ContactLab E-Marketing Platform Security Overview

Version <201805.1>

ContactLab S.p.A. – via Natale Battaglia, 12 - Milano, ITALY - http://www.ContactLab.com

Table of contents

ContactLab E-Marketing Platform

Security Overview

1. Introduction

An e-marketing platform such as ContactLab deals with personal data (PII, Personal Identifiable Information); data protection, privacy, confidentiality and security issues are of the utmost importance for ContactLab.

ContactLab's technical operations are based in the EU and as such subject to EU directives on data protection and privacy (directives 95/46/EC, 2002/58/EC, 2006/24/EC, GDPR) and more specifically to the Italian Privacy Law ("d.lgs. 196/2003"), the Italian "local execution" of the EU directives, one of the most severe data protection laws in the world to this date.

In this context, ContactLab operates as a Data Processor on behalf of its customers, the Data Controllers. ContactLab aims to systematically exceed the minimum security requirements set forth by the privacy legislation outlined above.

This document outlines some of the characteristics of ContactLab's architecture which are related to guarantee security and data protection. Only an overview is shown – details of our security implementation are not available for disclosure.

2. Physical Security

ContactLab operates two fully-managed farms located in state-of-the-art colocation facilities: Settimo Milanese, Milano, Italy (British Telecom Group) and Amsterdam, The Netherlands (The Datacenter Group). Services provided by BT and TDCG to ContactLab qualify for

- ISO9001:2008,
- ISO/IEC 27001:2013
- ISO 14001:2004

Our servers are positioned in tightly-controlled, closed-access dedicated rooms accessible through badge-controlled doors only to ContactLab pre-authorized personnel and the colocator's 7x24 staff ("remote eyes & hands") to perform emergency maintenance requested by ContactLab personnel though dedicated contact channels with an authorization code.

2.1 Milano Farm – Main Characteristics

The BT colocation facility is composed by two six-story buildings with a total surface of 18,000 m^2.
A total of 2,400 racks or 9,600 servers controlled by a 24/24 fully-redundant monitoring system can be housed in it. The facility buildings have been designed by BT with several top-line technology partners (Sanyo, Compagnia Elettrica Motori, Chloride Silectron and Siemens).

ContactLab's own farm is located in a private cage in the "Business Factory" building, with additional added-value characteristics with high-grade security, maximum support levels and basically unlimited in-facility bandwidth availability. This specially designed environment has been designed specifically for high-end e-commerce, e-trading and portal web sites requiring "no system failure" continuity.

Together with security features of the facilities, we also briefly describe electric continuity, temperature control and fire control subsystems as they're closely related to any security guarantee.

2.1.1 Environment

The facility is located in a site with no chemical/pharmaceutical plants, combustibles or other dangerous materials warehouses in a 4 km radius; no airports in close proximity. The area is also free from flooding risks and is elevated with respect to surrounding territory.

2.1.2 Electric power

BT's facilities provide a very high level of power continuity guarantee. Each building is divided in two sections; each section has 3 independent 1,5 Megawatt transformers. Sections are connected with 3200 Ampere busbar trunking ducts to guarantee instantaneous switching of power source even in the event an entire section's power infrastructure collapses.
Power surge protection is provided by 12 UPSes EDP90 (600 kVA each) in parallel, fully-redundant configuration. Redundancy of power distribution after the UPS subsystem is implemented with 12 800A CROSS realizing a fully-meshed power infrastructure.
The level of redundancy is 2N+2N to ensure even extraordinary maintainance activities can be performed with no interruption of service whatsoever.
No differential switch is installed in the whole power distribution matrix; only insulation transformers are used.
For long-term power outages from external sources, 4 CTM diesel generators (2 MW each) with a 45 m^3 diesel fuel reserve guarantee up to 48 hours of completely autonomous power generation without interruption of power continuity to housed devices.
Each dedicated room/module has two fully-redundant power terminals. The module switchboard, fully-redundant, provides a peak 60 kVA instantenous guarantee to each module.
ContactLab's farm is currently composed of 3 dedicated modules.

