boardlogic

Security Whitepaper

www.praxonomy.com

Table of Content

Security Whitepaper

At Praxonomy, security is our number one priority. Our application is secure-by-design and provides a protected environment for you to manage your board work. A sophisticated information security management system is implemented to protect the confidentiality, availability, and integrity of your assets on our system.

In this whitepaper, we outline Praxonomy's approach to security for the Boardlogic Board Portal.

Infrastructure

DATA CENTRE

The data centre is one of the key components of the Boardlogic Board Portal. Our data centre provider is located in Europe, a strategic choice for security and data privacy protection. It is both ISO 27001 and NEN 7510 certified, which aligns with Praxonomy's internal standard for information security management.

ARCHITECTURE

"Security-by-Design" is the design principle of our architecture. By adopting highly secure industry standards and best practices, we built a robust system with confidence.

NETWORK SEGREGATION

Systems with different operational functions are separated from each other in different "zones" for greater security and optimal performance. For example, testing or development systems are always hosted in a separate network from production systems. *(see figure 1)*

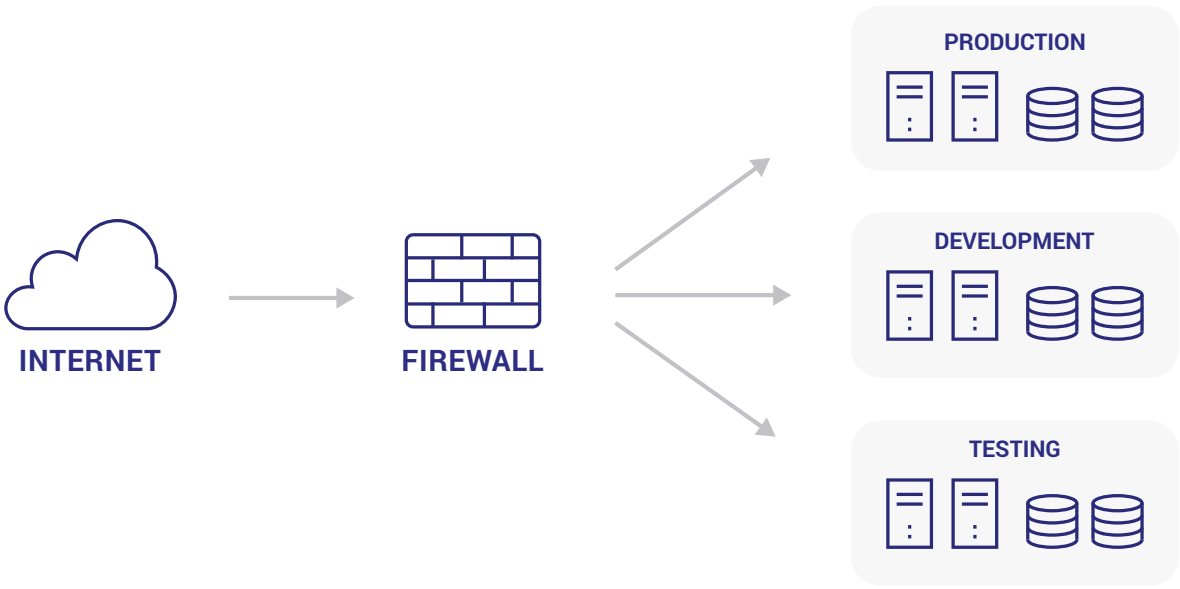


figure 1

NETWORK SEGMENTATION

Infrastructure components within a network are further isolated to independent segments based on their functionalities. Security controls are tuned specifically for each segmented network. And only trusted traffic is allow to be routed through the segmented layers. If a security incident arises, the affected entity can easily be isolated. This prevents attackers from disseminating and propagating malicious attacks over the network.

