Securing unified communications and collaboration solutions

What it takes in today's changing world

White Paper

Alcatel·Lucent
Enterprise

Table of contents

A stronger focus on cybersecurity

Over the course of the last few years, almost every enterprise and government organisation has changed the way its employees communicate, collaborate and share information. While the rapid shift to support employees working from home was crucial to maintain business continuity during the pandemic, it came with a price: The network perimeter now extends well beyond traditional office boundaries, significantly increasing the organisation's attack surface.

The risks associated with extended network perimeters aren't going away any time soon. According to Gartner, 39 percent of knowledge workers globally will work in hybrid remote and in-office models by the end of 2023. In the U.S., that number rises to 51 percent[1].

Geopolitical disruptions have further increased cybersecurity risks. The European Union Agency for Cybersecurity has called Russia's invasion of Ukraine a "game changer" for the global cyber domain.[2] According to the Association of Ukrainian IT Outsourcing Companies, one in five Fortune 500 companies relied on software developers in the country in 2022.[3]

At the same time, the societal impact of cyberattacks is increasing. In 2022, we saw major cyberattacks on critical civic infrastructure, causing a national emergency in Costa Rica,[4] and continued targeting of healthcare organisations.[5]

Organisations can't afford to delay cybersecurity improvements

Cybercrime is estimated to have cost the global economy €5.5 trillion in 2021 with damages expected to surpass €10 trillion by 2025.[6] The problem is so severe, the European Union is creating a Cyber Resilience Act and has issued a significantly enhanced version 2 of its Network and Information Security (NIS) Directive to safeguard consumers and businesses that buy or use products or software with a digital component.[7] The U.S. is also implementing measures to strengthen cybersecurity, including Executive Order 14028, which encourages agencies to adopt zero trust cybersecurity principles and adjust network architectures accordingly.[8]

As enterprises and governments look to digitally transform and more permanently support flexible work models, they have no choice but to strengthen cybersecurity. The solutions their teams use to communicate, collaborate and share information must incorporate best practices in cybersecurity at every level and across every aspect of functionality.

1 Gartner Forecasts 39% of Global Knowledge Workers Will Work Hybrid by the End of 2023. Gartner, March 2023.
2 Volatile Geopolitics Shake the Trends of the 2022 Cybersecurity Threat Landscape. European Union Agency for Cybersecurity. November 2022.
3 One in Five Fortune 500 Companies Rely on Ukraine for their Software Development Needs in 2022. Ukrainian Hi-Tech Initiative, October 2022.
4 The 13 Costliest Cyberattacks of 2022: Looking Back. Security Intelligence. December 2022.
5 2022 In Review: An Eventful Cybersecurity Year. Forbes, December 2022.
6 New European Union cybersecurity proposal takes aim at cybercrime. World Economic Forum, September 2022.
7 EU Cyber Resilience Act. European Commission, September 2022.
8 Executive Order on Improving the Nation's Cybersecurity. Cybersecurity & Infrastructure Security Agency.

Six key areas for end-to-end cybersecurity

Unified communications and collaboration solutions must implement cybersecurity end-to-end because it's the only way to ensure security is applied in an exhaustive way. An end-to-end approach to cybersecurity helps enterprises and governments:

- **Prevent cyberattacks** by implementing cybersecurity in every aspect of product design to reduce the attack surface
- **Protect against cyberattacks** by implementing the latest security standards and best practices in all solution components to increase resistance
- **React to cyberattacks** by taking swift and appropriate actions to limit impact and improve resilience, should an attack occur

To determine whether unified communications and collaboration solutions implement cybersecurity end-to-end, solution evaluations in the areas described below, should be undertaken. Focusing on these areas can help ensure solution assessments are comprehensive while targeting key vulnerabilities across the cyberthreat landscape.

1 Secure-by-design

Historically, most solution designs were driven by the need for new features, and security was an important, but secondary, consideration. With the changing landscape, traditional design priorities have reversed and solution designs must now be driven by cybersecurity requirements.

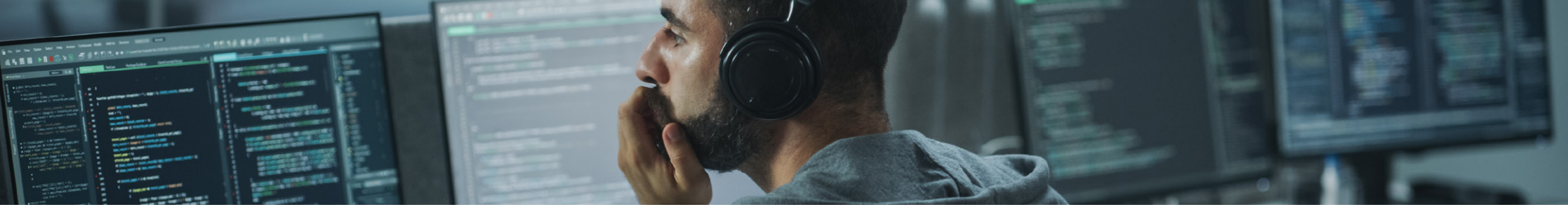
Hardware and software solutions that are secure-by-design take security into account during every step of product definition, development and delivery. All hardware and operating systems are hardened, Denial of Service (DoS) protection is built-in, and solutions implement the best practices in cybersecurity that are most important for the industry. For example, a unified communications and collaboration solution for homeland security organisations will meet the very high resilience and confidentiality standards these organisations require.