2.1.3 Temperature control

The air-conditioning subsystem has been specially designed by Sanyo Air Conditioning Research & Development dept. for BT. Heat dissipation is guaranteed for up to 3.5 KW for each rack (total head dissipation in I.NET facilities amount to 5,400 kWatts).
Temperature is guaranteed to stay between 20 and 24 ºC in every possible situation thanks to 400 evaporation units, 20 km of forced air-venting copper ducts and 66 condensing units (each rated for 84 KW) positioned on the roof of the buildings.

2.1.4 Fire and lightning protection

The fire control subsystem has 1,000 smoke detection devices and 600 Argonite-gas emitters with 6 reserves composed by 25 gas cylinders each, meshed and interconnected. The subsystem is able to control fire incidents in different locations simultaneously, providing protection against smoke diffusion, temperature anomalies, and fire residues potentially damaging electronic equipment.

2.1.5 Security monitoring and physical access

The exterior of the facility buildings is protected by a microwave system, an anti-jump barrier, 13 CCTV cameras with a 7x24 patrol squad stationing in the premises. The patrol squad is able to activate armed response from Police Authorities in 3 minutes thanks to special agreements.
Inside the buildings, 67 strategically located CCTV cameras provide full coverage of building interiors.
A manned reception desk clears every visitor at building entrance. Access to dedicated rooms such as ContactLab's is granted with personal badges and biometric confirmation.

Access to our rooms is guaranteed 365x7x24. Additionally, we have a support level agreement allowing us to require BT's staff to act as "remote eyes & hands" inside our rooms for emergency operations (e.g. to replace a damaged disk in a RAID array to minimize the failure window).

2.2 Amsterdam Farm – Main Characteristics

ContactLab's farm is collocated in a private cage inside The Datacenter Group's facility in Kabelweg 48a, Amsterdam.

2.2.1 Electric power

The Datacenter Group sets the highest standards for the quality and availability of power supply. Since its establishment in 2007 the datacenters have had an uptime of 100%. All power supplies in the racks are equipped with 32 Ampère overcurrent protection and are always powered by a UPS which filters out power dips or spikes from the NL national powergrid.
Power supply to each rack runs through two separate trajectories. The power supplies are connected to a separate UPS, diesel generator and transformer, in a completely 2N and offers solution.
TDCG peforms a Black Building Test every two months during which a power failure is simulated and

all backup systems are exercised.

Batteries, UPS and a SDMO / Mitsubishi emergency power generator (EPG) with local fuel supply for 24 hours autonomy, plus a special agreement with a supplier ensure power continuity in all conditions.

2.2.2 Temperature control

The Datacenter Group uses 'Closed Corridor' technology on all IT floors. This means that cold air is only released in areas where necessary, reducing the energy usage compared to older datacenters where complete datarooms are cooled including the hot air that is blown out by the IT equipment. To further increase the energy efficiency, each rack is supplied with the required number of blind plates to fill any unused gaps. This way no cold air goes through our datarooms unused. The entire air treatment installation is based on N+1 philosophy: for every critical part of our cooling sytem at least one active spare part is available in each dataroom. Chemical cooling agents, such as R404a, are not used at all. The Datacenter Group has developed its climate control system in-house and apart from being the most efficient in the market, knowing everything about our climate control system gives TDCG the advantage of having 100% control of such an essential part of the service. The system uses outside air to cool the air in the datarooms indirectly which prevents the servers from being damaged by dust or soot particles. The temperature at which air is blown at the inlets of the IT equipment is 22 degrees Celsius. The Datacenter Group has chosen to limit the temperature to these levels to improve the life of your installations while conserving as much energy as possible. The set point of 22 degrees Celsius means that the climate control system can be used to cool without any extra measures up to an external air temperature of 22 degrees Celsius (so called "free cooling"). On warmer days adiabatic cooling, or evaporative cooling, is automatically switched on.

