LOGEX

We earn trust by providing assurance

LOGEX Security Whitepaper

Table of contents

Products & Legal Entities Covered

This whitepaper describes the development, maintenance, and other relevant (internal) processes/activities undertaken by LOGEX and (or through) its associated legal entities, related to providing the LOGEX (SaaS) Financial Analytics solutions in a secure manner.

Collectively named “LOGEX”, the following legal entities are covered:

- LOGEX BV (The Netherlands)
- LOGEX Healthcare Analytics Ltd (United Kingdom)
- LOGEX Healthcare Analytics AB (Sweden)
- LOGEX Oy (Finland)
- LOGEX Solution Center s.r.o. (Czech Republic)

Privacy & Security Compliance

Privacy & GDPR

As a data analytics organisation, LOGEX acts as a data processor to perform data analysis on behalf of its clients. Therefore, LOGEX performs its activities solely on the lawful basis as described in GDPR article 6 (1) (b) (“Performance of a Contract”). LOGEX only works with data exported from clients’ systems and does not integrate with clients’ systems, nor does it modify data within those systems. This means data within clients’ systems remains unaffected and the (single) point of truth.

Given the nature of LOGEX’s business, LOGEX processes not just personal data but also, as defined under GDPR, “special categories” of personal data, being information concerning individuals’ health. Only authorised LOGEX employees and users at our customers will have access to this data.

LOGEX has appointed a Privacy Officer to oversee our company’s compliance to GDPR and other relevant privacy regulations. The Privacy Officer works closely with our Data Protection Officers (DPOs) to establish privacy governance structures in line with international and local data protection regulations and requirements.

Any inquiries about the processing of personal data can be directed at our DPOs, for which details can be found on the corresponding local LOGEX websites (https://www.logex.com).

Security Compliance

Customers worldwide require LOGEX to comply with both international and domestic security requirements where applicable. In order to fulfil those needs, LOGEX holds the following active security certifications and accreditations:

International:
- ISO 27001:2013

The Netherlands:
- NEN 7510-1:2017 + A1:2020
- ISAE 3402 type II

United Kingdom:
- Cyber Essentials
- Information Commissioner's Office registration
- NHS Data Security & Protection Toolkit

