Barium, Barium Live Security Whitepaper			
Security level: ***Public***	*Last updated:* **2017-12-17**	*Created by:* ***Mika Jolanki***	*Approved by:* ***Björn Asklöf***

Barium Security Whitepaper

This whitepaper applies to Barium Low Code Platform; Barium Live.

Introduction

As a cloud pioneer, Barium's flagship offering Barium Live has been natively in the cloud since November 2008, Barium fully understands the security implications of the cloud model. The intersection of good security and privacy builds trust in a cloud computing system.
To gain the trust from customer, a cloud provider like Barium must deliver levels of security and privacy (not to mention reliability, availability, and performance) that meet or exceed what is achievable with on-premises solutions.

Barium, Barium Live Security Whitepaper			
Security level: ***Public***	*Last updated:* **2017-12-17**	*Created by:* ***Mika Jolanki***	*Approved by:* ***Björn Asklöf***

Barium Live is used by organizations worldwide, from large enterprises with hundreds of thousands of employees to small companies' with just a few employees. The protection of customer data is a primary design consideration for all parts and components (infrastructure, service and personnel operations) when delivering Barium Live. We believe that Barium Live can offer a level of protection that very few public cloud providers or private enterprise IT teams can match. Because protecting data is core to Barium's business, we can make extensive investments in security, resources and expertise at a scale that many others cannot.

In the context of computing, the terms security, privacy, and trust are related, but have different meanings. Security refers to a computing system's level of resistance to threats. Privacy most often concerns the digital collection, storage, and sharing of information and data, including the transparency of such practices. Not before a system is reliable, secure and private can it deserve to be trusted.

Our claim is that Barium Live is trustworthy. This white-paper describes how Barium and Barium Live handles security and privacy with the aim to earn your trust.

Table of Contents

Barium, Barium Live Security Whitepaper			
Security level: ***Public***	*Last updated:* **2017-12-17**	*Created by:* ***Mika Jolanki***	*Approved by:* ***Björn Asklöf***

Barium has a strong security culture

For clients using Barium Live in their day-to-day business it is of the highest priority to know that their information is handled securely and that it is available to the right person at the right time while unavailable to anyone unauthorized. Barium aims for the highest possible security in all aspects of Barium Live and to provide its users with service availability round-the-clock, every day of the year.

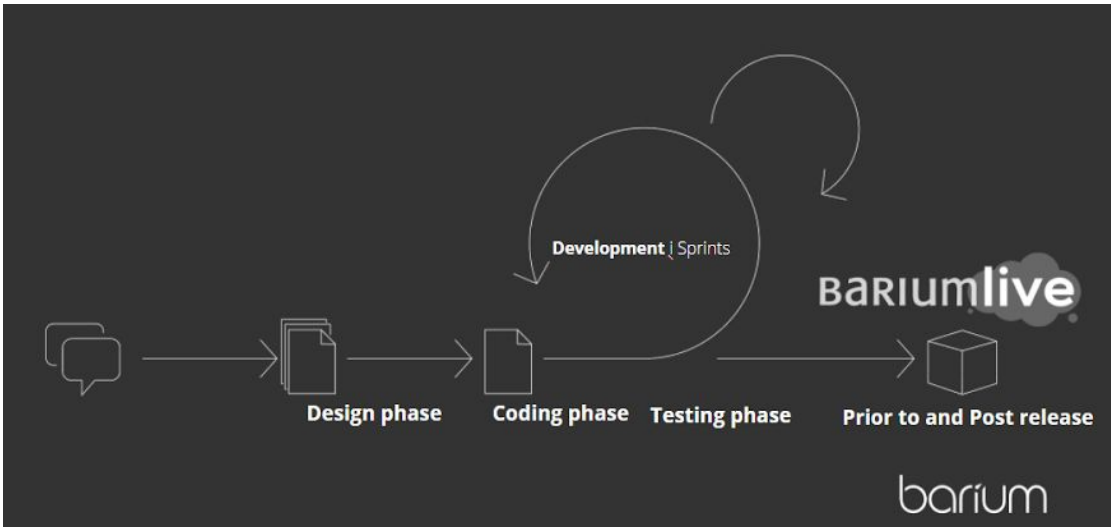
Security and privacy is essential to us:

- It drives our organizational structure, training priorities and hiring processes.
- It shapes our data centers and the technology we use.
- It's central to our everyday operations and disaster planning, including how we address threats.
- It's prioritized in the way we handle customer data.
- It's the cornerstone of our account controls, our compliance audits and the certifications we offer our customers, our ISO27001 certification is a proof point of this.