2.2.3 Fire and protection

All areas in the datacenter are equipped with extinguishing systems. Our extinguishing systems are environmentally safe and not harmful to your health or to equipment set up in the datacenters. One of the unique aspects of The Datacenter Group is that we also use extinguishing systems in all our technical areas. Generally speaking, the risk of fire is greatest in these areas.

All areas are also equipped with CO2 hand-extinguishers and a VESDA system (Very Early Smoke Detection Apparatus): a system that is able to detect a potential fire at a very early stage. In addition to these fully automatic systems, we have engineers on-site 24/7 to follow up on all fire alarms according to our procedures, and to interrupt and escalate, if necessary.

2.2.4 Security monitoring and physical access

Access to THE datacenter is arranged in such a way that only authorised personnel and authorised suppliers and engineers have access to ContactLab's private cage. To that end, the datacenter has multiple layers of physical security: a CCTV system (including video surveillance) both inside and outside the buildings, biometric access control, and 24/7 security.

Security personnel are on-site 24/7 to monitor camera footage, monitor access, make surveillance rounds, and monitor compliance with the Company Rules for all visitors. If activities or incidents that form a potential threat to continuity and availability occur in the datacenter, security personnel will take immediate action.

3. Network Security

The ContactLab platform is protected on the edge by multiple couples of F5 Networks BigIP and CISCO ASA 55x0 devices in automatic fail-over configurations. Block-all default rules are implemented on all network interfaces in firewall devices.

Internet connectivity is provided by our own Autonomous System (AS60227) since 2013. Each farm has at least two completely independent upstream providers announcing our AS. As of the date of this document, the upstream providers are:

- Telia and Metrolink in Milano
- NTT and Prolocation in Amsterdam

The two farms are connected by a redundant dual-path long-distance 10 Gbps fiber uplink provided by Telia.
A dual-path redundant fiber link connects our Settimo Milanese farm to the Avalon facility in the Milano Caldera campus where access to upstream connectivity is connected.

Fully-owned and fully-managed servers are used for our platform exclusively. Platform servers are completely isolated from optional services servers (such as housing and hosting services available to selected customers, completely separated from ContactLab platform services for the same customers). Isolation includes physical separation – virtualized servers for ContactLab platform are instantiated on convergent Hitachi UCP platforms running the VMWare hypervisor with connected Hitachi HUS-VM two-tier storage (high-performance Flash drives and SAS) or Hitachi G200 storage (for backups). Physical servers are used mostly for dedicated HDFS slave nodes and the specialized high-performance MTA infrastructure.

The platform is composed of several products which are themselves composed by a number of specialized Subsystems. Each Subsystem provides limited external access, in full respect of the “principle of least privilege”.

