SECURITY WHITEPAPER

Harbr_

Contents

Introduction

Harbr's ability to protect customer data is critical to our continued success - we have an existential interest in making sure that we keep our customers' data safe. Every person, team and organization expects their data to remain confidential - we take this responsibility extremely seriously, and work hard to maintain the trust of our current and future customers.

We take a defense in depth approach to information and infrastructure security, implementing a comprehensive suite of controls, tools, business processes and employee education to achieve a robust defensive security posture at every layer.

Security is a key pillar of our product and our company and we are committed to excellent execution of the basics, combined with industry leading security tooling that allows us to respond effectively to security issues throughout the product and software development lifecycle.

Our security program supports our ISO27001 certification, and all our cloud environments are continuously assessed against recognised industry standards, as follows:

Provider	Standards
AWS	AWS CIS 1.2.0 AWS Foundational Security Best Practices
GCP	GCP CIS 1.2.0

In addition, security is built into every stage of our software development lifecycle, from Threat Modelling at the design stages, through Software Composition Analysis and Static Code Testing, to Penetration Testing of the final deployed product. All identified vulnerabilities are validated for accuracy, triaged and then tracked until they are resolved.

The following sections give some detail of how we approach each area of security.

Application Security Patching

We use real-time source code scanning and software composition analysis tools to maintain visibility of all 3rd-party libraries used in our applications.

We aim to install updates containing Critical or High Priority updates within 48 hours of release by the vendor, and other updates within 30 days of release.

Application Unit Testing

We are working towards having all security-sensitive functions covered by unit testing and then ensuring that a developer cannot check in code that does not pass the unit tests. In addition, any findings from penetration tests and vulnerability assessments are used to create further unit tests, creating a model of continuous improvement.

Asset Management

Where technically feasible, we have automated the discovery of assets and their subsequent onboarding into the wider security tooling. This includes all end user devices, all resources in AWS and GCP environments and all 3rd-party libraries used in code.

Where automated asset discovery is not possible, for example, with assets we have created ourselves, we have a process in place to register these into a central asset management system, where they are linked to risks, data flows and business processes.

Business Continuity

Harbr has a business continuity plan (BCP) which is regularly reviewed and contains plans for events that would adversely affect the running of the business. The BCP includes recovery checklists and makes named individuals responsible for any required response.

Data Classification

Harbr company data is classified according to its sensitivity and potential impact of loss. Any customer data held by Harbr (i.e. not data products in the Data Services environment) is always classified at the most sensitive level.

Controls are being developed that will restrict the downloading of sensitive data only to known, well managed company devices.

Deployment

There are no hard-coded secrets in use - secrets are injected automatically from a secure location during deployment and we have tools in place to detect any secrets in code. Where possible, service principals are used instead of usernames and passwords.

Disaster Recovery

We have a well documented and regularly reviewed disaster recovery procedure that conforms to the standard set out in ISO27001.

Education and Employee Assurance

Harbr performs pre-employment background checks on all employees, and employee contracts contain confidentiality clauses.

All employees are subject to regular security awareness training, covering topics such as phishing awareness, social engineering and data protection.

Developers will soon undergo further training around secure coding practices and each developer has a plugin installed in their IDE that provides real-time feedback on code quality and security defects.

Encryption

All data is encrypted at rest and in transit. We use cloud-native key management services to create service-specific keys for data encryption in transit and at rest that are specific to each customer. Cipher suites in use are only those that are currently supported by the cloud services provider.

Endpoint Protection

All Harbr endpoints are protected with an industry leading Endpoint Detection and Response (EDR) engine that is centrally managed, and linked to access controls. Alerts from the EDR solution are managed as security incidents and triaged accordingly. Every device is subject to a baseline configuration policy and conformance with the policy is required for access to Harbr systems.

Firewall Management and Perimeter Protection

Web application firewalls are in place for all platform endpoints and are subject to a standard change control process. All changes are logged and shipped to a central Security Incident and Event Monitoring Service which provides 24/7 incident detection, backed by machine learning and threat analytics.

Identity and Access Management

Identity is at the heart of our zero-trust strategy, whether that's the identity of the user, or the device that is being used. All access to Harbr systems is MFA-protected, using robust MFA methods (i.e. OATH tokens, rather than SMS or phone calls).

Harbr adheres to the principles of least privilege and role-based access control - workers are only permitted to access data that they reasonably must handle in order to fulfil their job responsibilities. All access is reviewed regularly.

Where technically feasible, user accounts are provisioned and deprovisioned automatically and the creation of new user accounts outside the HR process is tightly controlled.

Incident Response

Harbr has a well defined security incident response process that supports the business need to minimise the impact of such events. All staff are trained to immediately report anything that may constitute a security incident. Reported incidents are assessed for impact and the appropriate response initiated. For critical and high impact incidents, on-call engineers and senior leaders are immediately engaged to manage the response.

All incidents result in a lessons-learned activity, where permanent mitigations are designed to avoid repeat events.

Infrastructure Scanning

All our cloud environments are continuously assessed against recognised industry standards, as follows:

Provider	Standards
AWS	AWS CIS 1.2.0 AWS Foundational Security Best Practices
GCP	GCP CIS 1.2.0

Any virtual machine endpoints that are spun up are automatically onboarded to Endpoint Detection and Response tooling, and continuously assessed for vulnerabilities and behavioural anomalies.

Logging

All customer platforms have their security and management logs centralised in a SIEM that is used for log correlation and incident detection and response. Access to logs is tightly controlled to minimise the risk of tampering. We use machine learning and pattern matching to confirm that no sensitive data is present in the logs.

Network Traffic Monitoring

All our platform endpoints are protected with Web Application Firewalls that detect common attack patterns such as SQL injection and cross-site scripting (although these vulnerabilities are also detected earlier by our source code security scanning tools). We also have the ability to restrict traffic for specific customers to specified IP address ranges and regions.

Penetration Testing

All our customer platforms are regularly penetration tested and each customer environment is individually tested before moving into production. Any findings from penetration testing are fed into the automated build and testing processes to ensure that defects are not repeated.

In future, we will move to a continuous penetration testing model, with a globally distributed Red Team, resulting in very high assurance of platform security.

Secure Configuration

All devices that access Harbr or customer data are required to be compliant with our secure configuration baseline, which includes device encryption, strong passwords, endpoint detection and response deployed, local firewalls, and up to date software.

Security Event Monitoring

We use a next-gen Security Incident and Event Monitoring (SIEM) tool that combines threat intelligence and behaviour analytics to surface high-fidelity incidents for investigation. All customer platforms and internal systems are connected to the SIEM and we regularly tune the alerts that we get.

Static Application Scanning

All code repositories are integrated into a modern and comprehensive code scanning solution, which surfaces code defects and security issues during the development of the software.

System Security Patching

All Harbr devices are required to install the latest security patches, without exception, and our Endpoint Detection and Response tool alerts immediately upon finding out of date operating systems or software.

Threat Modelling

As part of Harbr's defense in depth strategy, all new features undergo a rigorous process of threat modelling during the design phase, before coding begins. This process includes developers, architects, product managers and security personnel, so that a broad view of threats from a variety of perspectives can be gathered. Mitigations are then designed accordingly and fed into the requirements for the developers to build.

Vendor Management

Harbr relies on a number of vendors to operate effectively and we take appropriate measures to ensure that our security posture is maintained when engaging a new vendor, including necessary contractual commitments.