DEMILITARISED ZONE (DMZ)

As part of network segmentation, a layer of security, the Demilitarised Zone (DMZ), is setup to isolate the external network and the protected internal network. The external network can only access the exposed components at the DMZ, whereas the rest of the critical components stay inside the protected, enclosed network. *(see figure 2)*

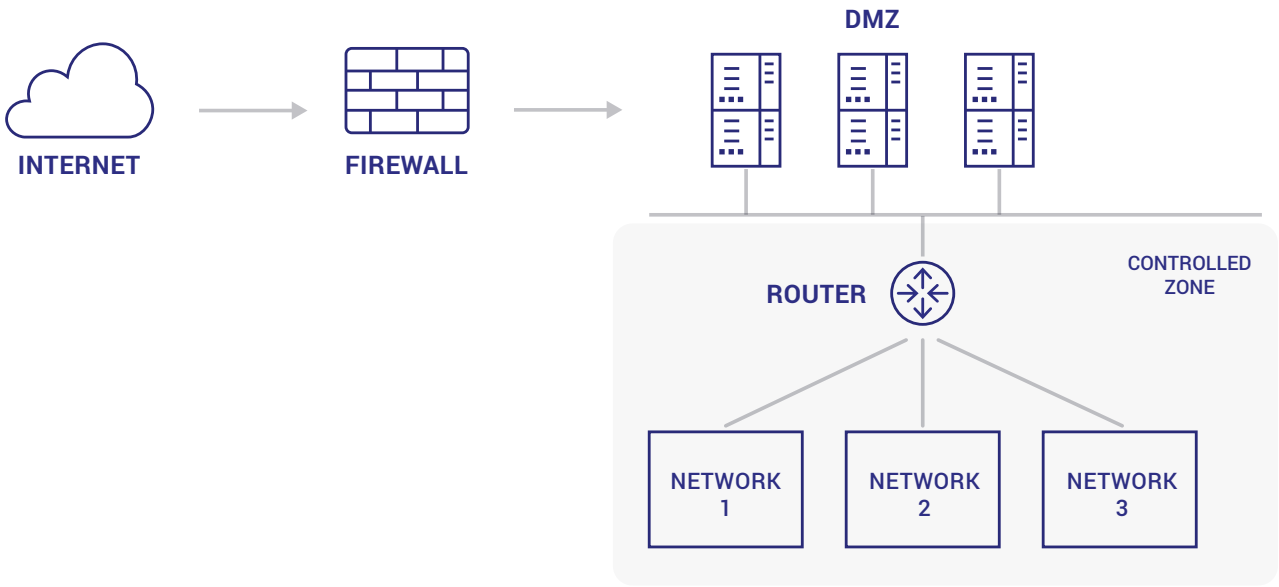


figure 2

ENCRYPTED DATABASE

Transparent Data Encryption (TDE) is a technology to protect “data-at-rest” by encrypting the database (both the physical file and the backup) . TDE is enabled on all Boardlogic production databases to secure the data of our clients.

NETWORK SECURITY

Multiple layers of defences are implemented at the edge and in the network to protect the availability and integrity of the application's data and systems.

FIREWALL

The firewall is set-up using a "deny all" approach. Rules are carefully designed and explicitly added to authorise necessary traffic. All changes to the rules must go through Praxonomy's Change Control Management procedure for review and approval.

INTRUSION PREVENTION SYSTEM (IPS)

IPS is deployed to proactively detect and handle threats. This provides a secondary layer of defence to stop suspicious traffic from entering the network.

ANTIVIRUS

Antivirus software is installed on all servers. Regular updates are performed on both the database and firmware for protection. Regular full system scan is setup to ensure the entire system is scanned using the latest virus definitions.

OPERATIONAL SECURITY

PHYSICAL SECURITY

Physical access to data centres is protected 24×7 by advanced, multi-layered security systems which include documented security policies and procedures for access, round-the-clock onsite security officers, CCTV surveillance, motion detection as well as biometric access control card readers.

RESTRICTED ACCESS

Only a dedicated group of employees are permitted to access the hosting environment. Access rights are assigned based on job role and functions, following the concept of need-to-know and least-privilege access. Necessary rights are only granted to appropriate individuals.