2 Zero Trust Network Access security

Security strategies that provide trust based on a user's location inside the corporate firewall, the credentials they enter, or the application or device they're using are no longer adequate — even when multiple security mechanisms are combined. Today, no user, device or application should have implicit trust.

Unified communications and collaboration solutions that implement a Zero Trust Network Access (ZTNA) security model help organisations effectively counter ever-evolving threats. ZTNA provides no trust to any user, device or application, no matter where it is located. It is based on five key assertions:

- The network is hostile
- External and internal threats are always present
- Location and identity are not enough to determine trust
- Every device, user and network flow must be authenticated and authorised
- Network and security policies must be dynamic and use as many data sources as possible



3 Macro- and micro-segmentation

Macro- and micro-segmentation enable a granular and highly controlled approach to cybersecurity for all the different users, devices and applications that access the network.

Macro-segmentation segregates users, devices and applications according to their functional domain so they cannot communicate with the elements in other macro-segments. For example, the unified communications and collaboration applications in one macro-segment cannot communicate with the security technologies, such as CCTV cameras and door-lock systems, in a second macro-segment or the sensors and controls for lighting, heating and air conditioning in a third macro-segment.

Micro-segmentation defines how the users, devices and applications within a macro-segment can interact with each other and is typically governed by very specific security policies. For example, a surveillance camera should not be allowed to interface with a door lock, despite the fact they are in the same security-related macro-segment.

4 End-to-end native encryption

In modern organisations, employees, customers, partners and suppliers can be located anywhere in the world. And the solutions they use to communicate and collaborate may be installed in the building they work from, on the other side of the city, or in a data centre on the other side of the world. In every case, people must be able to securely and confidentially exchange information using voice, video and text.

To ensure only conversation participants can access the information being exchanged, every conversation must be fully encrypted from origin to destination. That means each hardware and software element involved in the end-to-end communications must have encryption mechanisms that are approved by security agencies built natively into them.

5 Security and privacy certifications and accreditations

Just a few years ago, the most stringent security certifications and accreditations were only required for security products, such as firewalls, or in particular industries, such as defense. Today, security-specific standards must be applied to all technology products, across all industries.

It's extremely important to verify that cybersecurity claims are backed up by recognised certifications and accreditations. Here are a few examples of compliance to look for:

- **Global security and privacy standards**, such as ISO 27001 for information security, ISO 27017 for safer, more secure cloud-based environments, ISO 27018 for protection of personally identifiable information in cloud-based environments, and Common Criteria Evaluation Assurance Level (EAL) 2 and higher for computer system security
- **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
- **Regional security and privacy standards**, such as the General Data Protection Regulation (GDPR) in the European Union

6 Continuous, specialised security testing

Like security standards, specialised security testing processes that were once reserved for security products are now mandatory in unified communications and collaboration solutions.

Penetration tests are a prime example. These tests simulate cyberattacks to reveal security vulnerabilities so they can be proactively addressed before issues arise. To stay ahead of cyberthreats in an ever-evolving landscape, penetration tests that are driven solely by cybersecurity requirements must be performed on an ongoing basis.

Technology providers who are dedicated to helping their customers maintain maximum cybersecurity must provide the resources, tools and expertise needed to perform continuous penetration testing.

Achieve business goals with fewer risks

Unified communications and collaboration solutions that implement the complete range of cybersecurity measures described in the previous section give enterprises and government organisations the freedom and flexibility to drive activities forward while minimising risks and ensuring compliance. They can:

- **Empower employees** to securely and confidentially collaborate and share information using any media and any device, from any location
- **Improve the customer experience** with enriched, informative and engaging communications, faster decision-making, automated business processes and the ability to proactively detect issues before they affect the customer
- **Increase operational excellence and agility** using digital infrastructure that's deployed where it makes the most sense for their organisation — on premises or in a hybrid, private or public cloud — while adhering to strict data privacy policies and ensuring compliance with data privacy regulations

The examples below highlight just a few of the opportunities that become possible and can easily be adapted for other requirements and industries.

Create a flexible, digital workplace to empower employees

With the right mix of secure communications and collaboration solutions, employees can work in faster, more flexible ways while maintaining full compliance with industry regulations.