1) Front-end

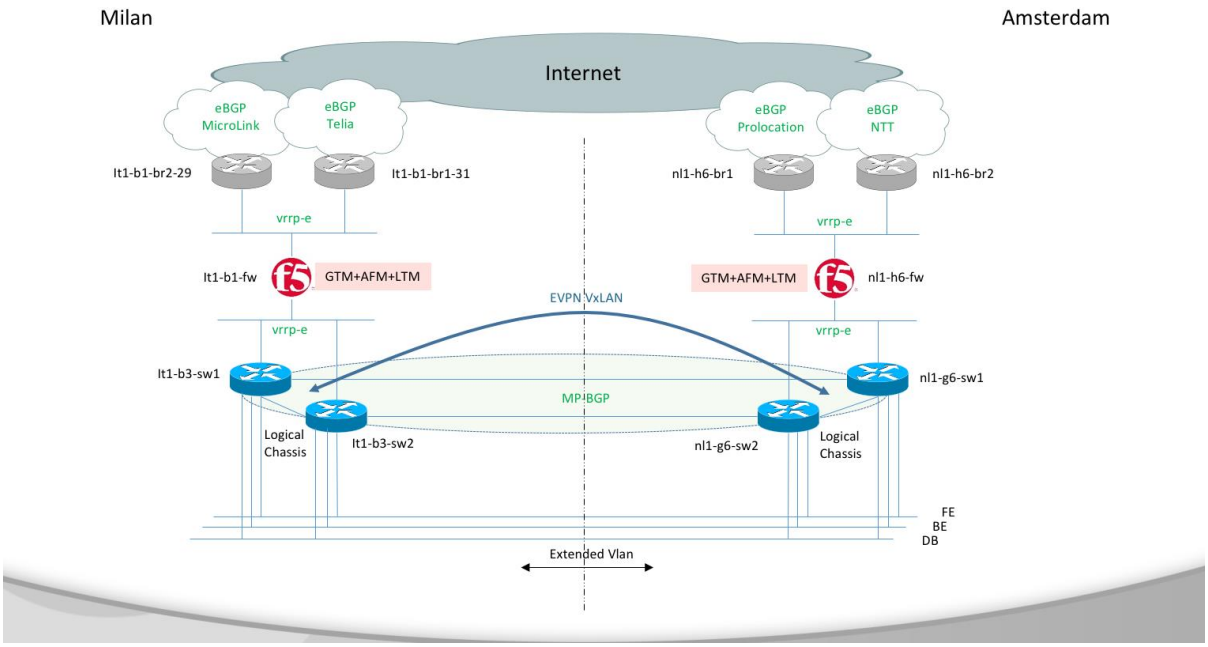
a. Private Web Servers Subsystem. These servers provide HTTPS only access to customers for the private-access User Interface applications for our Platform including SOAP API access. FTP/SFTP access to private area is also provided on request.
b. Public Web Servers Subsystem. These servers provide HTTP and HTTPS access to unrestricted resources such as open and click tracking services, static resources (complimentary hosting provided to customers)
c. Bounce/FBL Subsystem. Dedicated inbound-only stripped-down SMTP listeners for incoming out of band bounces, feedback loops and list-unsubscribe messages from external sources

2) Back-end
   a. Database Subsystem. Multiple MySQL Enterprise database servers in master-slave couples host each customer's private database shard (dedicated master/slave couples are available as an option)
   b. Engine Subsystem. This subsystem provides high-speed message composition. Messages are delivered to the Messaging Subystem.
   c. Messaging Subsystem. Dedicated outbound high-performance SMTP, SMPP, APN and GCM servers manage message delivery to destination (destination domain MXs for SMTP, SMPP integration points for SMPP gateway suppliers, Apple APN and Google GCM endpoint for the eponymous protocols).
   d. Work Server Subsystems. Dedicated servers hosting applications performing user data integration (bidirectional data flow to customer's own IS), feedback data collection, aggregation, statistics-based monitoring and alerting, and periodic data maintenance tasks.

All Front-end subsystems expose HTTP (unrestricted services only), HTTPS and FTP/SFTP protocol entry points exclusively through NAT configurations managed by the firewalls.
Additionally, HTTP/HTTPS protocol access gets through a layer of redundant reverse proxies performing the duties of load balancing, fault tolerance and URL filtering/sanitization.

Back-end servers are not accessible from the Internet.
Messaging servers allow limited IP-based ACL-authorized inbound SMTP traffic on dedicated listeners (IP addresses) for SMTP relay and SMTP SmartRelay customers only.

Access to servers by ContactLab personnel flows through dedicated subnetworks connecting ContactLab's premises via dual-path redundant fiber-optics LAN links to the farm.



4. Server configuration

Server configurations are specialized according to the Subsystem they are part of.
For each subsystem, the set of installed software is specifically defined by ContactLab to include only the bare minimum subset of applications and utilities need to perform its specialized function.