CHANGE CONTROL MANAGEMENT

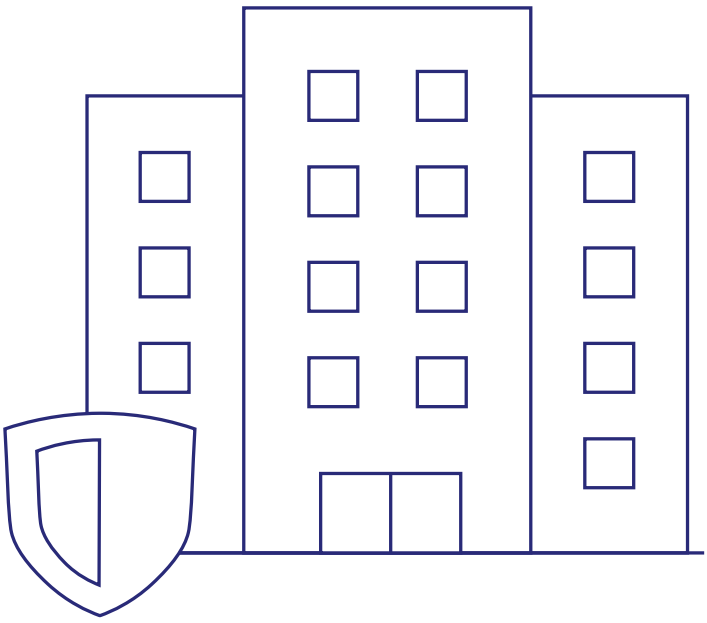
All changes to the operational environment must go through Praxonomy's Change Control Management procedure and an approval process. This maintains the integrity of the systems. Details of changes are recorded and kept. No changes can be deployed to the production environments without managerial review and security/risk analysis.

MONITORING AND LOGGING

System performance, access, and traffic, are monitored and reviewed regularly to ensure the integrity, confidentiality, and availability of the system. Proactive alerts are setup for abnormal system access and/or traffic.

PATCH MANAGEMENT

Outdated software can be a serious vulnerability. At Praxonomy, we have regular procedures to maintain and apply patches to all infrastructure components. This ensures our system is fully protected at all times.

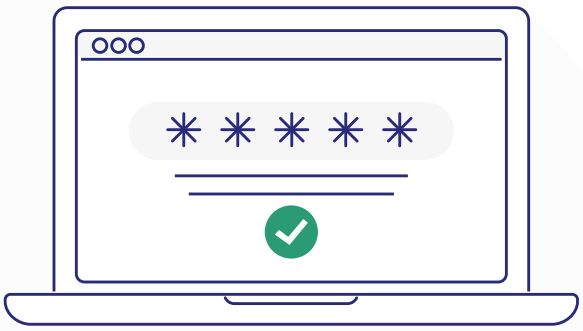


Application Design

Boardlogic is supported by an in-house developed, state-of-the-art framework that references industry standards and Best Practices. We exercise prudence in selecting third-party components for integration to prevent security vulnerabilities.

AUTHENTICATION

A secure session is established each time a user logs on to the system, allowing them to securely work within the Boardlogic Board Portal. In parallel, users are automatically logged-off from the Boardlogic Board Portal after a defined maximum idle period. This prevents unattended user sessions from exploitation.



AUTHORISATION

After authentication, the authorisation mechanism in the system determines if a user is granted with access to certain functionalities or resources. Authorisation on privilege escalation can be classified into two main types: horizontal and vertical. For horizontal access control, users only have access to information within his/her authorised committees or organisations. Access to information in an unauthorised committee or organisation is forbidden. For vertical access control, granular access control can be setup to assign different, customised privileges to different users. They are not able to execute an action without the right permissions.

Access control design should be simple and straightforward. Complex access controls will only lead to misconfiguration and consequently, permission or data leaks. In the Boardlogic Board Portal, permission setup is always intuitive and secure.

DATA SECURITY & ENCRYPTION

ENCRYPTION IN TRANSIT

Transport Layer Security (TLS 1.2) is enforced to create an encrypted communication channel, with at least 128-bit encryption, between clients' devices and Boardlogic's servers for data transfer. *(see figure 3)*

