enalyzer

enalyzer security

A documentation that provides an in depth description, that can be read as is, or forwarded to IT departments demanding more technical information.

Copenhagen, May 2018
www.enalyzer.com

Highlights

Enalyzer Security

Physical security

- Fully redundant systems
- Guaranteed uptime 99,8%
- Daily and monthly back up of all data, exported to separate locations
- Best in class firewalling, cooling and power supplies
- Restricted access for authenticated personnel only
- Substantial protection measures against burglary
- System security monitoring 24x7x365

Software security

- Login authentication with via security server
- Encryption on login and password
- Encryption on data collection and reporting
- Logging of user sessions

Internal security

- Access to server environment only by authenticated personnel and from Enalyzer HQ
- Support access to accounts only by user approval
- Enalyzer registered at the Danish Data Protection Agency

Third party approvals

- PwC audits Itadel

Table of content

Enalyzer Security

1. Physical security **4-6**

1.1 Managed Hosting 4
1.2 Access control 4
1.3 Power 4
1.4 Cooling 4
1.5 Fire 4
1.6 Monitoring 4
1.7 Firewall 5
1.8 Enalyzer's server set up in the datacenter 5
1.9 Server up time 5
1.10 Backup and restore 5

2. Software security **7**

2.1 Login safety 7
2.2 Encryption 7
2.3 Logging 7
2.4 Support 7

3. Internal security **8**

3.1 Servers 8
3.2 Data Protection Act 8

4. Third party approvals **9**

4.1 PWC audit Itadel 9

1. Physical security

Enalyzer Security

a Itadel

1.1 Managed Hosting

Enalyzer systems are hosted and operated (managed hosting) by Itadel. Itadel is a leading Danish hosting provider with more than 300 employees dedicated to provide state of the art solutions. Their data centers are located in Denmark and are designed with fully redundant systems, where each system has individual back up. Network connections from data centers are also fully redundant.

All data centers' common infrastructure devices are designed with fully redundant systems where each system has individual backup. Network Connections from data centers are also fully redundant.

1.2 Access control

Itadel's data centers are shell secured and the data centers' exterior walls, doors and windows are thus secured against burglary and fire. All external doors are made of steel, with steel bulkheads in front of all windows located on the ground floor. All data centers are equipped with sensors to detect break-ins and burglary attempts. Mounted opening switches on all doors and windows, as well as "shake switches" on ventilations, windows and doors are installed together with motion sensors that cover walkways in the office.
Itadel is under constant surveillance by security cameras outside the entrance doors and inside with extra cameras in selected rooms.

The installed access control system ensures that it is only possible to enter the data centers using access cards and a personal code. Doors require signing a logbook when entering and exiting the room, restricting excess.

Only a small pre-approved group of Enalyzer employees, can access the datacenters after contacting Itadel, and by being accompanied by an Itadel employee.

1.3 Power

All electrical installations at Itadel are set up in accordance with applicable international rules based on the so-called N +1 solution. This includes backup batteries and reserve power systems (diesel generators). In other words, the available power backup systems are capable of delivering sufficient power to keep the systems running. Diesel generators can provide power to Itadel for 3 days at no extra filling of oil.
Battery systems are checked every six months and diesel generators are tested at least 3 times a year. Enalyzer's equipment is connected to two separate fuse groups. The floors in data centers are equipped with an anti-static coating and grounding.

1.4 Cooling

Itadel refrigeration system is also built in accordance with the N +1 model. The installed cooling unit is capable of providing all the necessary cooling in order to fully utilize power capacity. The climate control system ensures that the temperature in Itadel's data centers is at a Best Practice for Telco / IT industry level.

1.5 Fire

Data centers are equipped with sensitive fire alarm systems consisting of sniffing plants and ion detectors. In order to extinguish fires, so-called Inergen systems are installed.
Lightning protection systems with earthing are checked every five years. The fire fighting system's alarms are directly linked to the fire department. Alarms from fire detectors, access control and building management systems are directed to a central operating and monitoring center within Itadel while an SMS can also be sent to selected individuals in Itadel.

1.6 Monitoring

Itadel carries out 24x7 monitoring of the entire system. Itadel uses a variety of tools that are tailored to monitor separate system areas. Itadel does surveillance on all system levels, from networks to response times on selected applications.

Additionally all Enalyzer applications are monitored for performance and uptime through an external service provider site24x7.com.

All production servers are equipped with a monitoring agent that monitors error messages in various logs, and also collects performance numbers and messages from the hardware, for example SNMP traps.

Additionally, CPU load, RAM usage, disk load and I/O load are monitored. Furthermore, constant surveillance is carried out to prevent hardware failure.

Storage systems are monitored for capacity and performance management. This ensures sufficient storage is available and the performance is optimal at any time.

SAN, LAN and WAN networks are monitored for bandwidth usage and error conditions, such as line breakage.

Middleware components are monitored for ongoing services and availability. Irregularities are addressed immediately and reported to the Service Desk. Monitoring is set up in close cooperation with Enalyzer. For databases, monitoring is carried out on log files for errors and necessary services, capacity degrees in table spaces available “undo space” and backup logs. The measurements are collected and stored continuously so that a history analysis and trend analysis is possible. The historical data and trend analysis forms the subsequent basis for making the surveillance proactive.

1.7 Firewall

Access from the Internet to the production environment is protected by firewalls. The advanced firewall protects against attacks on three different layers. (1) the network layer, where it protects against IP spoofing and various IP Denial-of-Service (DoS) attacks, (2) the transport layer, where participants are checked for appropriate TCP flags and blocking of unknown protocols, and (3) the application layer, where among other things it checks if the content of the traffic corresponds to what is expected for several protocols.

