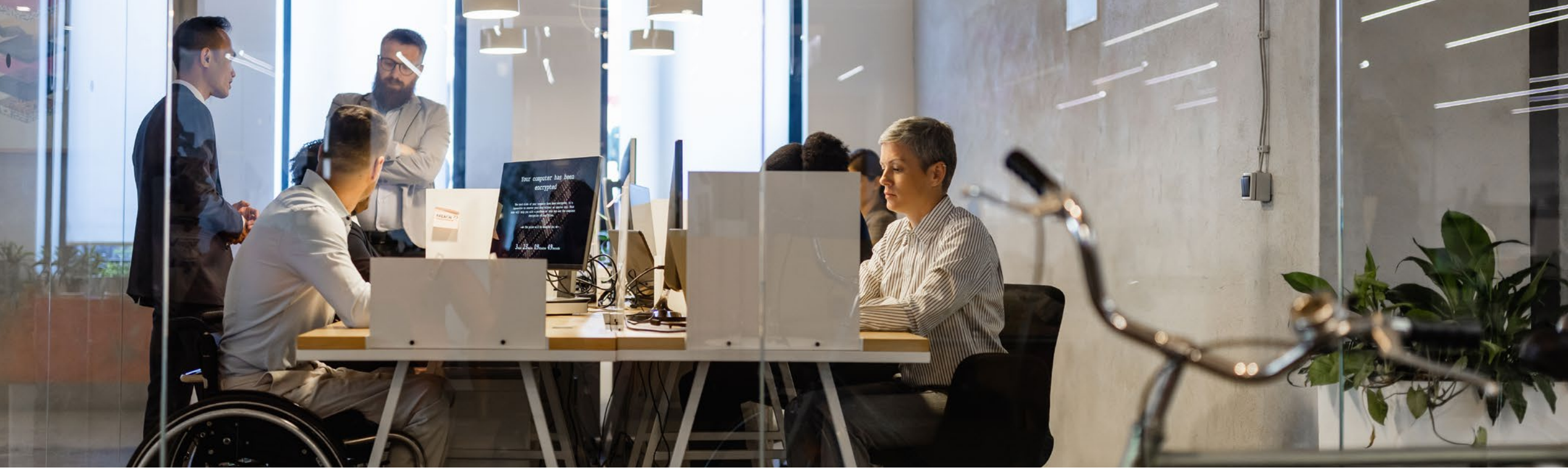
Resilient and secure communications solutions

Communications systems must always be available. Resilience and security are constantly evolving, and it is important to keep up to date with emerging cybersecurity 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 it complies with recognized certifications and accreditations for global security and privacy standards (ISO 27001, ISO 27017 and ISO 27018). ALE adheres 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