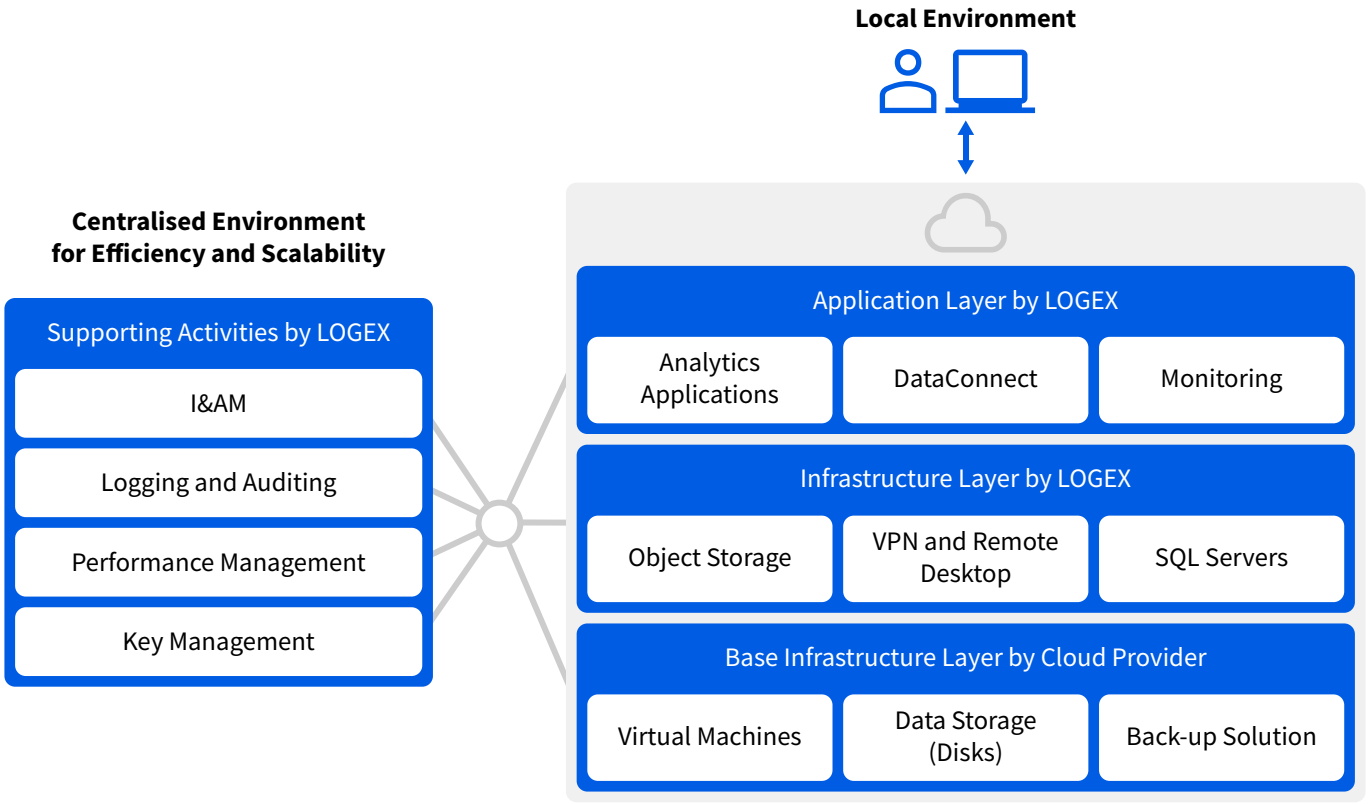
All mentioned certifications contain an annual (external) audit and/or annual re-certification requirement.

Platform & Technology

LOGEX delivers online healthcare analytics as Software-as-a-Service (SaaS), meaning that the entire LOGEX application runs online, unlike in the past when a local or client-side installation was required. Both our client's data and the calculations logic are deployed on our cloud infrastructure. Users of our customers can access the application on any computer with a web-browser (specifications are described below).

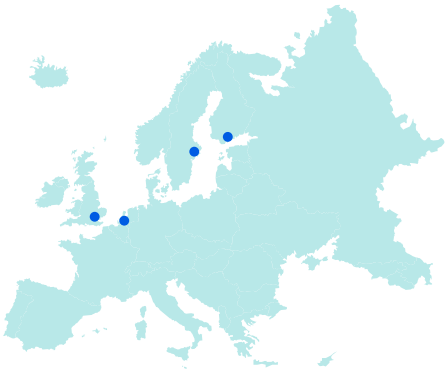
A SaaS platform allows us to scale our products without (linearly) increasing supporting resources, and it enables us to ensure all clients benefit from having access to the latest features and being provisioned with important maintenance and security updates without delay.

Hosting & Infrastructure
We employ a so-called 'cloud-agnostic' architecture, meaning that our technology is built with minimal dependence on our cloud providers, thereby eliminating any potential vendor lock-in risk. This approach enables us to quickly migrate our products from one cloud provider to another, to ensure continuity of our business if it were ever at risk. As outlined in the next chapter, LOGEX products are hosted at different cloud providers in different countries, both at international and at local partners. We make use of different cloud providers in order to respect local privacy regulations, data residency requirements, and local sentiment. Where possible, we make use of proven vendor-supplied solutions for operational efficiency and security.



