Alcatel-Lucent Rainbow

Solution Brief – Security White Paper

Rainbow™
www.openrainbow.com

Alcatel-Lucent Rainbow™ is a cloud-based, enterprise-grade, Unified Communication as a Service hybrid cloud approach. Rainbow offers a global solution for collaboration and communications while addressing the specific needs of ALE's end-customers. Whether it is a small business requiring cost-effective mobility or a multinational organization that wants a single standard for unified communications across their complex IT, broad geography and business process environment - Rainbow can address their UC needs. Rainbow features a scalable cloud-computing UCaaS and CPaaS platform designed with high-availability and resilience in mind. Protecting ALE users' confidentiality, integrity and availability of their data while maintaining their trust and confidence is also a high priority.

Responsibility Model

The Rainbow infrastructure has been architected with security by design. It provides a scalable and reliable platform that enables customers to interface with, but also deploy custom applications, quickly and securely. ALE's infrastructure is built and managed according to the Cloud industry standards' security controls and policies such as OWASP. We make use of redundant and layered controls as well as continuous validation and testing. Plus, everything is automated to ensure the underlying infrastructure is monitored, reliable and secure 24x7x365.

ALE operates under a shared security responsibility model, where ALE is responsible for the security of the underlying Rainbow infrastructure and services, while letting our customers manage their respective security at the application layer, including connectivity to the Cloud, as well as their company and users' privacy rules, identities and access control management within the Rainbow realm, as presented in figure 1.

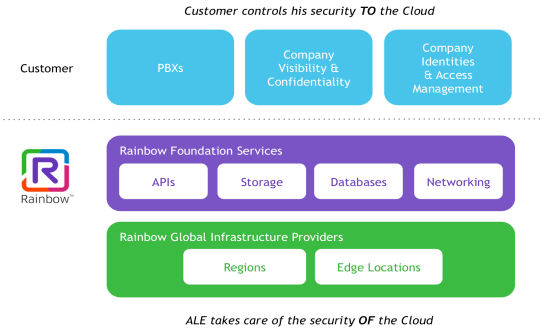
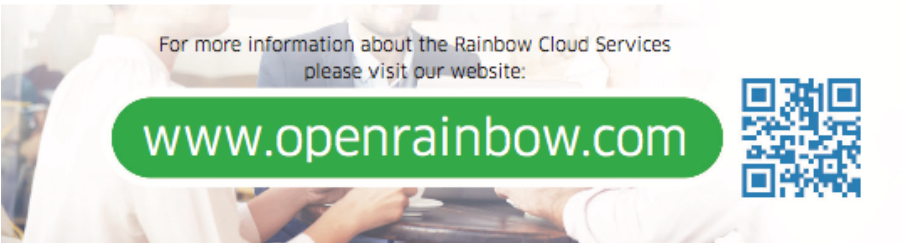


Figure 1: Rainbow Shared Security Responsibility Model

Physical and environmental security

Confidentiality of data in the infrastructure, integrity of the service content, and availability of data stored are ALE's top concerns. ALE is responsible for protecting the global infrastructure that runs all the services offered by Rainbow, including hardware, software, networking equipment and facilities that operates Rainbow services. Rainbow data centers rely on modern ISO-27001 and SOC certified technologies, being isolated with barbed-wire fences and physical access is strictly monitored 24x7 — both at the perimeter and building ingress points by professional security staff using video surveillance. Authorized staff receives a nominative RFID-controlled badge with recurrent reviews of personal accreditations.



Alcatel·Lucent Enterprise

Every data center room is fitted with a fire detection and extinction system as well as fire doors to prevent risks. The fire detection system uses smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms, complying with the APSAD R4 rule and N4 conformity certification.

Each data center electrical power system is designed to be fully redundant and maintainable without impact to operations, 24 hours a day, seven days a week, supporting 48 hours of initial autonomy to counteract any failure of the electrical supply network. An uninterruptible power supply (UPS) also provides back-up power in the event of electrical failure.

Our data centers rely on their own fiber optic network across the globe, providing a total network bandwidth capacity of up to 4.5 Tb/s in Europe and 8 Tb/s in North America. Proprietary Distributed Denial of Service (DDoS) mitigation techniques are used at the networking level to protect ALE services against various attacks, detected in a one second timeframe, filtering illegitimate traffic and hoovering it up to 4 Tb/s, while letting legitimate packets goes through with a 1 ms delay.

Geographies

Rainbow is architected to support multiple geographically isolated regions, to comply with legal regulations and provide its users with the best possible experience. ALE ensures data privacy at a regional level by guaranteeing users that their sensitive data will never be replicated across boundaries. Rainbow service is then distributed across regions to minimize service latency towards users, while guaranteeing data boundaries.

As of this writing, as represented in figure 2, user data is bound to seven key regions: North America, Caribbean and Latin America, Europe Middle-East and Africa (default), Germany, Asia-Pacific, Australia – New Zealand and Mainland China, with extended coverage in USA and Asia. ALE's primary data centers are in Canada, Brazil, France, Germany, Singapore, Australia and China. Secondary data-centers, hosting no data but acting as cache and media relays only, reside in the United States, South Africa and Japan. These locations offload the network infrastructure by providing Rainbow's users direct local access to static resources through an IP AnyCast mechanism. ALE also offers a dedicated datacenter for hosting of sensitive healthcare data.

