



Borealis Security Infokit

Borealis provides a secure collaborative work platform for large infrastructure projects to manage social and environmental risks. We feature powerful data management tools, customizable platforms, and analytics capabilities into one workspace. Our product follows the Software-as-a-Service delivery model and also supports On-Premises software deployment.

Borealis integrates industry-standard security practices in its software and extends them to data storage in a hardened hosting infrastructure.

Security has been integrated into the architecture, policies, and procedures of the Borealis application. This paper focuses on some of these measures, including:

Confidentiality

Security in operations

Data security

Application-level security

Organizational security and change management processes

Security certification and accreditation

Data center security implementation

Privacy

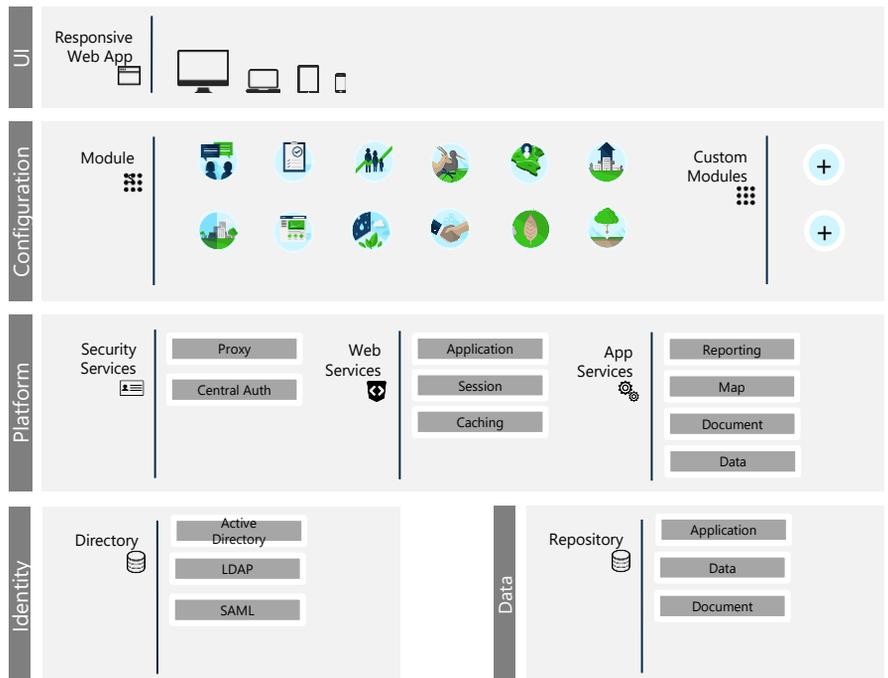
Borealis Platform Security Overview

The Borealis application is designed to organize functional and security aspects into well-defined multi-tenant layers: presentation, configuration, platform, and database.

Only application administrators are allowed to create users and assign data security rules. The access control is based on a roles hierarchy. Data can be segregated by group of users.

All accesses are governed by strict password security policies with configurable complexity.

All activities performed within the application are logged with Audit Trail.



Confidentiality

- At Borealis, confidentiality begins with contractual agreements to which all our employees and consultants must adhere to, followed by our Security Awareness Program, which is conducted on a yearly basis.
- To ensure confidentiality is implemented as defined, we only grant access on a *need to know* basis to information entrusted to us.
- We treat all client information with the utmost level of confidentiality and by default, we classify all client information and data as confidential. In that perspective, we encrypt client data, ensure that access is limited to a *need to know* basis. The encryption methods we use are kept up to date. Our Risk Assessment methodology ensures that controls are in place and work appropriately to protect client data.

Security in operations

Risks Assessments

Through our risk assessments and vulnerability detection and prevention mechanisms, we respond to security events and incidents that could impact our infrastructure. This function involves the overarching networking and physical environment including the monitoring of internal networks and employee access customer environments.

Configuration Hardening and Monitoring

Hardening is part of our server build books. Through proactively monitoring changes to the environment, deviations are identified in real-time and are reviewed for change legitimacy. Any change identified as not legitimate triggers investigation and appropriate actions are taken. We assign security configuration profiles to hosts based on accepted standards and best practices.

Patch Monitoring

We constantly monitor, verify and take appropriate actions to address threats that are applicable to our environment, including which Common Vulnerabilities and Exposures (CVE) are present.

User Monitoring

We monitor and document user host access, authentication level and login times to demonstrate compliance to access controls.

File Integrity Management

We detect, report, and document changes to files in alignment with security and compliance requirements.