Data Residency
LOGEX stores customer data domestically. Therefore, data is stored in the following data centres:

- The Netherlands:
  Microsoft Azure EU-WEST
- United Kingdom:
  Microsoft Azure UK-SOUTH
- Sweden:
  Local hosting provider (Elastx)
- Finland:
  Local hosting provider (Telia)



LOGEX requires its infrastructure partners to be ISO 27001 certified and/or make use of ISO 27001 certified data centres, to ensure continued security assurance throughout key elements of the LOGEX supply chain. Besides ensuring data is stored in well-protected data centres, from a logical perspective we ascertain that data never leaves the data centres as part of LOGEX's operations: LOGEX employees only have access to the data through a secure Remote Desktop connection to the data centre.

Network Segmentation
Our network environments are logically and/or physically separated, to ensure only those who need access to certain data or services actually have access. Think of the guest networks vs. authorised company networks in our offices, hosted enterprise services such as O365 vs. the LOGEX-hosted customer-facing

applications, and the separation of development/testing/acceptance/production environments for the LOGEX applications. By segmenting networks based on the relevant data assets, and controlling access to those environments, we make sure confidential information remains confidential.

Application Requirements

The LOGEX applications are accessible from any modern browser (Chrome and Microsoft Edge are preferred, Firefox support is best-effort) via HTTPS (no VPN is required). In terms of PC specifications, 8 GB RAM and 20 Mbit Internet speed are recommended, along with Windows 10 or 11 64-bit.

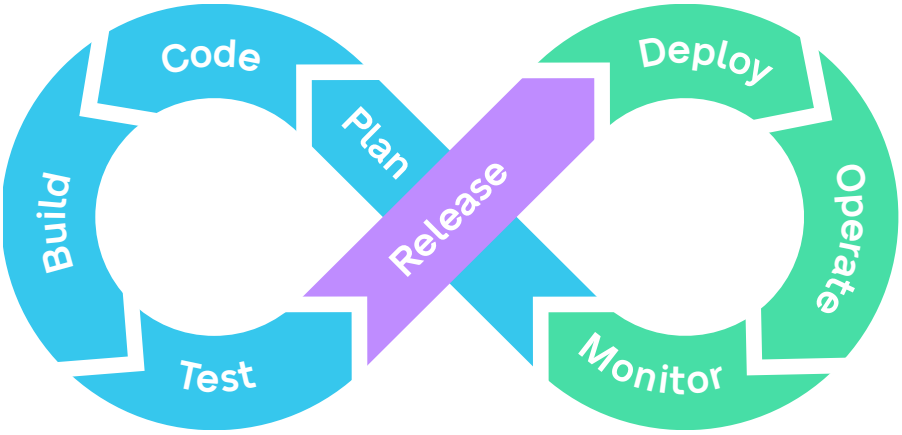
LOGEX applications function as so-called 'single-page' applications, where data is incrementally loaded in the browser, thereby creating a responsive user experience. Network connection speed and memory specifications will influence how quickly data is loaded to the browser, as likely a handsome amount of data will need to be loaded.

The LOGEX applications are designed for use on laptop/PC. Use on tablet and mobile devices is not recommended, as LOGEX applications are not designed for touch interaction.

Development Process

LOGEX has embraced the DevOps methodology for developing and operating its applications.