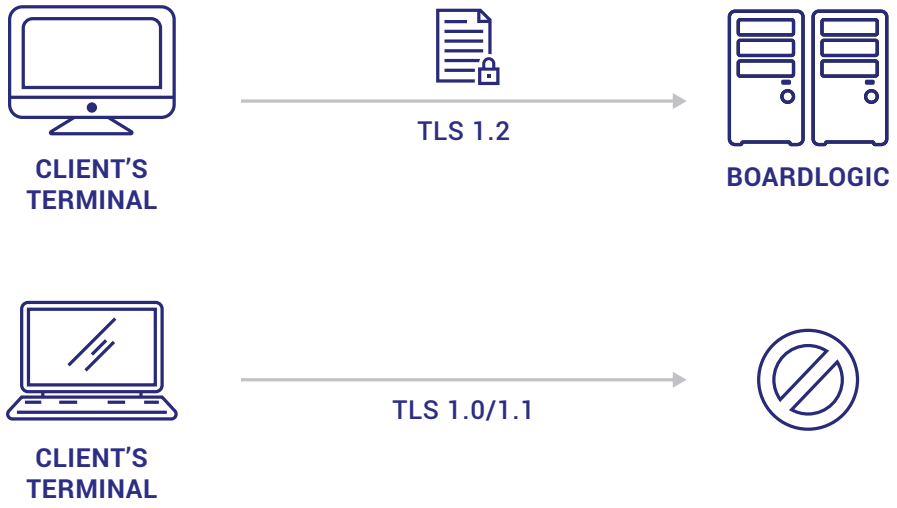


figure 3

PARAMETER PROTECTION

Data is cryptographically protected by TLS while it is in transit. To prevent possible manipulation to the URL parameters or form data before they are in transit, Boardlogic utilises sophisticated encryption techniques and session-based tokens to protect data against attacks (e.g. URL Manipulation and Cross-Site Request Forgery [CSRF]). Furthermore, only needed and minimal parameters are sent through URLs to avoid unnecessary disclosure of sensitive data.

ENCRYPTION AT REST

Database

The physical file of the database is encrypted with AES-256 using MySQL Enterprise Transparent Data Encryption (TDE). The encryption happens in real time. Therefore, data is encrypted prior writing into storage and decrypted upon retrieving from storage. All unauthorised users will not be able to read the data directly from the database file. *(see figure 4)*

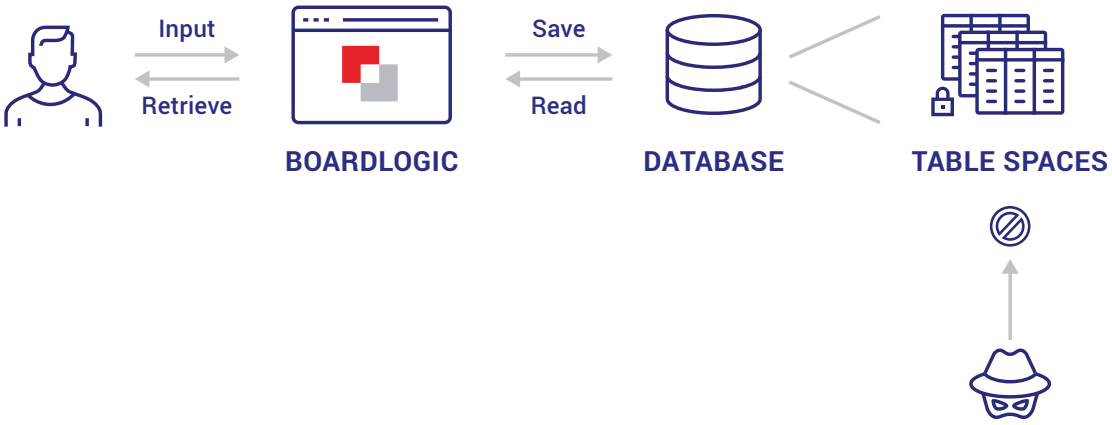


figure 4

Files

Hybrid cryptosystem

All files uploaded to, or generated within Boardlogic are encrypted. To maximise protection, we have implemented an in-house designed hybrid cryptosystem that incorporates the advantages, such as security complexity and performance, offered by various industry-recognised encryption algorithms. Among the algorithms employed, at least AES-128 and RSA-2048 are used.