Security Incident Management

If and when security incidents occur, we respond in a timely manner to incidents, through investigation to identify the nature of the incident, the impacted clients and work closely with all relevant parties to address and resolve the issue followed by documented lessons learned which are fed back to the policy and planning functions as part of our security management system to drive continuous improvement of our practices.

Data Security

The data is logically separated in instance, and each instance is an individual physical entity. Connection to the data store is restricted through access credentials configured and stored within the platform layer. The platform is built over a multi-tenant architecture enabling multiple footprint scenarios, from corporate wide deployments involving partners and contractors to project sites deployments.

Multi-Tenant

All business units are installed on one installation, but do not share a common database. Share a same version of the Borealis application but may be configured independently of each other.

Multi-Instance

A tenant may have multiple instances, assigned for example to different environments. Each instance may be configured differently.

Data Segregation with Row Level Security

Within an instance, data segregation may be enforced to hide or show information according to user permissions. Groups are defined and associated to users to control access on records. The Borealis application supports a hierarchy of control to build a complex data segregation between teams, business units, contractors, and partners.

Application-Level Security

The Borealis application provides a range of application-level security mechanisms that allow to fine-tune the implementation to meet specific requirements. Software architectural patterns are strategically selected around data confidentiality, integrity and availability. These patterns include row level security data segregation, roles-based access control list, audit trail, and log management.

Authentication

The Borealis application supports multiple authentication providers and complex password policies. LDAP, SAML and Active Directory services can be integrated for enterprise authentication.

Administration

Security and privacy are enforced at the instance level. An instance contains a data store and its users. Users in an instance can never see into other instances. The application contains a self-service administration console, super users can manage their own users: add users, deactivate users, assign user profiles, access login stats, access audit trail, change preferred language, etc.

User roles and groups permissions

Each granular action can be controlled by configurable permission. Permissions are assembled in user profiles defined by roles and groups.

Communication

All communications with the Borealis application are encrypted using high-grade SSL with 256-bit AES, a cryptographic protocol which is designed to provide communication security over the Internet. Encryption keys are securely stored. Individual user sessions are identified and re-verified with each transaction, using a unique token created at login.

Organizational Security and Change Management Processes

On the Borealis application, secure operations extend beyond putting the right systems and technologies in place. Our effective security infrastructure is also embedded within our organizational culture and everyday business processes.

Change management also is a critical aspect of Borealis' security. From development to operation stages, our processes integrate security best practices in the full product lifecycle during requirements, version control, continuous integration testing, packaging, deployment, and quality control. We also proactively monitor for security vulnerabilities and incidents.

People Access and Global Support

The Borealis operations and support team monitors our infrastructure 24/7. Access control is enforced with policies to control user registration, grant the correct level of access privilege, control password use, password change and password removal, review of access rights, and control network service access.

Our support team maintains an account on all hosted applications for the purposes of maintenance and support. Applications and data are accessed only for health monitoring of application purposes, to perform system or application maintenance, and upon customer request via our support system. Only security qualified and authorized Borealis employees have access to system using 2-factor authentication. Customers are responsible for maintaining the security of their own login information.

Monitoring and Vulnerability management

Borealis uses third-party security specialists and enterprise-class security solutions (like Qualys) to find & help us fix vulnerabilities in the IT infrastructure and the web application. Reports of latest third party intrusion tests as well Qualys reports are available upon request.

Borealis uses vulnerability management systems to continuously secure the IT infrastructure against the latest Internet threats. A web application scanning system automatically identifies OWASP top 10 risks including SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and URL redirection.

All web applications, network and hardware are constantly monitored by both Borealis and the managed Infrastructure-as-a-Service (IaaS) providers.

Technologies

The Borealis Application uses recent technologies and constantly evolves with them. The latest features available for these technologies are also available for the app, which ensures a high level of security for our backend. For example, security issues are quickly rectified. Plus, new versions are released on a regular basis.

Here are some of the technologies we built into our app:

- Node.js
- MongoDB
- PostgreSQL
- Apache2
- OpenSSL

Privacy

Borealis understands the importance of ensuring the privacy of your information.

For more information, please see our Master Subscription Agreement:

<https://www.boreal-is.com/terms-of-use/>

Borealis Security Certification and Accreditation

Borealis offers solutions designed and used by many large organisations. We adhere to the highest industry standards for enterprise security to maintain confidentiality, integrity, and availability of our customers' information.

Borealis Security

To ensure Borealis security requirements and sustainability policy, our service is collocated in dedicated spaces at a top-tier data center that maintains industry-standard certifications. We perform third-party security audits of our product and infrastructure regularly. Furthermore, we reinforce internal security with various politics and processes to protect access to data.