Barium, Barium Live Security Whitepaper			
Security level: ***Public***	*Last updated:* **2017-12-17**	*Created by:* ***Mika Jolanki***	*Approved by:* ***Björn Asklöf***

Security & Privacy, our way of working

We focus on security and protection of customer data throughout all steps when delivering Barium Live. Barium incorporates security into its platform development processes at all stages. This includes all tasks related to developing, delivering and supporting of Barium Live, everything from initial architecture considerations to post-release.



- **Design phase** – Guiding security principles and required security training help ensure Barium DevOps staff to make the best security decisions possible. Threat assessments on high-risk features help to identify potential security issues as early in the development lifecycle as possible.
- **Coding phase** – Barium addresses standard vulnerability types through the use of secure coding patterns and use of frameworks, and uses both manual and automated code analysis tools to identify security flaws.
- **Testing phase** – Internal Barium staff and independent security consultants use scanners and proprietary tools along with manual security testing to identify potential security issues.
- **Pre and Post release** – Barium validates that the functionality being developed and maintained meets its internal security requirements. Barium uses independent security service providers, both prior to and after the release, to analyze and monitor the product for potential security issues. These reports can in some cases be reviewed with prospects and customers under a nondisclosure agreement.

Barium, Barium Live Security Whitepaper			
Security level: ***Public***	*Last updated:* **2017-12-17**	*Created by:* ***Mika Jolanki***	*Approved by:* ***Björn Asklöf***

Information security management system

Barium Live is certified according to the internationally recognized ISO-27001 information security standard. The certification encompasses development, delivery and support of Barium Live as well as the handling of client data related to providing the service. The standard demands far-reaching business management practices as means to ensure the confidentiality, accuracy and availability of the information handled.

- Confidentiality ensures that information is accessible only to those authorized to have access.
- Integrity safeguards the accuracy and completeness of information and processing methods.
- Availability ensures that authorized users have access to information and associated assets when required.

Adequate risk management and continuity planning are key activities in this work. The systematic work with information security conducted by Barium is an integrated part of the overall business and management structure of the company. Information security is also a top priority when designing all business processes, information systems and security measures.
DNV Business Assurance conducts recurring revisions of Barium's information security practices, auditing it according to the ISO-27001 standard.

Employee background checks

Before they join our staff (sometimes also during the employment) Barium will verify an individual's education, previous employment and also perform internal and external reference checks when applicable. Depending on what kind of customers and solutions the employee will be in contact with Barium may also let relevant authorities and or external services conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the sensitivity to customer information, data and solution.

Mandatory security training for all employees

All Barium employees undergo mandatory security training throughout their Barium careers as part of their day to day business. During the on-boarding process new employees agree to our internal way of working (processes, terms and conditions), which highlights our commitment to keep customer information safe and secure. New employees have to sign off that they have read and understands Barium's information security policy document. Depending on their job role, and customers they will get in

contact with additional training on specific aspects of security may be required. For instance, the development lead for security instructs new developers on topics like secure coding practices, product design and automated vulnerability testing tools. R&D and Product Management personnel also attend technical presentations on security-related topics and discuss security related topics like new threats, attack patterns, mitigation techniques and more.

Internal security and privacy events

Barium hosts regular internal sessions to raise awareness and drive innovation in security and data privacy, these are mandatory to all employees. Security and privacy is an ever-evolving area, and Barium recognizes that dedicated employee engagement is a key means of raising awareness. One example is the Barium employee security awareness training during which all barium employees gets updated Security awareness in all facets, from software development, data handling and policy enforcement to living our privacy principles. Another example are in-depth sessions for R&D and Product Management lead by our security lead where relevant security and privacy topics are discussed in more depth.