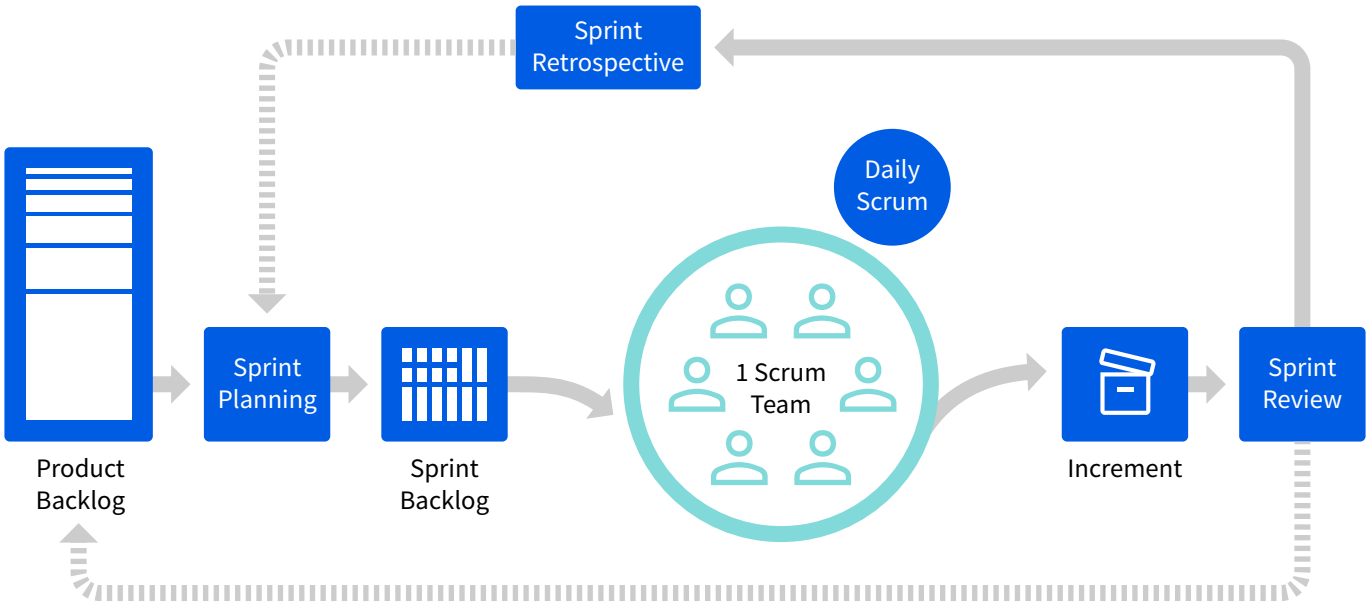
Since LOGEX products are often offered/hosted in multiple countries, we develop our applications under the philosophy of "developing centrally, deploying locally". Our ever-growing software development team is located in our Solution Center in Brno, Czech Republic, consisting of – among others – backend developers, database developers, frontend developers, UX/UI designers, system analysts, scrum masters and test automation specialists.



LOGEX software is developed according to a software development lifecycle (SDLC), which means requirements and best practices are applied to the various

stages software evolves through in its lifetime, safeguarded by quality gates all around. Any changes, new features, improvements or fixes are defined and created through our implementation of the Scrum methodology, where sprint cycles last 2 weeks.

After development, applications are deployed in their respective local infrastructures for (acceptance) testing purposes and ultimately production roll-out.



Change Management
Changes of any kind to the LOGEX applications and infrastructure are managed and logged through a central documentation and ticketing platform (Atlassian). Along with the ability to review and approve changes (in code) before integrating them into production, the platform enables us to manage changes in a transparent and traceable manner.

Security

Information Security Management System (ISMS)
LOGEX has designed and implemented an ISMS, which is the collection of responsibilities, objectives, policies, and technological and procedural security controls to effectively manage information security risks to our organisation. Our ISMS is managed centrally and covers all previously referenced legal entities. Our ISMS is designed, implemented, certified and annually audited according to the ISO 27001 and NEN 7510 standards.

Security Testing (Code Scanning, Vulnerability Scanning and Penetration Testing)
LOGEX applications and infrastructure are subjected to external penetration tests at least once a year. In addition to external security testing activities, LOGEX employs a security testing strategy which covers the entire software development lifecycle. We regularly test for (known) vulnerabilities and

software weaknesses internally through the use of third-party or community-developed Static Code Analysis, Software Composition Analysis, and Vulnerability Scanning tools. Factoring these testing activities in our development process allows us to:

- identify and eliminate software weaknesses introduced by coding errors at the time of coding self-developed software
- identify and eliminate known vulnerabilities introduced by third-party/ open-source software components that are integrated into LOGEX applications/infrastructure
- identify and eliminate vulnerabilities on production systems

Security Incident Response
Security incidents are viewed as an opportunity to learn and improve our way of working. Therefore, LOGEX encourages employees to always report incidents, regardless of size of the incident, whether an employee caused or witnessed an incident, and regardless of whether a vulnerability has resulted in actual damage or not. LOGEX employees understand they all have an individual responsibility to protect the security of the organisation, and reporting (potential) incidents is a key element of this responsibility.