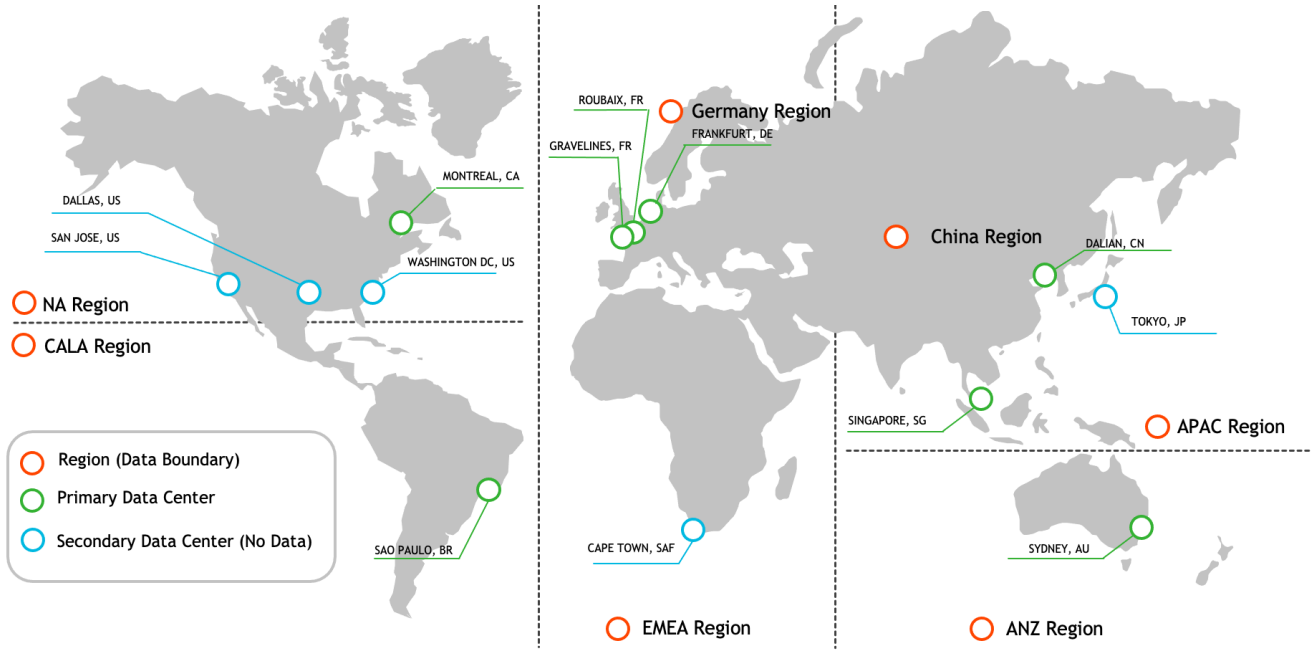


Figure 2: Rainbow Availability Regions

Alcatel·Lucent Enterprise

Business continuity

ALE has designed Rainbow to tolerate site, data-center, system or hardware failures with minimal customer impact. All ALE services are deployed in an N+1 redundant configuration to ensure no single point of failure (SPOF) and sufficient computing capacity to enable traffic to be load-balanced to the remaining servers in case of instance failures. All application requests are evenly distributed among internal and external load balancers. Databases and user-generated data all are multiple time replicated and backed up, region-wise, to ensure no possible loss. ALE adds up GeoDNS mechanisms and automatic failover support to cope with possible Internet routing issues and ensure user access to the closest point of presence. Rainbow's complete production infrastructure is automated to ensure a 100% reliable and reproducible deployment of the various components.

The Rainbow Customer Care and Operations teams employ industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents and to manage the impact and resolution. Internal communications methods are in place to ensure ALE Cloud Operations team employees understand their individual roles and responsibilities and how to communicate significant events in a timely manner. ALE also has implemented various methods of external communication to support its customer base. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience.

Routines, emergency, and configuration changes to existing Rainbow infrastructure are authorized, tested, approved, automated and deployed by designated staff members from ALE Cloud Operations team only. Updates to Rainbow's infrastructure are done to minimize any impact on the customer and his use of the services. Changes are tested before being applied to production environment to help ensure they will behave as expected and not adversely impact performance. All changes must be authorized by internal Change Advisory Board (CAB) members to provide appropriate oversight and understanding of potential business impact.

Key changes are scheduled during regular rollout windows (Sunday CET). Emergency changes to production systems that require deviations from standard change management procedures are associated with an incident and are logged and approved as appropriate.

Design principles

Rainbow provides several security capabilities and services to increase privacy and control network accesses, including firewalls, encryption in transit with highest grading of TLS protocol specifications across all services, and DDoS mitigation technologies.