Inside the Boardlogic portal, each file is secured by multiple layers of protection. When a file is uploaded to the system, it will be encrypted immediately by a system-generated (unique) key. Once the file is secured physically, the key will be further secured by a Key Protection Mechanism, forming a second layer of defence. The Key Protection Mechanism encrypts the unique file key and generates a specific key set for the file owner. The Key Protection Mechanism supports both online and offline encryption. *(see figure 5)*

Shareable encrypted files

In addition to physical protection, files are safeguarded by a third level of security – Access Control. Although each user has his/her own set of keys for file encryption, encrypted files are shareable within the application. The file owner can share a file to the selected users along with specific permissions (e.g. Read Only, Download or Manage, etc). When a file is shared, the Key Protection Mechanism will generate another set of user-specific keys to the permitted users. The permitted users will then be able to decrypt and retrieve the file using his/her own set of keys.

It is through Boardlogic's multi-layered file protection that we can ensure the security of documents stored within the application. This design guarantees that only the file owners and the users who have been granted the appropriate permissions can decrypt and view a file. *(see figure 5)*

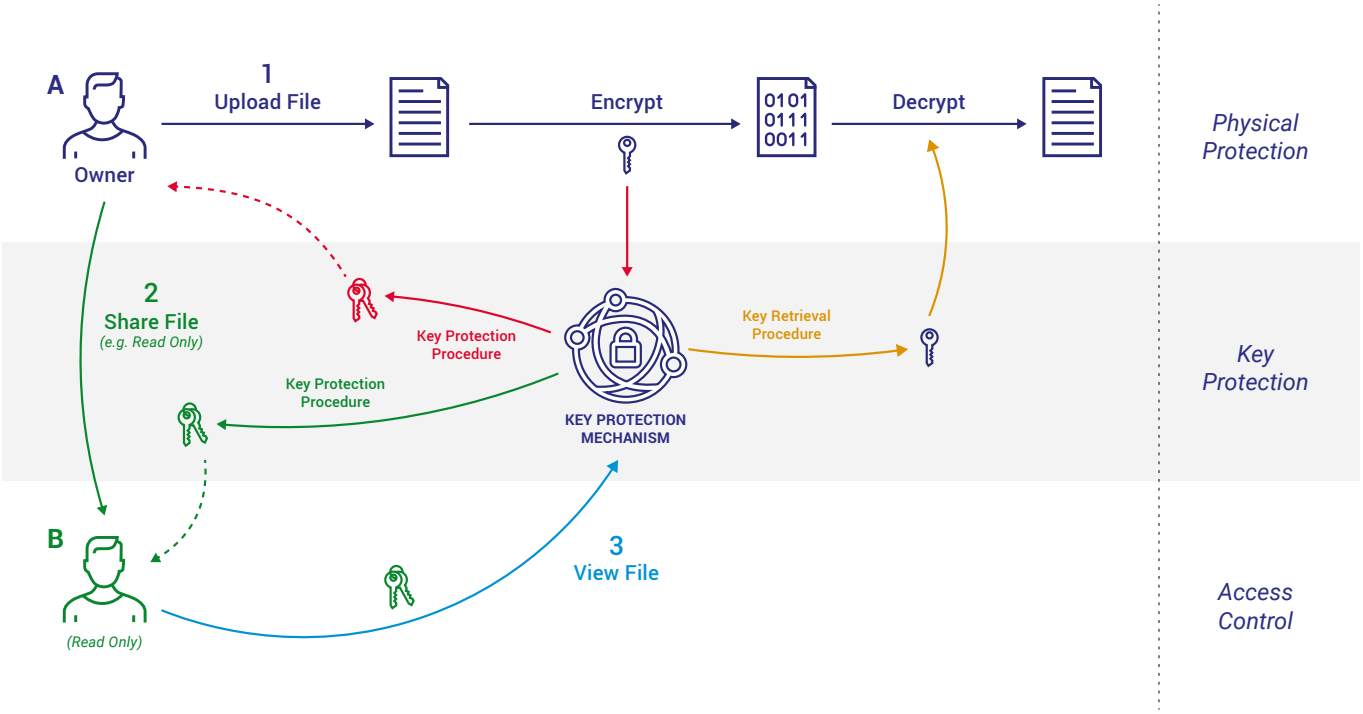


figure 5

File Storage

Encrypted files are stored on our repository server with an arbitrary file name. No one will be able to lookup a file by its original name within the repository. The arbitrary file name provides an additional layer of complexity and security to protect the encrypted files.