In case of a security incident and/or data breach, an Incident Response Procedure is followed in order to manage and resolve the incident. The Procedure includes the following steps:

- Identification and classification of the incident
- Damage control and incident investigation
- Remediation and recovery
- (Timely) Communication to affected parties, where needed
- Reporting and evaluation, including root cause analysis

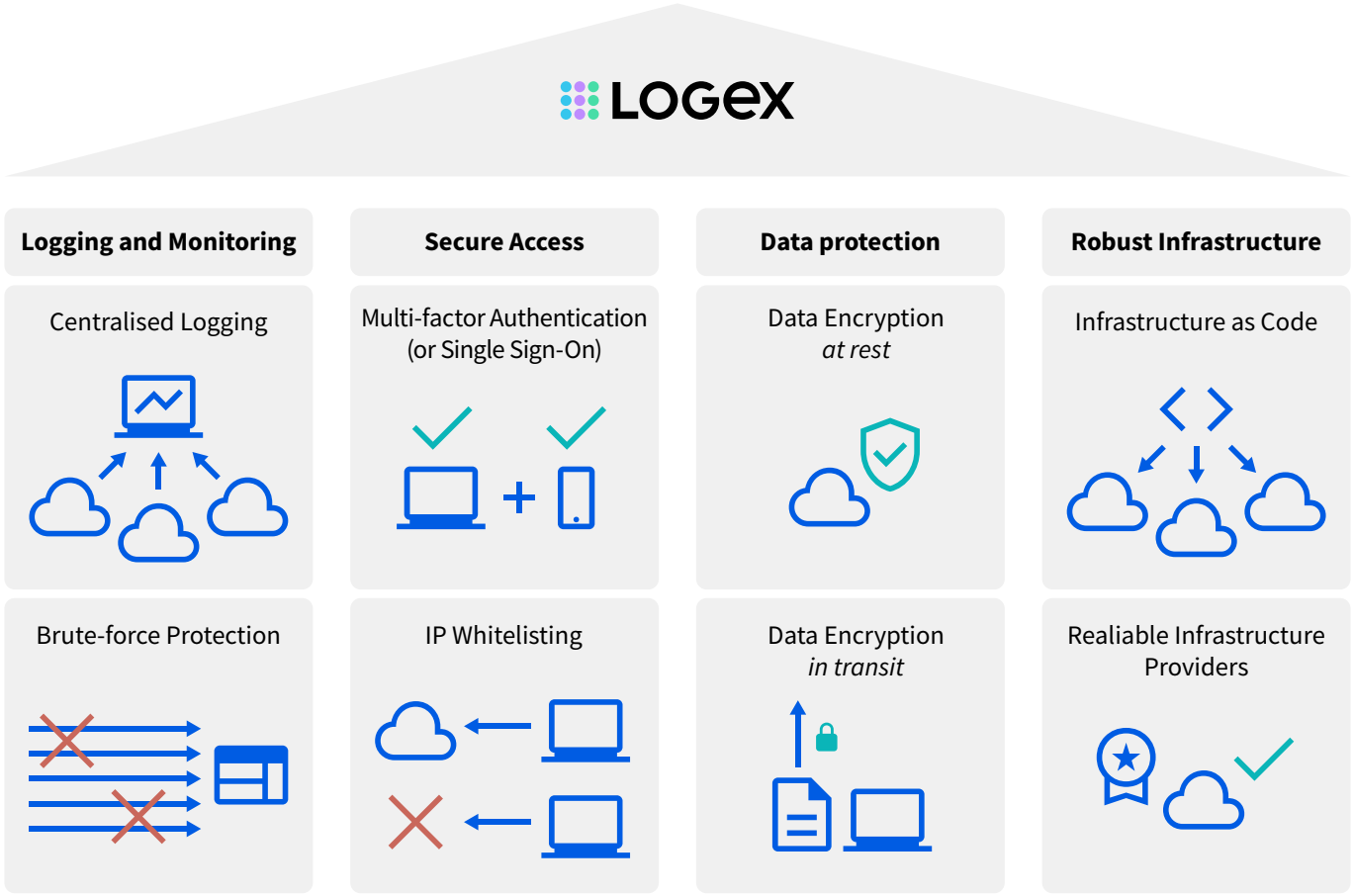
Incident reports and follow-ups are recorded centrally for evidencing, traceability and auditing purposes.

