Keep your business secure when working remotely

Alcatel-Lucent Enterprise Chief Information Security Officer, Sebastien Roche, shares insights into ALE's approach to business continuity and security.

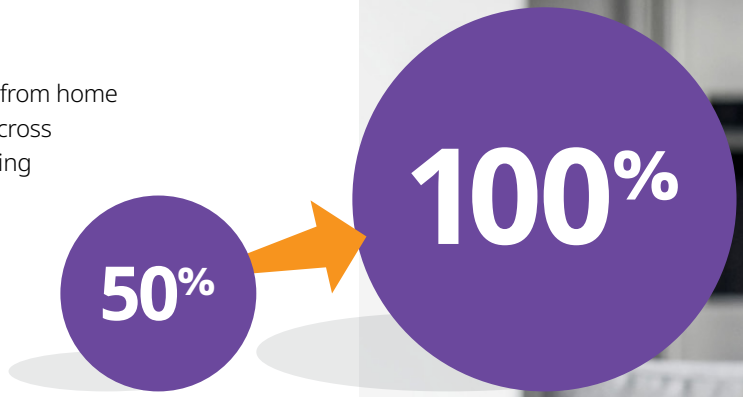
Brochure

Alcatel·Lucent
Enterprise

The new #WFH reality

Since 2020, companies that had not previously offered a work from home (#WFH) option have been challenged to transform their organisations to ensure business continuity and security.

More than 15 years ago, Alcatel-Lucent Enterprise initiated a work from home strategy embraced by more than 50% of the employees working across 50 offices worldwide. With more than half of ALE employees working from home, we already had the network and IT architecture necessary to support remote working. The challenge was really a question of how we would transition from 50% online workers to 100%.



Ready for action

For almost 10 years, ALE has embarked on an extensive IT transformation. A network architecture was adopted, which provided cloud security to proactively block threads, identify potential attacks and ensure secure access for employees.

The transformation included:

- Security in the cloud with virtual access points
- Real-time tracing
- Identifying unusual behaviour patterns to detect threats

Preparation = Agile response in crisis situations

When crisis struck, the decision was made on Friday afternoon to begin remote working on Monday. Employees were instructed to take their laptops and monitors home with them. On Monday morning, work began as usual with no interruption as employees started their day from their remote offices. The network transformation previously undertaken ensured secure remote connectivity regardless of an employee's location.

The access challenge

User profiles posed a significant challenge for our #WFH plan. In particular, the R&D and technical support teams require access to certain servers and development platforms, which our remote access solution did not allow.

When the effort to transition all employees to #WFH began, we adapted our infrastructure to increase our bandwidth to support the increase in the number of remote connections required by employees working from home.

Security is key

Security and enterprise data protection are extremely important in uncertain times and affect many organisations handling sensitive data, such as public-sector organisations, ministries, cities and towns.

Before we even started talking about #WFH at ALE, we deployed a distributed and secured infrastructure as well as a fully cloud-based private connection solution for all employees to ensure secure remote access to the network. We maintained the legacy VPN solution for a small number of teams who had specific needs, such as connecting IP phones in their remote offices. We also provided employees with professional PCs that could manage automatic software downloads and updates.

Close the door on security breaches

As expected, during extensive remote working, there has been an increase in calls and emails regarding suspicious emails and requests for password updates. We have also seen a spike in phishing attacks as well as targeted attacks on vulnerable software.

While the use of proxies protects ALE from major cybersecurity issues, we still see new breaches every day from emails, downloads and non-updated software/OS versions.

Keep communications open

At ALE, we keep a continuous virtual link with the ALE teams. We communicate on a regular basis, share tips and best practices and ensure that our team is available to support all employees.

ALE checklist for secure remote working:

- Do not allow or encourage the use of personal devices (PCs) for professional data exchange and communications
- Enable private and secure access for employees
- Automate software upgrades throughout the enterprise network
- Pay attention to suspicious email requests
- Use certified software. Audits and certifications provide software security authentication.
- Simplify your decision-making processes. In emergency situations, a CISO or CIO needs to make decisions quickly to address issues in order to ensure services continuity.

Six ALE recommendations for secure remote connectivity

1. Automate password change reminders

Help employees change corporate passwords before they expire. Prior to the expiration, employees should receive a daily email with instructions inviting them to change the password.

2. Enable data backup in the cloud

Allow and encourage employees to save their data regularly to avoid any loss in the event of an issue with their laptops. Enable data backup storage spaces and offer remote assistance through an IT Service Desk or IT specialists.