Our dedicated Security Officer and his team

Barium has an appointed Security Officer responsible for security issues within our organization and products. Main focus lies within the field of information security and data protection associated to customer data being processed in any of Bariums products. To enhance the level of security, the Security Officer is responsible of maintaining, enhancing and enforcing our Security Information Management System (ISMS). This way we have a structured way of maintaining compliance to security standards and legislations e.g. ISO-27001 and GDPR.

Other important duties and tasks are among others:

- Investigate risk assessments.
- Plan, enhance and conducting security review processes
- Plan and conduct employee awareness educations
- Handle discrepancies and information security incidents
- Perform routine security evaluations and audits
- Engage outside experts to conduct regular security assessments
- Lead activities for penetration tests, security scans for security threats using commercial and custom tools.
- Quality assurance (QA) measures and other software security reviews
- Coordinate security analyzes and penetration tests
- Ensure that on- and off-boarding of Barium personnel is up to date and is carried out fully

- Review our security infrastructure and the related processes to run it

Barium Security Officer also proactively drives activities to ensure that Barium and Barium Live is compliant with security laws and regulations around the world. As new auditing standards are created (like GDPR) Bariums Security Officer determines together with the Product Manager team what controls, processes, and systems are needed to meet them.

Security Lead Developer within R&D

Within R&D there is a designated developer responsible for security-related topics. The Security lead developer educates, documents best practices and raise awareness of security issues and vulnerabilities. The security lead supports the development teams during planning, development and test to ensure secure features. The security lead developer is also responsible for analysing the results of Barium's bi-weekly security scan (performed with an external security scanning tool).

The DevOps teams

The DevOps teams are responsible for monitoring suspicious activities on Barium Live. Barium DevOps teams get alerts on security incidents that might affect Barium Live. The DevOps team actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Barium security staff. Manual task, activities and analysis are supplemented by automated analysis of system logs.

Security requirements

Guiding principles

OWASP - The OWASP Top 10

(https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet#OWASP_Top_Ten_Cheat_Sheet) is a powerful awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications. Project members include a variety of security experts from around the world who have shared their expertise to produce this list. Barium is committed to follow the OWASP recommendations during the development of Barium Live in order to minimize security exposure and to produce secure code. All of the the OWASP Top 10 threats are tested before any public Barium Live release, it's part of our normal development and release processes (we use external specialized tools to validate these requirements, these tests our platform against over 700 known security threats, including OWASP Top 10).

Information management & privacy

ISO-20071

As described earlier this standard takes a comprehensive approach to information security. The standard stipulates over 100 security requirements and control points that modern organizations need to address. Barium has implemented both technical and organizational security measures to ensure full compliance with the requirements. These requirements are tested and validated according to a revision schedule performed by independent parties.

GDPR

The general data protection regulation (GDPR) lists 99 articles including many sub requirements and security controls related to information security with a focus on privacy and personal identifiable information (PII). The GDPR requires organisations to take the necessary steps to ensure that security controls work as designed. Achieving accredited certification to ISO-27001 delivers an independent, expert assessment of whether Barium has implemented adequate measures to protect our customers PII:s. One of the many requirements in ISO-27001 state that: *"A18.1.4 - Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable"*. GDPR is one of these referred legislations that ISO-27001 is

forced to validate. This is the main reason why Barium has implemented the ISO-27001 standard to show compliance to GDPR.

Operational Security

Security is an integral part of our Barium Live operations. Barium Live runs on a technology platform that is conceived, designed and built to operate securely. Our claim is that it is more secure and easier to manage than more traditional on premise solutions. Barium has many layers of defense that repel threats and secure customer data.

Vulnerability management and malware prevention

An effective malware attack or a hidden security leak can lead to account compromise, data theft, and possibly additional access to a network. Barium takes these threats to its networks and its customers very seriously and we use a variety of methods to prevent, detect and eradicate malware.

Barium actively administers vulnerability management tasks and processes to scan for security threats using:

- Combination of commercially available and purpose-built in-house tools
- Regular manual penetration efforts and Continuously executed automated scanners with Detectify (https://detectify.com)
- State-of-art intrusion detection systems (NSS labs Recommended Web Application Firewall from Fortinet https://www.fortinet.com/products/web-application-firewall/fortiweb.html)
- External software security reviews, hacking sessions and audits conducted by security experts such as Sentor (www.sentor.se)
- Quality assurance processes

All of these activities aim to find security leakages, harmful SQL injections, cross site scripting and similar (Detectify alone test our platform against over 700 known vulnerabilities, including the ones listed in OWASP Top 10).