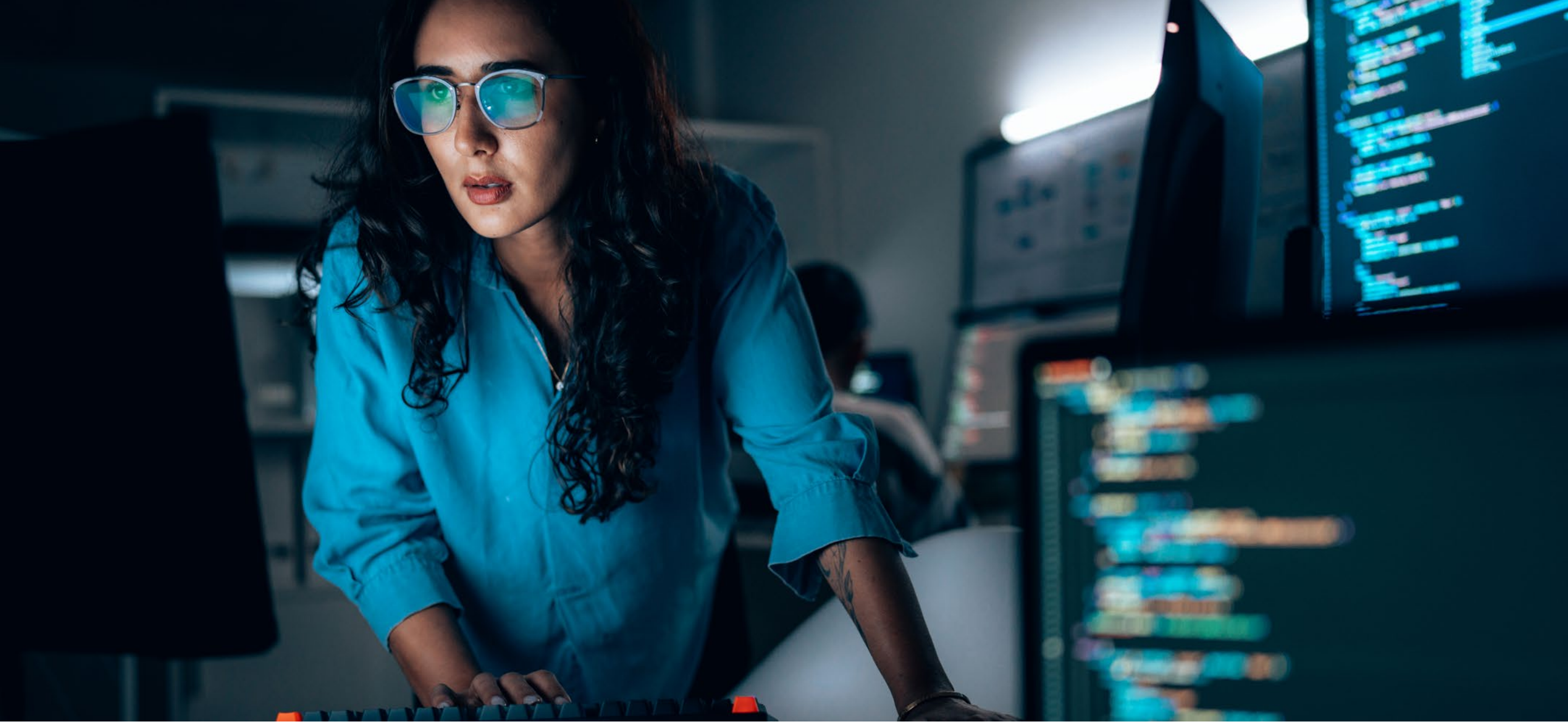
1. Ensure you have an automated remote system backup to avoid configuration data loss
2. Consider a solution that includes alarm monitoring, but remember to ensure it is regularly updated with the right thresholds. Additionally, verify that notifications for communication system failures or quality alerts are 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 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 communications in any organization. The following are some key areas to consider for investment in communications solutions to ensure resiliency and security.

- 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 (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. This 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 improved resiliency.
- For organizations 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 center, providing complete control over servers, storage and networks and empowering agencies to customize and configure the infrastructure according to their requirements. It is a critical requirement that personalized 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 optimize performance in alignment with their objectives.



About Alcatel-Lucent Enterprise

Alcatel-Lucent Enterprise is one of the world's leading networking, communications and cloud solutions providers. With flexible business models in cloud, on premises and in hybrid environments, our technology connects everything and everyone.

We bring together our fully converged cloud, communications and network portfolio and partner ecosystem with a holistic security approach to optimize effectiveness for organizations of all kinds. We meet the IT and operational requirements of verticals such as government, defence, healthcare, education, transportation and energy and utilities who have rigorous specifications for cyber and physical security, privacy and public safety.

By leveraging automation and built-in security features, we simplify the creation of efficient and compliant digital infrastructure with products and solutions configured to meet the highest global security standards.

If you would like to know more about Alcatel-Lucent Enterprise solutions, visit our website: **al-enterprise.com**.

Alcatel·Lucent
Enterprise