Tier 3 certified design and SSAE 16 compliant data center

Borealis hosting services are deployed in a Tier 3 certified design data center. OVH is certified ISO 27001:2005 for providing and operating dedicated cloud computing infrastructures. OVH is based on the ISO 27002 and ISO 27005 security management and risk assessment norms and associated processes. OVH has obtained SOC 1 and 2 type II certifications.

Data Center Security Implementation

Borealis' hosting services are built on top of enterprise-ready co-managed services from OVH in Canada and in France, and from Amazon AWS in Australia. A scalable, distributed computing infrastructure is used to host and manage the Borealis application. To ensure it has control over its capacities, Borealis chooses where client data is hosted: should a client require a specific production data center or data center replication location, some fees apply.

Data Center Security

Borealis production servers are hosted in Tier 3 certified design data centers (Uptime Institute rating). The facilities are ISO 27001: 2005, SOC 1 type II (SSAE 16 and ISAE 3402) and SOC 2 type II compliant. The data centers are equipped with robust physical security including biometrics and smartcard access and logical security including firewall, intrusion detection, video surveillance and prevention, and denial of service attack protection. Redundant and diverse power, cooling and networks are built to a minimum of N+1 redundancy. The Cloud Security Alliance STAR self-assessment are available:

<https://cloudsecurityalliance.org/star-registrant/ovh/>

<https://cloudsecurityalliance.org/registry/amazon/>

Data Center Efficiency

The customized, inherently redundant, modular design guarantees an unprecedented industry leading 1 to 1.2 Power Usage Effectiveness (PUE), which will drive efficiencies in performance and environmental sustainability. 98% of OVH hosting rooms are free from air conditioning. The Water cooling enables 70% of heat emitted by the processors to be dispersed.

OVH and Amazon AWS Data Centers

For more information on data centers, see

<http://www.ovh.com/ca/en/about-us/>

<https://aws.amazon.com/>

Physical Infrastructure

The Borealis infrastructure, including network switches, firewalls, servers, and shared storage devices, is managed and configured by Borealis personnel, in conjunction with the OVH support team. OVH is a top provider of managed services and has achieved a high standard regarding its security certifications. All Borealis services are configured for high availability with automatic failover capabilities. In the hypothetical situation of downtime on a physical server, the virtual machines that host the Borealis Application will automatically restart on another available physical server to keep downtime to a minimum.

Backup

Complete virtual server backups are made on a daily basis. Backups are retained with the following policy: retain the 5 most recent backups as well as the most recent backup from each of the last 7 days, 4 weeks, 12 months, and 1 year.

Disaster Recovery

Borealis uses multiple data centers to host its application and data, providing essential redundancy. All data centers employ physical security, strict access policies and secure vaults and cages. The disaster recovery center is located at more than 100 km (62 miles) from the production data center. Borealis service performs near real-time data replication between the production data center and the disaster recovery center. Hot-site disaster recovery tests are performed daily and complete disaster recovery diagnostic is done quarterly to verify our projected recovery times and the integrity of the customer data.

Network security

The Borealis network is protected by enterprise grade firewall and Intrusion Prevention and Detection System (IPS/IDS) to monitor network traffic in order to block a wide range of known vulnerability exploits. The OVH network is protected against DoS/DDoS attack.

Transmission

Multiple Internet backbone connections provide routing redundancy and high-performance connectivity.

Privacy

We place a very high value on the protection of privacy.

Every day, businesses are at risk from a security or data breach which can come from anywhere in the world. There's so much at stake, from the sensitive data that gives you industry insights to the trust you've built with your customers - trust that can be hard to regain and breaches that can force many companies into bankruptcy following negative advertisement resulting from such breaches.

As opposed to other organizations, we imbed privacy by design through all the gates of our development lifecycle.

Thinking and addressing privacy, compliance and security after the fact, results in increased costs to implement risk mitigation. We at Borealis, address these from the design phase and constantly review our solutions to ensure adherence to these privacy principles.

Privacy requirements are backed into our solution to ensure that data hosting facilities meet Privacy requirements.

When required specifically by a client and in order to meet their specific privacy and regulatory requirements, we will work with the client and through contractual agreements to host their data in a data center of their choice, with the client's formal approval of the country where their data will be hosted.

For the full Privacy Policy, please go to: <https://www.borealis.com/privacy-policy/>

We're here to help. Ready to simplify operations?

Contact Us

+1 819 575-6037
Mon - Fri / 8am - 5pm EST
contact-us@boreal-is.com

Address

Borealis
175, rue Péladeau, Magog (Qc)
J1X 5G9 Canada