Encryption
Communication with the LOGEX products is encrypted *in transit* using *TLS v1.2* and strong ciphers.

Data provided to the LOGEX products is encrypted *at rest* through disk encryption at the data centre, using *AES-256*.

Additionally, passwords, which are managed through a managed ID platform (Auth0), are encrypted with the *bcrypt* algorithm to securely hash and salt the passwords.

Centralised Logging & Monitoring
LOGEX centrally logs events taking place within the different environments/ infrastructures where LOGEX products are deployed. Events such as user management actions (creating, modifying, deleting users), authentication attempts and user actions within systems are captured and monitored for anomalies and potential indicators of compromise.



Identity & Access Management

User Authentication (incl. brute-force and IP-throttling protection)
Where possible, LOGEX encourages customers to use their own identity provider (e.g. Open ID Connect or SAML) as a means of customer user authentication. We also promote the use of Single Sign-On (SSO), so that users can seamlessly sign in to the LOGEX applications.

If a customer's identity provider cannot be integrated, LOGEX will issue dedicated user accounts for customer users, consisting of a username (typically the user's work email address) and password. Passwords are subjected to password length and complexity requirements, to ensure they are of sufficient strength. Users will be required to use multi-factor authentication (MFA) when signing in to the LOGEX application, meaning that besides the username and password a second authentication factor (e.g. through the Microsoft Authenticator app) is required.

The managed ID platform (Auth0) utilised by the LOGEX applications offers additional forms of account protection, including brute-force protection – which limits the amount of faulty passwords that can be entered sequentially – and protection from suspicious IP throttling – which will result in blocking of specific IP addresses that rapidly make a large number of login attempts.

User Authorisation
We make use of the so-called Role-Based Access Control (RBAC) authorisation model, where (groups of) users are assigned permissions to access resources

based on their role in the organisation. This applies both to LOGEX internal users and client users. To ensure that such permissions are distributed and managed correctly, we perform regular reviews of such RBAC groups and adjust permissions where needed. Similarly, we periodically request clients to review their user base so that the client user base permissions remain accurate.

Availability & Back-ups

Availability
LOGEX has recovery mechanisms in place to not only restore data, but also re-build its entire infrastructure. We have created all our infrastructure as code, which supports us to standardise infrastructure deployments across different locations and cloud providers, and therefore enables us to scale our SaaS solutions across countries. Following this Infrastructure-as-Code paradigm also allows us to re-deploy our solutions quickly at a different data centre in case of disaster recovery. Our Recovery Point and Recovery Time Objectives aim for minimal disruption to the availability of our solutions.

Back-ups
In order to support our and our customers' business continuity, we have implemented a complete back-up schedule where full back-ups of application databases are created every week, differential back-ups are created daily, and transaction logs are backed up every 15 minutes. Back-ups have a 4-week retention period. Regardless of the cloud service provider, we require back-ups to be stored in encrypted form (using AES-256).


LOGEX