FreeBSD and RedHat/CentOS, Debian/Ubuntu Linux are the only Operating Systems utilized by ContactLab in its platform. Interactive access to servers is granted to the IT Operations team only. In addition, the most senior technicians in the Software Engineering team can be authorized for troubleshooting reasons, on a need-to basis only. The latter requires specific case-by-case authorization by the CTO.

Critical security patches are automatically applied. Non-critical/security patches are applied in bi-monthly routine maintenance cycles after evaluation of the patch sets by the System Engineering team. Access is granted to non-privileged personal accounts with both a login/password and personal (company provided) public key authorization through SSH.

All servers implement both short-lived local and remote centralized logging for all access operations. Local logging is used only to ensure logging continuity is guaranteed even in case of network failure for the internal network. Remote logging is archived for 12 months (according to current regulations, access

to logging data might be restricted even to our customers, access restrictions also apply to specific information). Mandatory system administrator logging is archived in encrypted tamper proof format to a remote trusted supplier for all uses required by law.

All servers are protected by automatically updating anti-malware software (currently ESET NOD32, re-evaluated yearly according to industry benchmarks).

5. Database Security

ContactLab utilizes a sharded approach to its data model to provide both performance and data protection guarantee to its customers. All customer-level data are stored in one or more of our database systems (MySQL, Elasticsearch, Vertica, Hadoop) and all those products uses the same security as described below.

Each ContactLab platform account (a customer might have several platform accounts) has a dedicated database shard including all customer-level data (e.g. “user databases” with recipients’ email address and profile information provided by customer) and also most of the platform’s data points related to a customer’s activity.

As an example, every message sent through ContactLab is recorded in a platform data structure residing *inside* the customer’s dedicated shard.

Shards are implemented at the database level and every shard has a different application user with privileges and visibility limited to that shard. ContactLab applications impersonate this user (with a different database connection) as soon as the ContactLab customer’s user profile requesting access to a given account is validated in the centralized Access Control dictionary.

This approach also ensures that when a customer contract expires *all* data related to a customer is permanently deleted. According to EU GDPR and the Italian Privacy Law, ContactLab operates as a Data Processor as explicitly authorized by the Customer who is the Owner of the Data (Data Controller). Therefore, when a Customer leaves, we destroy all data the Customer decided to store in its database shard(s) on our servers.

Please be aware that current regulations require us to securely archive specific information (e.g. the record of a message being sent to a specific recipient, but not its content) for specific periods. We only keep these archives in case Public Authorities order us to disclose them. After the mandatory archival period expires we destroy these copies too.

Data protection is also guaranteeing continued availability. This is ensured by the master-slave setup or data replication across multiple nodes, ensuring continuous replication of the databases.

A dedicated MySQL master-slave server couple is available as an option to interested customers. In this case, two dedicated MySQL servers are dedicated to a single Customer's accounts and will host only the Customer's database shards.

Only System Engineers part of the IT Operation teams are allowed interactive access to the Database servers. Access and authorizations are logged.

Encryption at rest at the storage level is implemented for all database systems with hardware-based, FIPS-140-2 compliant AES 256 encryption in XTS mode applied to all logical devices (LDEV) where the database systems' data volumes are located.

6. Data Backup

Customers' personally identifiable information is stored in the Database subsystem.
ContactLab implements a comprehensive automated backup system based on CommVault Simpana. Main data sources from the MySQL databases follow this backup policy: 1 full backup daily, plus a differential incremental backup every 6 hours each day. The full daily backups are kept for 14 days. The first daily backup performed in any given calendar month is kept for 12 months. Vertica and Elastic follow a daily backup policy. Hadoop data are replicated across multiple nodes and can be re-generated from the databases in case of disaster.