Barium also monitors application and database activities and uses event management tools that pings the DevOps teams attention for potential internal and external threats. The DevOps team together with the Barium Security Officer is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, put high up in the product backlog and firmly released on Barium Live.

Incident management

We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the Security Officer logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities.

Monitoring of services from Customers end

Barium uses several external and internal services for monitoring Barium Live. Some of these are available for our customers to allow them to see and monitor status of Barium Live themselves. A publicly available Pingdom status page can be found at http://stats.pingdom.com/nniqhyze09ob that displays uptime and status of the Barium Live services. A more detailed status page with information about individual subsystems can be made available on request.

Administrative access

To keep data private and secure Barium Live logically isolates each customer's data from that of other customers and users. Only a small group of Barium employees have access to customer data and this access is controlled and approved through an "Request access to production environment" process where requests are motivated, logged and approved. Access is only approved for a set period of time and the process ensures that access is removed after the approved time slot.

Access is granted on a per system level meaning that a technician that needs access to a web server won't automatically have access to customer data. Access to the databases and customer data must be explicitly requested and approved.

For Barium employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities.

All system access in the production environment is also logged, separately from the request access logs. The combination of these two separate tools and logs ensures that the modification of authorization settings and the approval process is done in accordance with our approval policies and processes.

When access to the production environment has been approved the employee must connect to the production network with two-factor authentication and then the employee's unique user id and password are used to control access to all resources, including databases.

Administration in Customer solutions

Within customer organizations and projects in which Barium Consultants or other roles are involved, administrative roles and privileges for Barium Live are configured and controlled by the solution owner (the customer). Access to customer solutions can at any time be changed and revoked by the solution owner (customer).

Third-party suppliers

Barium may engage some third-party suppliers to provide services related to Barium Live, including customer and technical support. Prior to onboarding third-party suppliers, Barium conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Barium has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms. This include the rare case when a third-party supplier needs to process customer data (including PII:s) to fulfill Bariums agreement towards our customers. In these cases the contract clearly state what a subcontractor can and cannot do when processing the data. All according to GDPR article 28.

Data Usage

Barium Live customers always own their data, never Barium. The data that customers put into our systems is theirs, and we do not use it in any way for our own purposes nor sell it to third parties. We offer our customers a detailed data processing amendment that describes our commitment to protecting customer data. It states that Barium will not process data for any purpose other than to fulfill our contractual obligations. Finally, we provide REST based APIs that make it easy for customers to take their data with them if they choose to stop using our services, without penalty or additional cost.

Retention policy

To allow our customers to comply with regulatory requirements and company policies we offer a variety options to control redaction of data. There are options to redact all

