Keep your business secure when remote working is required

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

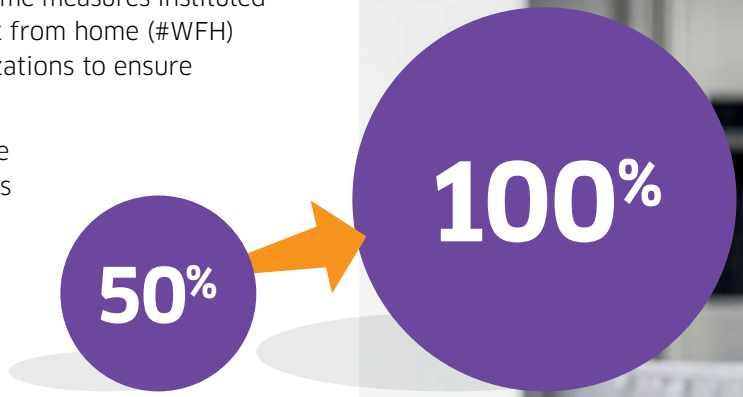
Brochure

Alcatel·Lucent Enterprise

The new #WFH reality

With the recent international health crisis and the stay-at-home measures instituted globally, companies that had not previously offered a work from home (#WFH) option are now being challenged to transform their organizations to ensure business continuity and security.

In 2008 Alcatel-Lucent Enterprise initiated a work from home strategy embraced by more than 50% of the 2,000 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

In the three years prior to the recent healthcare crisis, ALE had embarked on an extensive IT transformation. A Service Defined WAN 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 behavior patterns to detect threats

Brochure
Keep your business secure when remote working is required

Preparation = Agile response in crisis situations

The decision to begin remote working on Monday was made on the previous Friday afternoon. 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 where employees were located.

The access challenge

One of the major challenges we faced was with user profiles, including the R&D and technical support teams, who have specific needs to access certain servers and development platforms, which our remote access solution did not allow. These employee user profiles passed through a different private access solution than the rest of the teams.

When the effort to transition all employees to #WFH began, we adapted our infrastructure to increase our bandwidth and be able 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 organizations handling sensitive data, such as public-sector organizations, 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 percentage of the teams who had specific needs, such as connecting IP phone sets in their remote offices. We also provided employees with professional PCs, with the ability to manage automatic software downloads and updates.

Close the door on security breaches

As expected, during this period of 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 or from non-updated software/OS versions.

Keep communications open

During this challenging time we have kept 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 need 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 will 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 and IT Service Desk or IT specialists as necessary.

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:

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

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.

Alcatel-Lucent Rainbow™ for connected collaboration

Rainbow: a cloud collaboration platform for chat, video and audio calls, as well as for screen and document sharing provides ALE employees with the tools they need to stay connected. During this #WFH time the platform has been used extensively by all employees to collaborate with colleagues.

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, ISO 27001, HDS, among others.

Rainbow™

Brochure
Keep your business secure when remote working is required

Supporting our community

As part of the Business Continuity campaign, ALE has offered hundreds of thousands of licenses free of charge to support enterprises, cities, and governments to help them maintain continuity of services. In addition, to address the surging demand, as well as surging number of users, we have extended our cloud hosting capacity.

For more cybersecurity best practices check out the EU Cybersecurity Agency recommendations.

We are Alcatel-Lucent Enterprise.
We make everything connect by delivering technology that works, for you. With our global reach, and local focus, we deliver networking and communications.
On Premises. On Hybrid. On Cloud

Alcatel·Lucent
Enterprise