SECURITY ASSESSMENT

PENETRATION TESTING

To protect the application from hidden risks, Praxonomy regularly hires independent professional security consultants to perform penetration testing against the application and its infrastructure. A thorough assessment was performed to identify vulnerabilities and attempt to gain unauthorised access to data and documents. Penetration testing results are available for review upon request.

OWASP TOP 10

OWASP (The Open Web Application Security Project) is an international non-profit organisation dedicated to web application security. Security experts from all over the world contribute to the “OWASP Top 10” ---a regularly updated document that highlights and addresses relevant security risks for web applications.

At Praxonomy, known vulnerabilities like those in the “OWASP Top 10” are assessed and evaluated. Corresponding controls and measures are integrated into our development processes and security best practices to minimise vulnerabilities.

SECURITY SCAN

Security scans are executed regularly to ensure the application is safe from known risks.

> "In light of this Cure53 black-box security assessment, it can be stated that the Boardlogic application makes a rather positive, robust impression."
>
> **Dr.-Ing. Mario Heiderich**
> *Founder of Cure53, Berlin-based cybersecurity firm*

SECURE DEVELOPMENT

The human component remains to be a significant vulnerability when it comes to information technology security. As part of the Information Security Management System (ISMS), we have established development procedures to ensure the overall security of the application. For instance, we have proper processes to define and review requirements, developer guidelines and stringent coding standards to guarantee coding quality, and a comprehensive Change Control Management framework to safeguard the integrity of the system.

Security is considered in every aspect throughout the software development lifecycle, following the Security by Design principles. As an example, at the application framework level, all incoming requests are required to be validated prior to processing by the system. And all feature development follows the same high level of standardised security checking.

Certifications

ISO 27001:2013

Praxonomy is ISO/IEC 27001:2013 certified. ISO/IEC 27001:2013 uses a risk-based approach for evaluation and identifies requirements and specifications for a comprehensive Information Security Management System (ISMS). To achieve and maintain this certification, Praxonomy is required to be audited annually by the British Standards Institution (BSI Group), the certification body, for its security compliance. The rigorous audit assesses Praxonomy's ability to demonstrate an ongoing and systematic approach to managing and protecting the company and client data, covering areas such as risk management procedures, threat mitigation, loss prevention, access control, physical security, security practices and business continuity planning.

ISO 9001:2005

ISO9001 is an international standard for quality management systems. The certificate demonstrates Praxonomy's ability to consistently provide products and services that meet customer and regulatory requirements, as well as ongoing efforts towards continuous improvement.

VERASAFE PRIVACY SEAL

Praxonomy's data governance and data security in relation to the processing of personal information (see our Privacy Policy) is certified by Verasafe. Praxonomy is required to maintain a high standard and implement best practices for data privacy. See the full certification criteria here. In addition, Praxonomy is fully compliant to the requirements set out in the GDPR.

Conclusion

Security is a moving target, and it should be considered from all angles. As illustrated throughout this whitepaper, security is reviewed from different aspects. The Boardlogic application is secure-by-design. Security considerations are taken into account throughout the entire Software Development Lifecycle. We deliberately chose to host the application in data centres in the E.U. for its strict data protection laws. We reference the industry security standards from highly-regarded institutes and organisations, such as National Institute of Standard and Technology (NIST) and Open Web Application Security Project (OWASP), and follow best practices to design and develop both our infrastructure and application. Encryption mechanism is enforced in applicable areas for the best protection of clients' data and assets. In terms of process management, guidelines and procedures are implemented to avoid unintentional errors. Finally, we have achieved and are committed to maintaining certifications such as ISO27001:2013 and ISO9001:2005.

The sensitive and confidential nature of the information boards possess makes them a prime target of cyber threats. A single-layer defence system is not sufficient, and yet a heavily protected system can easily result in slow performance or present complicated configurations. At Praxonomy, we have attained the optimal scenario of prioritising security without compromising application performance or usability. The end-product is a Boardlogic Board Portal that our clients can use with utmost trust and confidence.