3. Remind employees about device protection best practices

Keep your laptop in top condition:

- Turn off the laptop at the end of every day (avoid sleep/lock mode)
- Keep laptops away from heat sources (such as the sun or heater)
- Avoid eating or drinking next to laptops
- Secure cables away from kids and pets

4. Security first

Educate teams about risks and security best practices:

- Encourage employees to think twice before clicking on links in emails, even when it looks like it was sent by someone familiar
- Offer IT follow-up in case of doubt
- Provide reporting tools for suspicious emails
- Use gamification to create a security-first culture: At ALE, we used gamification to encourage employees to detect and report suspicious emails

5. Communicate

Isolation makes people vulnerable to cyber attacks. Find ways to keep your teams connected:

- Organise regular updates, virtual meetings, events, collaboration spaces, happy hour
- Encourage people to connect regularly with their teams
- Send regular emails to let employees know the IT team is available to help and remind them about security best practices

6. Encourage healthy connectivity habits

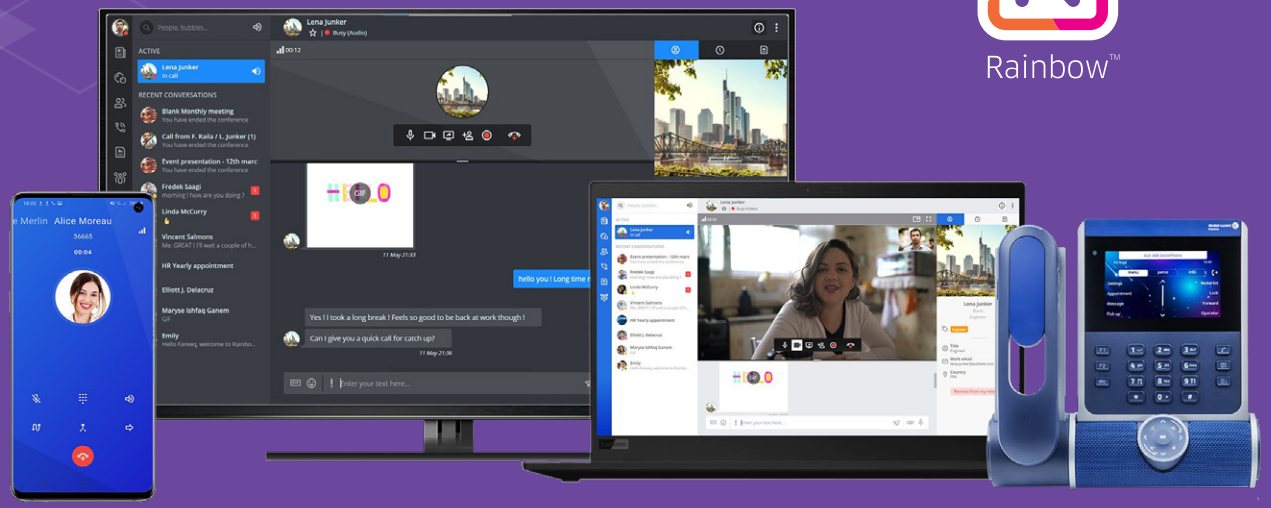
The risk with remote working is a 12-hour workday with continuous connectivity or back-to-back meetings. Encourage employees to have screen-free and disconnection times and to spend time with family or outdoors.

Rainbow™ by Alcatel-Lucent Enterprise for connected collaboration

Rainbow: A cloud team collaboration platform for chat, video and audio calls, as well as for screen and document sharing provides ALE employees with the services they need to stay connected. The platform is used extensively by all employees to collaborate with colleagues, customers and business partners and is connected to the telephone system for external calls.

In addition, our partners and customers have also adopted Rainbow as their collaboration solution of choice. Rainbow addresses the security requirements of public sector, defense, healthcare and other specific sectors and is compliant with strict security regulations including GDPR and HDS, among others. Rainbow is certified ISO 27001 and CSPN by ANSSI.

Rainbow™



Brochure
Keep your business secure when working remotely

Working remotely in complete safety

While organisations are allowing more employees to work remotely, analysts confirm the increased risks of cyber attacks.

At ALE, we use the communication and collaboration applications and services that we deploy for our customers. These solutions are developed with cybersecurity in mind, whatever the conditions of use – in the office, remotely or on the move. The best guarantee we can give our customers, apart from the fact that these solutions are certified by international security agencies and comply with current regulations, is that we use them everyday with complete confidence for thousands of ALE employees around the world.

Visit our website for more information.

DID20060201EN (April 2024)

Alcatel·Lucent Enterprise