- **In healthcare,** a highly mobile workforce can collaborate and share information while remaining fully compliant with data security standards. Staff can easily exchange updates and quickly get the assistance they need. Medical staff can use secure, real-time communications to improve patient outcomes and workflow efficiency. Non-medical staff can accelerate processes and responses to maintenance issues that could affect patient and staff safety.
- **In education**, teachers can deliver richer and more engaging remote learning experiences with more opportunities for students to participate in activities, collaborate on projects, and interact using their preferred medium. Comprehensive access control and automated policies maintain data integrity, and analytics prioritise critical communications and network resources.
- **In government organisations**, staff can securely exchange information throughout dispersed teams. They can share screens, remotely control someone else's desktop and exchange large files to improve collaboration. And they can securely interact with citizens through web-based or mobile applications using voice, video, chat or instant messaging.
- **In transportation**, the digital workplace empowers employees to use their own devices while working, introduce more efficient processes, and provide passengers with enhanced services, such as the ability to work while they travel. Secure communications protocols, hardened installations and diversified code protect data everywhere on the network.

Connect everything to improve the customer experience

Securely connecting people, objects and applications with real-time communications allows enterprises and government organisations to:

- Give employees the devices, technologies and data they need to better support customers while minimising the risk that human error or lack of awareness will compromise security
- Use integrated, secure devices to communicate and collaborate with clients while on the move with full access to customer relationship management (CRM) solutions
- Increase protection, control and visibility over a fast-growing and diverse range of Internet of Things (IoT) devices
- Keep communications and collaboration systems up-to-date to avoid the risk that outdated applications will increase the attack surface and expose vulnerabilities
- Implement effective access controls and end-to-end encryption across all platforms

Unified network management allows all communications platforms, applications and IoT devices to be managed holistically. Unified network management:

- Simplifies management tasks across wired and wireless networks and IoT devices to reduce network management costs, optimise network performance and increase operational efficiency
- Accelerates troubleshooting across increasingly diverse technology environments to reduce the risk of service interruptions and downtime

Unified network management across industries provides a whole host of benefits. For example:

In healthcare, IoT solutions can track the location of critical equipment such as oxygen tanks, crash carts, patient monitors, IV poles and wheelchairs to improve safety and efficiency. The connections among people, objects and applications can also be used to trigger alarms that alert medical staff to patient needs, equipment malfunctions, and can alert everyone in the facility about unsafe situations.

In education, there's new potential to connect smart campus devices and applications with multiple layers of security to protect the institution's assets from under-secured devices that access the network. Educational institutions can also use IoT device fingerprinting to identify device characteristics such as type, manufacturer, model and operating system to simplify and accelerate IoT network setup and device onboarding.

Increase operational excellence and agility

With the flexibility to securely deploy unified communications and collaboration solutions on premises or in a hybrid, private or public cloud, enterprises and government organisations can benefit from digital technologies in the way that best aligns with their goals and mandate. Each organisation can achieve new levels of operational excellence while meeting industry-specific requirements by adopting cloud models for operational and agility improvements such as in:

- **Healthcare**, where digital records can be used to improve patient care and increase efficiency with full confidence personal information is being stored in a secure and certified data centre in the cloud
- **Education**, where faculty, staff and students have secure, privacy-sensitive access to cloud-based applications and services from anywhere. And IT departments can reduce the time and costs associated with deploying, supporting and upgrading the wide variety of applications.
- **Government**, where confidential communications can be supported with high availability and protected with built-in DoS mechanisms and security-hardened hardware and operating systems
- **Transportation**, where altering communications capabilities can create dangerous situations, making resilient, data sovereign solutions essential

Cybersecurity: Built into the technology provider's mindset

While many technology providers emphasise cybersecurity, not all have the comprehensive expertise to implement end-to-end security.

Alcatel-Lucent Enterprise goes above and beyond other providers to implement all the best practices required for end-to-end cybersecurity. We:

- Follow 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 of 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 all of our products
- Ensure our products achieve key industry certifications, such as HDS, HIPAA and the Family Educational Rights and Privacy Act (FERPA) like Rainbow by Alcatel-Lucent Enterprise.

As recognised cybersecurity experts, we contribute to European Union proposals for cybersecurity directives. We also leverage our expertise to help our customers choose and implement the right mix of secure unified communications and collaboration solutions for their needs and train their employees in cybersecurity best practices.

Alcatel-Lucent Enterprise is trusted around the world

Leading organisations across industries rely on our secure, Digital Age Communications solutions to achieve their goals, including:

- Metropolis and City of Perpignan in France, where government officials are implementing a strategic digital transition plan that includes videoconferencing and voice communications for employees, support for IoT applications, and new content and services for Perpignan residents, tourists and municipal employees.
- Newman University in the U.S., a Catholic liberal arts college that has provided staff with mobile phone capabilities that don't require direct phone numbers and the IT team with a single, intuitive, cloud-based platform to manage, provision and monitor all network infrastructure.
- Kingsway Hospitals in India, which has implemented real-time communications infrastructure solutions that keep clinical and administrative staff connected so they can optimise care delivery and improve the patient experience.
- J. Malucelli Group in Brazil, which has modernised its network with a converged voice and data solution that includes cloud telephony as well as LAN and Wi-Fi networks with cloud management to simplify and reduce the cost of communications for several of the companies within the group.

Learn more

To learn how we can help your organisation take full advantage of secure Digital Age Communications solutions, visit our website or contact us today.

Alcatel·Lucent Enterprise