7. Platform Application-level Security

7.1 User Interface access

ContactLab platform user-level functionality can only be accessed through a Web-based interface on HTTPS protocol (TLS only).
Personal access is granted to Customer-specified users with a personal login/password pair automatically and unconditionally expiring every 3 months (90 days).
If the user does not change the password within 30 days of each expiration, her credentials will be automatically suspended and reactivation requires a request to our Customer Care from an authorized Customer representative.
Automatic checks for suspicious activity might trigger a second authentication request. This is implemented using a personal 8-digit PIN (personal identification number). 2 random digits from the 8-digit PIN are requested each time. In case the second authentication request is triggered, user will not be able to proceed until it is satisfied, even if it tries to reconnect later on.

Automatic blocks in case of repeated authentication failures (both on the primary and secondary authentication) are implemented.

Passwords must be long a minimum of 8 characters and are checked for minimum complexity requirements

They are stored in the Access Control dictionary encrypted with a one-way salted hashing Blowfish algorithm.

It is possible to give specific Customer user accounts the functionality to manage other users for the same Customer (admin level). This only happens on request. All other requests must go through our Customer Care staff.

Access to Contactsend accounts (tenants) can optionally be limited to a set of IP network addresses using CIDR masks. These network addresses can also be managed by admin-level Customer user accounts if they exist. Please notice this protection is applied to customer accounts (tenants) and not to user credentials. This is by design to ensure IP-based ensure dataset protection cannot be circumvented by mistake when creating new user credentials or authorizing credentials to access restricted accounts.

7.2 SOAP API access

Access to the legacy SOAP API is granted exclusively via HTTPS with mandatory IP-based ACL for origin servers.

Specific credentials are generated for API access. API access to platform functionality is validated against authorization profiles, as user accounts.

7.3 REST API access

Access to the modern REST API is granted exclusively via HTTPS. Oauth2 authentication schemes are supported; a proper authorization (bearer) token must be obtained and then presented to API endpoints to gain access to resources. Tokens have limited access to available functionality, and restricted access to Customer data.

7.4 Data Exchange private area access

Private access to private SFTP areas can be granted to customers to implement file transfers needed for Data Exchange synchronization configurations. Mandatory IP-based ACL are implemented for these accesses.

FTP access is requested only if customer explicitly requests it and strongly discouraged.

7.5 Public area access

Private access via SFTP or FTP can be provided to customers to upload publicly accessible resources

(images, stylesheets, etc.) that customers wish to delegate to ContactLab. This areas are completely separated and independent from the Data Exchange private areas. IP-based constraints for access to these areas can be applied but are not mandatory.

Access and operations performed by users are logged also in the application database with source IP and timestamp of the HTTP request originating the operation.
Inbound HTTP requests logs are collected at the reverse proxy perimeter and kept for 12 months with restricted access.
An operation audit log is available to customers on request.

8. System-level Monitoring and Alerting

Any server in ContactLab is actively monitored using both agents installed on the server and remote sensors (SNMP). Monitoring is performed up to application-level key indicators such as number of bounces being collected in a period of time or number of clicks being recorded in a period of time.
All of the collected indicators have low and high values triggering automatic alerts when reached.
Alerts are sent to the System Engineering team and, for specific indicators, to other specialized teams (for instance, bounce collection anomalies also generate alerts to the Deliverability team).

Monitoring activity and data collection is performed on a dedicated in-house installation of multiple tools with different scopes; Zabbix and Grafana as main monitoring and alarm system, Centreon for network related systems, Kibana as SIEM, performance monitoring, capacity management and planning. External monitoring is implemented with dedicated off-location servers running Nagios/Zabbix.

ContactLab also uses MySQL Enterprise tools to monitor specific MySQL-level indicators not available to other tools for its database servers. ContactLab is a MySQL Enterprise customer and utilizes MySQL Enterprise official binaries on all its database servers.

9. Security and compliance validation

ContactLab performs regular perimeter testing and application-level vulnerability assessment / penetration tests . Tests are performed by selected independent 3rd parties.
IT Risk Analysis and Compliance Audits by trusted 3rd parties are also performed at least once per year.