Rainbow's security policy implements traffic blocking rules to deny all traffic by default and only open necessary ports on the various load balancers in place. ALE systems only accept inbound HTTPS / WSS (443) connections, all plain-text accesses being redirected to TLS-secured connections. To the extent of highly secured load balancers, mail servers and WebRTC media relays, no component is exposed or accessible through the internet (public). Operations of such servers is possible only on highly controlled access points through a restricted two-factor authentication-based VPN, following a no-password policy, preventing any possible brute force attack.

ALE controls security quality of exposed interfaces using external tools such as Qualys SSL Labs, ensuring an appropriate level of service is maintained. Standard wildcard SSL/TLS certificates from Comodo CA are used and trusted by 99.9% of browsers. They employ a 256 bit EC key and are signed with RSA SHA-256. ALE's policy is to only support the strongest ciphers, enforcing TLSv1.2+ connections (and disabling SSLv2, SSLv3, TLSv1.0 and TLSv1.1), and consequently rejecting connections from weak browsers and clients such as IE 6-10, Safari 5-6, Android < 4.4, Java 6-7 and OpenSSL < 1.0.

Rainbow load balancers support Perfect Forward Secrecy (PFS), using Diffie-Hellmann (DH) and Elliptic Curve Diffie-Hellmann Ephemeral (ECDHE) cipher suites, Downgrade Attack Prevention, OCSP stapling and are known to be safe against all the last popular threats such as DROWN, BEAST, POODLE, HeartBleed and Spectre attacks (amongst others). ALE's policy is to mangle the application server's version numbers to prevent scan-based attacks.

ALE uses Strict Transport Security (HSTS) and are preloaded in browsers' public HSTS white-lists to enforce TLS connections. Rainbow servers all run on GNU/Linux Debian distribution, configured to always follow the latest security branch, ensuring that system packages get upgraded in case of zero-day breaches. The Rainbow production network is a completely autonomous information system, segregated from the ALE corporate network by means of a complex set of network security and authentication mechanism.

Application Layer

To help ensure only authorized Rainbow users and administrators access their accounts and associated resources, Rainbow uses several types of credentials for authentication. User authentication is done using basic authentication over TLS by associating user's email address and his/her private password, and further API calls rely on signed JSON Web Token (JWT). End user passwords are hashed and salted in Rainbow's internal database. Consequently, and for security reasons, forgotten credentials cannot be recovered, providing user with additional safety in the unfortunate event of data breach. The Rainbow system will then reset the user's password.

A password is required to access a Rainbow account. It is specified at the time the account is created and can be changed at any time. A high level of complexity is mandatory for user passwords, with a minimum of eight characters, including at least one lower-case letter, one upper-case letter, one number and one special character. Rainbow Multi-Factor Authentication (MFA) is an additional layer of security when it comes to account self-registration or password reset mechanism. A one-time temporary six-digit PIN code is sent to a user's email address and must be validated in Rainbow to ensure password setup.

Once authenticated, Rainbow ACLs ensure each user is offered the limited set of capabilities his profile currently offers. Company administrators are granted the capability to associate users to their company, promote users to various Rainbow service plan levels and to update company's visibility within Rainbow. Except from the public "Rainbow" company, private companies are isolated by default, default visibility restricting people from reaching out other companies than his own, as presented in Figure 3.

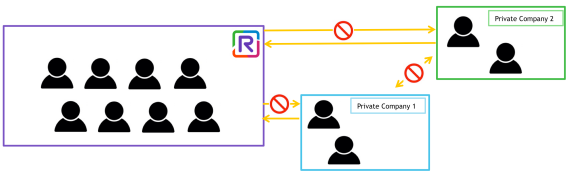


Figure 3: Rainbow Companies Visibility

Enforced data boundaries are in place, preventing any logical access to users and companies' data but to explicitly authorized peers.

Security framework compliance

The Rainbow infrastructure that ALE provides to its customers is designed and managed in alignment with cloud security standards, ALE Cloud Services being ISO/IEC 27001:2013, 27017:2015 and 27018:2014 and HDS 1.1 certified, ALE's hosting provider being certified to ISO/IEC 27001:2013, SOC 1 / SSAE 16 / ISAE 3402 (formerly SAS 70), SOC 2 and SOC 3 standards, ALE Operations staff members also being ISO 27001 "Lead Implementer" certified.

ALE infrastructure and software solution is under constant scrutiny through third-party network vulnerability scanners, web applications scanning and manual security audits conducted by external independent actors. Security being a priority, all necessary actions are taken to mitigate or eliminate any discovered threat.

Data privacy compliance

Rainbow services are designed to be compliant with personal data protection rules and regulations and in particular with European General Data Protection Regulation (GDPR) that enforces privacy and data protection for individuals. GDPR is built upon three main principles that have driven the philosophy of Rainbow data security: privacy by design, security by default, and accountability. The protection of customers' data is paramount, so ALE built security mechanisms and processes to ensure in-depth security for the respect of data subject privacy. Your data only belongs to yourself and is never processed for any commercial use nor transferred to any third party outside anywhere, unless it is necessary to do so. The level of personal data protection is at least at the level required by the GDPR where your data is transferred and you have given your prior consent. User data also remains stored in the geographies they belong to, ensuring legal conformance wherever it applies.

(Apr 2021)

Alcatel·Lucent Enterprise