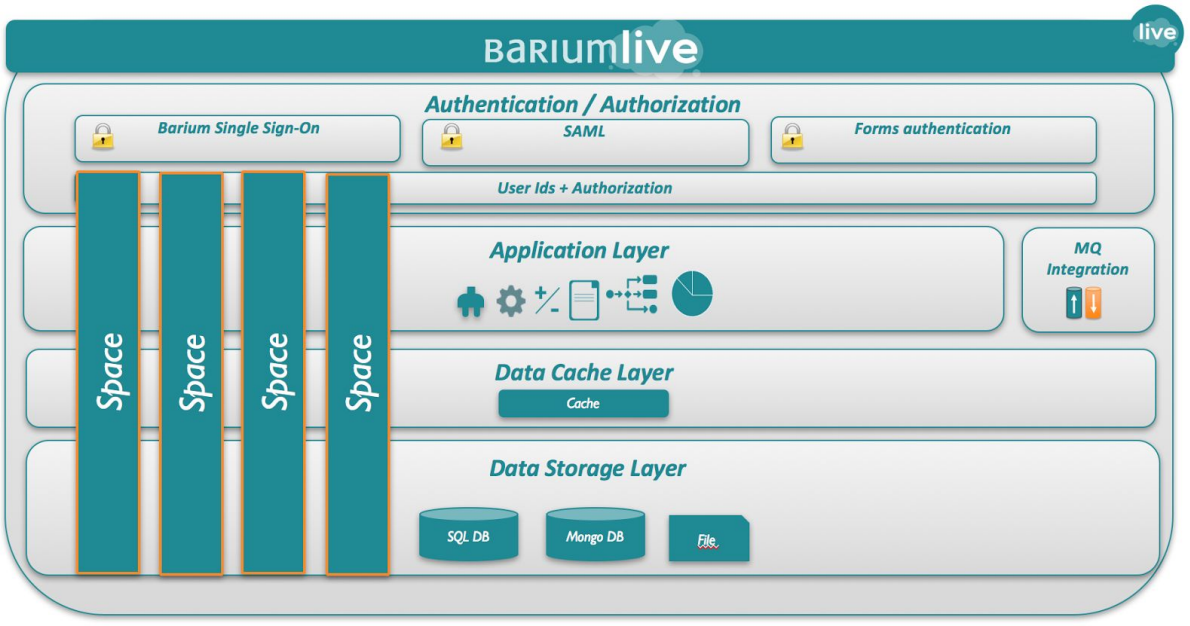
data or to specify it more granularly at application level. It's also possible to specify when redaction should occur.

Technical implementation

Built in security in Barium Live

All customer data resides within a space. The space is the entity for multi tenancy and data within a space is not available in other spaces. This logical separation runs through all layers of the technical implementation.

To be able to see any information at all within a space the user needs to be a member of that space. Within each space there are two levels of additional security models controlling the access to information. First all users in a space have explicit permissions to access individual modules in Barium Live. This means that a user that only have access to the process modelling module won't have access to information in any Barium Live applications, in that space, regardless of other permission settings.
Secondly objects in Barium Live have explicit permissions defining who can view, edit or manage that specific object. This permission model alone would ensure customer data separation. The concept of a space and the validation also on this level is to have a redundancy in the logic for separating customer data with the purpose to not have a possible "single point of failure" in this critical logic.



Authentication

All access except publicly shared objects requires the user to be authenticated. Users authenticate by using the built-in in login form or a single sign-on mechanism via the customer's identity provider (IdP) using SAML (Security Assertion Markup Language).

- **SAML** - Federated authentication single sign-on using Security Assertion Markup Language (SAML) allows a session to send authentication and authorization data between affiliated but unrelated Web services.
- **Form based login** - User provide a username and password (credentials) to establish a connection

An authenticated user is connected to one or more spaces (tenant container) and groups within the spaces.
All communication and data transfer to Barium Live is encrypted by Transport Layer Security (TLS) using the latest in encryption technology concerning protocols, ciphers and algorithms. To protect established sessions, Barium Live monitors and terminates idle sessions after a configurable period of time. Barium Live session security limits help defend system access when a user leaves his/her computer unattended without first disconnecting.

Endpoint protection

Endpoints within a space are located under a https endpoint starting with /spaces/[space identifier]. A user is blocked if trying to access any url for a space where he/she is not a member. This security feature is implemented at base class level and not necessary to add for each endpoint method to ensure that all endpoints have this protection by default. There are also role and permission based access checks performed in this layer to determine if a user is allowed to access a specific endpoint.

API endpoints

When accessing the API you need to authenticate with username and password. You also need to provide an api-key to be able to get a ticket for accessing the api. There is a separate api-key for each space that is managed by the customer. The customer can at any time revoke an api-key.