Firewalls are configured so that maintenance can be performed without affecting availability, as well as automatic failover in the event of a failure of the one component.

1.8 Enalyzer’s server set up in the datacenter

The servers operate with full redundancy and are updated by Itadel on a continuous basis according to best practice in the market. The servers have direct access to the internet backbone.

Middleware operations & patch management Operating systems and server applications are managed by Itadel.

Patch updates for operating systems, firewalls, etc. are handled by Itadel. Itadel ensures that all hardware is included in the solution, and wherever possible is updated with the latest security updates. Security Updates are assessed by threat level and approved by Enalyzer before being implemented on the servers. Emergency and other important updates can be performed by Itadel without consulting Enalyzer beforehand.

Scheduled updates will be communicated to Enalyzer’s customers up to 1 week prior. Scheduled updates are usually performed from 22:00 to 06:00. At each scheduled update set, an update plan that describes all part of the update and any rollback scenarios will be provided. Typically updates are done swiftly without any implications for the users.

1.9 Server up time

Enalyzer guarantees through its agreement with Itadel an uptime of 99.8%.

1.10 Backup and restore

Itadel handles backup and restore of all operating servers. The agreement with Enalyzer includes hardware, basic backup agents for OS and Middleware, as well as all operational services for backup and restore. Backups are exported to a backup system that is physically separated from data centers. Itadel back-up to disks as disk-based backups provide faster restoring than similar, tape-based solutions. Backups are done in accordance with the guidelines of Itadel.

Once an hour a differential backup is taken. Once a day a full backup is taken. Once a month a full backup is stored on a separate location. Data on terminated license accounts is deleted after 6 months. The customer is given a prior notice in order to be able to export the data.

Server Load Balancing (SLB) consists of fully redundant web switches, that balance internet-users traffic versus Enalyzers pool of available web servers, based on various load balancing algorithms.

2. Software security

Enalyzer Security

2.1 Login safety

Enalyzer systems are delivered as SaaS systems and can be accessed through any modern web browser. All users have separate usernames and passwords. Authentication is done via a central security server ("single sign-on server") that makes it possible to use the same credentials for all Enalyzer systems. The security server is located behind a firewall so that only Enalyzer systems can communicate with it.

Multiple failed login attempts from the same user is blocked.

Multiple failed login attempts from the same IP address, enhances the security process by using capture security technology.

2.2 Encryption

All login and password information to the application is encrypted and stored as hash values.

All administrator actions within the application are encrypted. Data collected from respondents is by default encrypted.

Communication to the application from Enalyzer systemadministrators and developers are encrypted using VPN.

2.3 Logging

On the servers, logging is done on all internet traffic. All operations can be identified by a security token that can be traced back to the individual user. For applications, Logging is done on all critical operations. Each log contains information about who did what and when. The log is available to the systems administrative users.

2.4 Support

Enalyzer support can only access an Enalyzer user account by approval from the user.

3. Internal security

Enalyzer Security

3.1 Servers

Only Enalyzer's it-personnel, authorized by Enalyzer's it-manager, are allowed to access Enalyzer's servers. Access is only possible by way of a 2-factor authentication. Access from outside Enalyzer's headquarters (home computers, laptops et cetera) is only possible through a VPN-connection and by way of a 2-factor authentication. The authorized personnel is instructed always to secure such workstations and always to log off when not in use.

3.2 GDPR

The GDPR applies to the relation between the customer and Enalyzer. The customer's use of the service implies that Enalyzer will be processing data, including personal information, belonging to the customer. Consequently, the agreement between Enalyzer and the customer constitutes a data processing agreement with Enalyzer as the data processer and the customer as the data controller. Both Enalyzer and the customer are obligated to follow the provisions of the GDPR, and further the customer may be obligated to abide by other data protection provisions in force in the Territory or Territories from which the customer has collected personal data.

As stated in the agreement with the customer, Enalyzer shall use and process the customer's data only in accordance with the customer's instructions with the exceptions stated in the said agreement.
Enalyzer has, as the data processor, taken technical and organizational security measures as described in the present document to secure that the data is not by accident or illegally destroyed, lost or impaired, that the data shall not become known by any unauthorized third person, is misused or is in any other way used in contravention of the GDPR.

Enalyzer hereby states that the data may be processed by the use of home offices.

Enalyzer is registered with the Danish Data Protection Agency as a computer service agency.

3.3 Security incidents

A security incident is an alert that a breach of security may be taking place or may have taken place. An act, event or omission that could result in the compromise of data.

Any suspicion of a security incident found by either Enalyzer or its users must be reported immediately to Enalyzers technical personal, so that further investigations can occur.
3.4 Security breaches
A security incident that leads to a confirmed compromise of data is considered a security breach.
In the unlikely event of any security breach, we will contact the affected users immediately. All necessary actions will be taken to minimize the extend of the breach and to close down all related security wholes. In the notice to the affected users we will include:

1. A situation report
2. A description of the compromised data
3. A description of the planned steps to minimize and control the breach.

3.5 Authorization and access control

Only authorized personal have access to the Enalyzer production systems and data. Authorized personal are only allowed to access customer specific data to solve system issues, or if specifically requested to do so by the customer.

4. Third party approval

Enalyzer Security

4.1 PWC audit Itadel

Since October 2005 $ has been audited annually by PwC (PriceWaterhouse-Cooper), the world's largest professional services firm and the largest of the "Big Four" accountancy firms measured by 2012 revenues.