Application layer

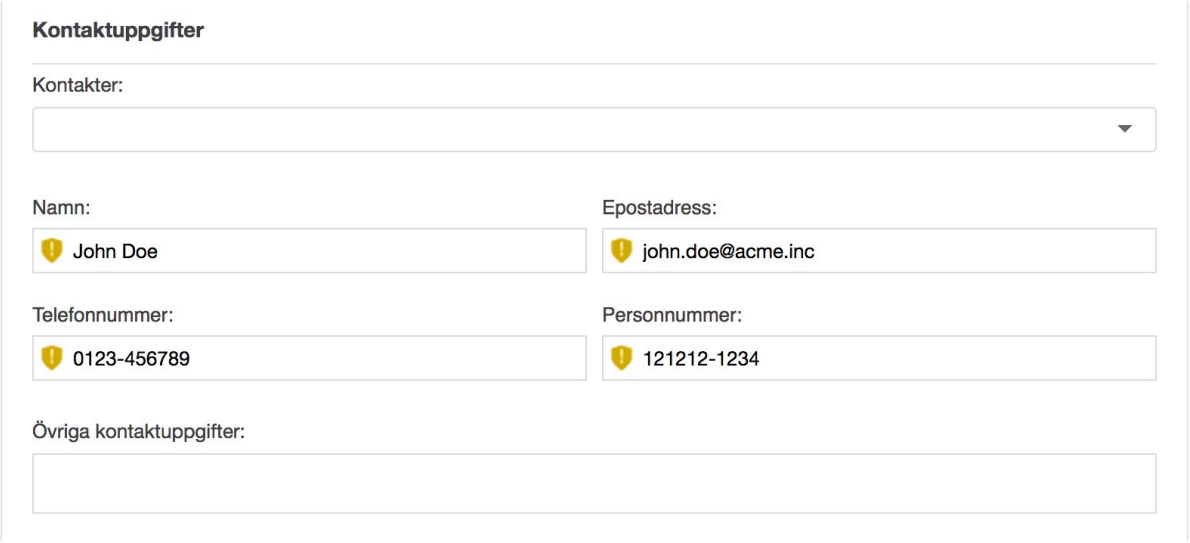
The space identifier verified at the endpoint is used for access within the application layer. Queries are filtered by space as an extra measure to ensure no data from other spaces is included. Access to objects in the system are restricted by permissions. The user will only be able to access objects (processes,files etc.) to which he/she has been granted access, either individually or by group membership. All spaces have distinct groups so this feature alone prevents a user to get data from a space he/she is not a member of. Additional role and permission based access checks performed in this layer depending on application feature.

To ensure encapsulation of data within a space we have an extensive set of tests. Unit tests, integration tests as well as both manual and automated UI tests cover encapsulation of data.

Confidential field-data

Today, we have the option to define certain fields as containing confidential data. This is primarily used in applications such as managing social management cases that contain personal data. What the function allows us to do today is that in a more granular way ensure that only appointed administrators or certified personnel have the rights to view this information. It is also possible to set rules of thinning that only affect these fields, etc.

These fields provide increased security around those who are able to view the information but also with restrictions in terms of how to use the confidential information. For example, you can not present this information in lists, index or search it, sort it, or let the process make decisions based on the information.

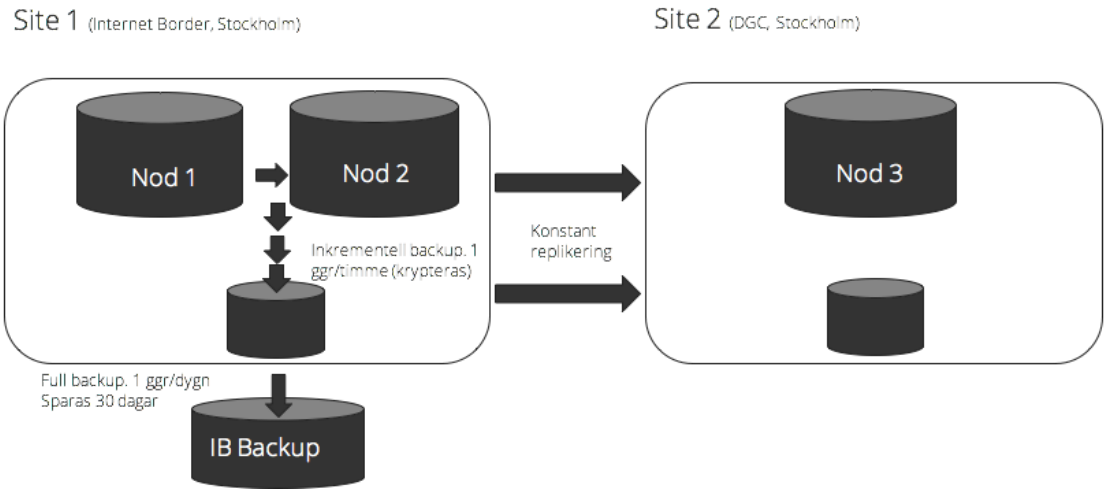


Backup Routines

All data handled using Barium Live is stored and processed within Sweden's borders. To ensure efficient and secure data management, backups on customer data are combined with server backups ("snapshots" on virtual VmWare-servers) as follows:

- Data is incrementally secured once per hour, rolling for 48 hours, to a primary node / file server. The backup is then replicated via DFS to a geographically separated second node. These encrypted backups are saved 48 hours.

- Every day, a fully encrypted version of the service's data is backed up. The backup is saved redundantly on several geographically different nodes for 48 hours.
- On virtual machines (VmWare images), encrypted backups are taken once a night, these are saved separately for 30 days at our hosting-partners safe location.
- VmWare images also capture encrypted snapshots, which are saved for 24 hours.
- There is also the possibility, if desired, for customers to take backups of their own data that is handled on Barium Live using the service data API.



Securing data at rest

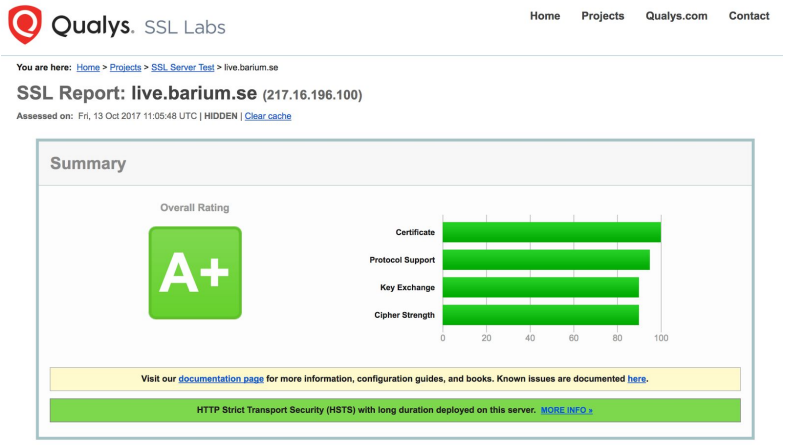
Barium Live database is encrypted with the MS SQL Server function Transparent Data Encryption (TDE). TDE encrypts all SQL Server data files (data and log files) in real-time, also known as encrypting data at rest. Since all data in the database is encrypted this prevents anyone without the keys from using the data. You can read more about the feature here: https://docs.microsoft.com/sv-se/sql/relational-databases/security/encryption/transparent-data-encryption

Securing data in transit

Data is vulnerable to unauthorized access as it travels across the Internet or within networks. For this reason, securing data in transit is a high priority for Barium. Barium

Live support strong encryption protocols such as TLS to secure the connections between customer devices and Barium's web services and APIs.

Barium continuously validates this with services like Qualys SSL Labs where we aim to always have the highest possible rating for every frontend instance.



Disaster recovery

We rely on our geographical redundancy that makes us independent of a single datacenter. The production environment is based on High Availability (HA) where every component is split up in at least two nodes, each in a different geographical location, replicating data in realtime. Even if both locations should become unavailable, we still have our backups to start up our platform in a third datacenter that our hosting-partner provides.

Highly available solution

All vital components for delivering Barium Live are redundant, this redundancy applies to our infrastructure, how we store data, network and Internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependent on a single server, data center, or network connection. Barium’s data centers are geographically distributed to two locations in order to minimize the effects of regional disruptions on global products such as natural disasters and local outages. In the event of hardware, software, or network failure, platform services and control planes are automatically and instantly shifted from one facility to another so that platform services can continue without interruption .

State-of-the-art data centers

Barium has commissioned a professional subcontractor to provide a safe, redundant, modern and efficient data center. These data centers physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and the data centers floor features laser beam intrusion detection. These data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Access to the data center floor is only possible via access control using security badges. Only approved employees with specific roles may enter.

To keep things running 24/7/365 and ensure uninterrupted services, Barium's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Fully redundant cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment help prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks.