PowerHouse Hub

PowerHouse Hub

Architecture, Security and Technical Overview

V.2023-4.1

Version Information

Version	Date	Update	Author / Reviewers	Approved by
2020_AU	2020	Annual Review and update	Philip Gay, Network Admin	Tony Carrucan, CEO
2022	Feb, 2022	Annual Review and update	Philip Gay, Network Admin	Tony Carrucan, CEO
2022-1.1	Mar,2023	Additional update	Philip Gay, Network Admin	Tony Carrucan, CEO
2023-1	Jan, 2023	Annual Review and update	Philip Gay, Network Admin	Tony Carrucan, CEO
2023.4	Apr, 2023	Additional update	Philip Gay, Network Admin	Tony Carrucan, CEO

Contents

Overview

By using industry leading hardware and software, Powerhouse Hub provides a stable, high performing redundant hosted solution.

Protected by our ISO accredited hosting partner (Amazon Web Service – AWS), robust firewalls and intrusion detection systems, your portal is monitored 24 hours a day | 7 days a week.

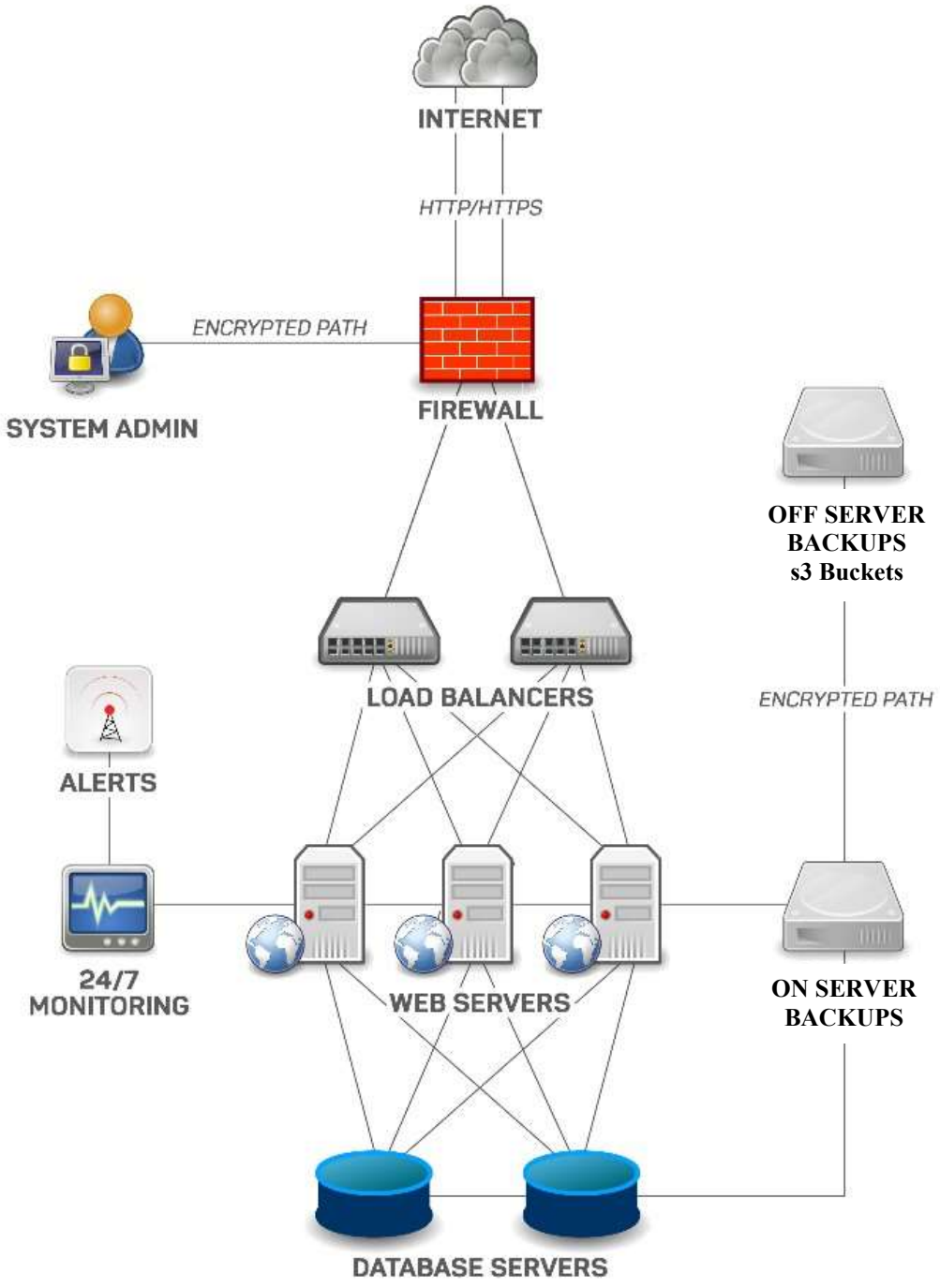
Network Topology

The network typology diagram (below) provides a high-level overview of core elements in our infrastructure. These include:

- Secure firewalls
- Encrypted paths for system administrators
- Secure https gateways to the Internet
- Load Balancers
- Multiple web servers – shared and dedicated deployments
- 24/7 monitoring
- 24/7 alerts and helpdesk triggers
- On-site cloud database back-ups
- Database encrypted paths
- Secure off-site back-ups
- Database server

Each part of the ecosystem is strategically designed for redundancy and high availability to keep your data safe and deliver fast access.

Topology Map



Server and Network Architecture

The Network Infrastructure is handled by AWS. Firewalls, Application servers, and database servers are managed by our staff.

Cloud Monitoring

1. AWS provides monitoring services and send alerts via SMS and email when the underline instance is pre-emptively going to have an issue or is currently experiencing an issue.
2. As a secondary off network monitoring service, Powerhouse Hub uses Site24x7 which monitors the state of services as well as the quality of service. Any issue that is detected an administrator is sent an SMS and Email to attend to the issue.
3. Site24x7 also monitors the performance of the application and tracks any software level issues.
4. Load Balancers are also monitoring nodes and automatically redirect traffic to exclude broken nodes

Firewalls, Load Balancers, SSL Certificates

Each service provided is setup to use an AWS firewall load balancer to manage traffic securely and efficiently through to each service.

1. Firewalls have strict policies only allowing approved traffic through ports. These ports are usually limited to port 80, and port 443.
2. Protections are in place to mitigate DDOS attacks.
3. Load balancers are used to route traffic efficiently and create redundancy in case of failovers.

All data is transferred through HTTPS and is encrypted in transit.

Application Servers

Powerhouse Hub products use multiple types of web servers. LMS requests use Apache2 in combination with PHP on top of Debian Linux. For Recruit sites, IIS and .NET is used with Windows 2019 Server.

Both types of servers utilize AWS's burstable instance type that allow large traffic spikes without any degradation of service. Pages will remain fast and responsive.

File Storage

Application files and user generated content is stored on encrypted AES256 block storage devices or s3 Buckets. Each device or instance has a minimum durability of 99.999%.

All data is backed up on an external network within the same country to ensure data protection and redundancy.

Database Storage

Powerhouse Hub utilizes two different database technologies, MySQL, and MongoDB. Each database is backed up in regular intervals. For redundancy, each backup is maintained on-network for fast recovery if required, and additionally in an off-network, but in-country s3 Bucket.

SQL Injection Prevention

Powerhouse Hub has taken the necessary caution and measures in handling user input that may be required in queries made to an SQL server. All user input is sanitized by using frequently updated, industry renowned anti-XSS packages prior to any *necessary* input being transmitted to the database. Powerhouse Hub utilizes an advanced SQL query builder that also ensures ALL input (system or user-provided) is correctly escaped.

Security Measures

All access to the Powerhouse network is encrypted by SSH2 and administrators have their own unique credentials. Each administrator is vetted and goes through thorough training and is only given the appropriate level of permissions.

Any tasks performed on production servers / data is carried out by the appropriate person. All actions that are completed are approved prior to any action and are logged.

Service Monitoring

Powerhouse Hub has an automatic monitoring system which is constantly checking all services for any performance issues.

When the system detects a potential problem, an alert is immediately sent to all on-call system administrators to notify them of the issue. When an administrator receives an alert, they investigate it immediately following the set protocols.

If an issue occurs, our central focus is data protection and maintaining the integrity of your information. Service accessibility and availability is a key deliverable in our solution with 99% availability assured through the AWS service level agreement.

Platform Hardening

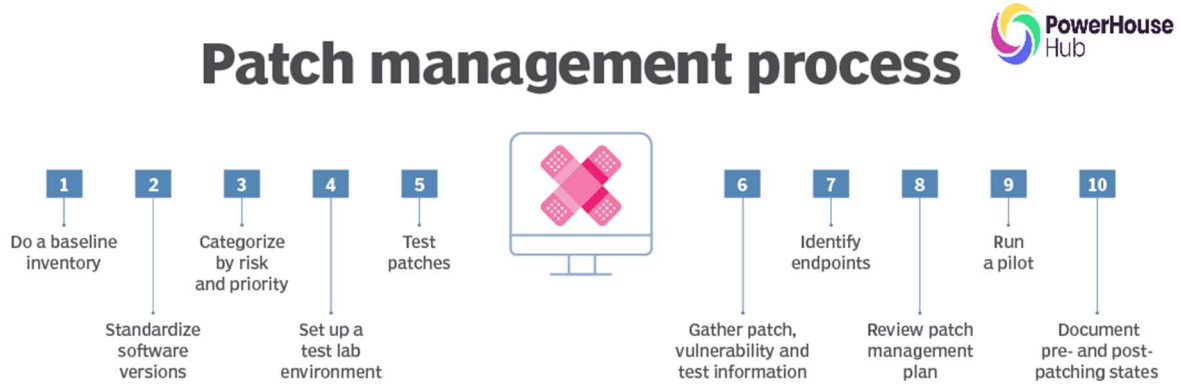
Powerhouse Hub's platform hardening policies are based on industry standards and best practices, such as the Center for Internet Security (CIS) Critical Security Controls, NIST Cybersecurity Framework, and OWASP Top Ten Project. The guidelines shall cover the following areas:

a) Operating System (OS) Hardening: The OS is configured to minimize the attack surface, including disabling unnecessary services, removing unused software, and applying security patches promptly.
b) Network Security: Security measures such as firewalls, intrusion detection and prevention systems (IDPS), and virtual private networks (VPNs) to protect the network infrastructure are implemented when necessary.
c) Access Control: Enforce the principle of least privilege by granting users and applications the minimum level of access necessary to perform their tasks. Strong authentication and authorization mechanisms, such as multi-factor authentication (MFA) and role-based access control (RBAC).

d) Application Security: Develop and deploy applications following secure coding practices and conduct regular security testing, such as vulnerability scanning and penetration testing.
e) Encryption and Key Management: Powerhouse Hub uses strong encryption algorithms to protect sensitive data at rest and in transit. And use proper key management procedures to safeguard encryption keys.
f) Logging and Monitoring: Enable comprehensive logging and monitoring to detect and respond to security incidents promptly.

All personnel involved in the management, maintenance, and operation of PowerHouse Hub's infrastructure shall receive appropriate training on platform hardening principles and techniques.

Patch Management



Our Patch Management Process applies to all software components within PowerHouse Hub's infrastructure, including operating systems, applications, libraries, frameworks, and third-party software.

Roles and Responsibilities

a) The Security Team is responsible for monitoring security bulletins, vendor notifications, and industry resources to identify new vulnerabilities and patches.
b) The Patch Management Team is responsible for evaluating, prioritizing, testing, and deploying patches, as well as maintaining the patch inventory and documentation.
c) System Administrators are responsible for applying patches to the relevant systems in accordance with the patch management process and policy.
d) Developers are responsible for applying patches to software components and ensuring compatibility with the overall system.

Patch Identification and Prioritization

The Security Team shall monitor various sources, including vendor notifications and security bulletins, to identify new patches and vulnerabilities. Patches shall be prioritized based on the severity of the vulnerability, potential impact on the organization, and the likelihood of exploitation.

Patch Testing

Before deployment, patches shall be tested in a controlled, non-production environment to assess their compatibility, functionality, and potential impact on the SaaS infrastructure. The Patch Management Team shall document the results of the testing and make necessary adjustments before proceeding with the deployment.

Patch Deployment

The Patch Management Team shall schedule and deploy patches based on their priority and the availability of resources. The deployment schedule shall be communicated to relevant stakeholders, and any downtime or service disruptions shall be minimized to the extent possible. The Patch Management Team shall coordinate with System Administrators and Developers to ensure the successful deployment of patches.

Verification and Validation

After deployment, the Patch Management Team shall verify the successful installation of patches and validate their effectiveness in addressing the identified vulnerabilities. Any issues or discrepancies shall be documented and resolved promptly.

Documentation and Reporting

The Patch Management Team shall maintain a record of all patch management activities, including patch identification, testing, deployment, and verification. Periodic reports shall be generated to track the status of patch management and share the findings with relevant stakeholders.

Cryptographic Controls

All possible measures are taken to secure data to the highest possible level.

- **Web Requests**: HTTPS is used with a minimum 2048 bit RSA key. SSL Certificates are rated A+ by Qualys.
- **File Storage**: Encrypted at rest using AES256.
- **Database**: Encrypted at rest using AES256.
- **Sensitive Information**: Encrypted using the bcrypt algorithm.

AWS Data Centre's

The Powerhouse Hub network resides within AWS's world class data center. AWS implement controls, build automated systems, and undergo third-party audits to confirm security and compliance.

Perimeter Layer

ACCESS IS SCRUTINIZED

AWS restricts physical access to people who need to be at a location for a justified business reason. Employees and vendors who have a need to be present at a data center must first apply for access and provide a valid business justification. The request is reviewed by specially designated personnel, including an area access manager. If access is granted, it is revoked once necessary work is completed.

ENTRY IS CONTROLLED AND MONITORED

Entering the Perimeter Layer is a controlled process. We staff our entry gates with security officers and employ supervisors who monitor officers and visitors via security cameras. When approved individuals are on site, they are given a badge that requires multi-factor authentication and limits access to pre-approved areas.

AWS DATA CENTER WORKERS ARE SCRUTINIZED, TOO

AWS employees who routinely need access to a data center are given permissions to relevant areas of the facility based on job function. But their access is regularly scrutinized, too. Staff lists are routinely reviewed by an area access manager to ensure each employee's authorization is still necessary. If an employee doesn't have an ongoing business need to be at a data center, they have to go through the visitor process.

MONITORING FOR UNAUTHORIZED ENTRY

We are continuously watching for unauthorized entry on our property, using video surveillance, intrusion detection, and access log monitoring systems. Entrances are secured with devices that sound alarms if a door is forced or held open.

AWS SECURITY OPERATIONS CENTERS MONITORS GLOBAL SECURITY

AWS Security Operations Centers are located around the world and are responsible for monitoring, triaging, and executing security programs for our data centers. They oversee physical access management and intrusion detection response while also providing global, 24/7 support to the on-site data center security teams. In short, they support our security with continuous monitoring activities such as tracking access activities, revoking access permissions, and being available to respond to and analyze a potential security incident.

Infrastructure Layer

LAYER-BY-LAYER ACCESS REVIEW

Like other layers, access to the Infrastructure Layer is restricted based on business need. By implementing a layer-by-layer access review, the right to enter every layer is not granted by

default. Access to any particular layer is only granted if there is a specific need to access that specific layer.

MAINTAINING EQUIPMENT IS A PART OF REGULAR OPERATIONS

AWS teams run diagnostics on machines, networks, and backup equipment to ensure they're in working order now and in an emergency. Routine maintenance checks on data center equipment and utilities are part of our regular operations.

EMERGENCY-READY BACKUP EQUIPMENT

Water, power, telecommunications, and internet connectivity are designed with redundancy, so we can maintain continuous operations in an emergency. Electrical power systems are designed to be fully redundant so that in the event of a disruption, uninterruptible power supply units can be engaged for certain functions, while generators can provide backup power for the entire facility. People and systems monitor and control the temperature and humidity to prevent overheating, further reducing possible service outages.

Data Layer

TECHNOLOGY AND PEOPLE WORK TOGETHER FOR ADDED SECURITY

There are mandatory procedures to obtain authorization to enter the Data Layer. This includes review and approval of a person's access application by authorized individuals. Meanwhile, threat and electronic intrusion detection systems monitor and automatically trigger alerts of identified threats or suspicious activity. For example, if a door is held or forced open an alarm is triggered. We deploy security cameras and retain footage in alignment with legal and compliance requirements.

PREVENTING PHYSICAL AND TECHNOLOGICAL INTRUSION

Access points to server rooms are fortified with electronic control devices that require multifactor authorization. We're also prepared to prevent technological intrusion. AWS servers can warn employees of any attempts to remove data. In the unlikely event of a breach, the server is automatically disabled.

SERVERS AND MEDIA RECEIVE EXACTING ATTENTION

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycle. We have exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

THIRD-PARTY AUDITORS VERIFY OUR PROCEDURES AND SYSTEMS

AWS is audited by external auditors on more than 2,600 requirements throughout the year. When third-party auditors inspect our data centres they do a deep dive to confirm we're following established rules needed to obtain our security certifications. Depending on the compliance program and its requirements, external auditors may interview AWS employees about how they handle and dispose of media. Auditors may also watch security camera feeds

and observe entrances and hallways throughout a data center. And they often examine equipment such as our electronic access control devices and security cameras.

As an overview we provide fully isolated cloud-based networks in a custom array that is fully redundant.

As well as our own measures, AWS provide us with the following:

- Guaranteed uptime and availability
- Fully redundant, enterprise-class routing equipment
- 9 network providers, for high-performance bandwidth
- 24/7 Technical support from fully certified network technicians
- A wide range of industry ISO's
- In-country secure hosting
- Option for dedicated hosting and hardware solutions
- Biometric and identity management access guarantees

Compliance

The following links provide more information on the AWS Compliance Programs

- https://aws.amazon.com/compliance/iso-27001-faqs/
- https://aws.amazon.com/compliance/iso-9001-faqs/
- https://aws.amazon.com/compliance/programs/

GDPR and Privacy Legislation

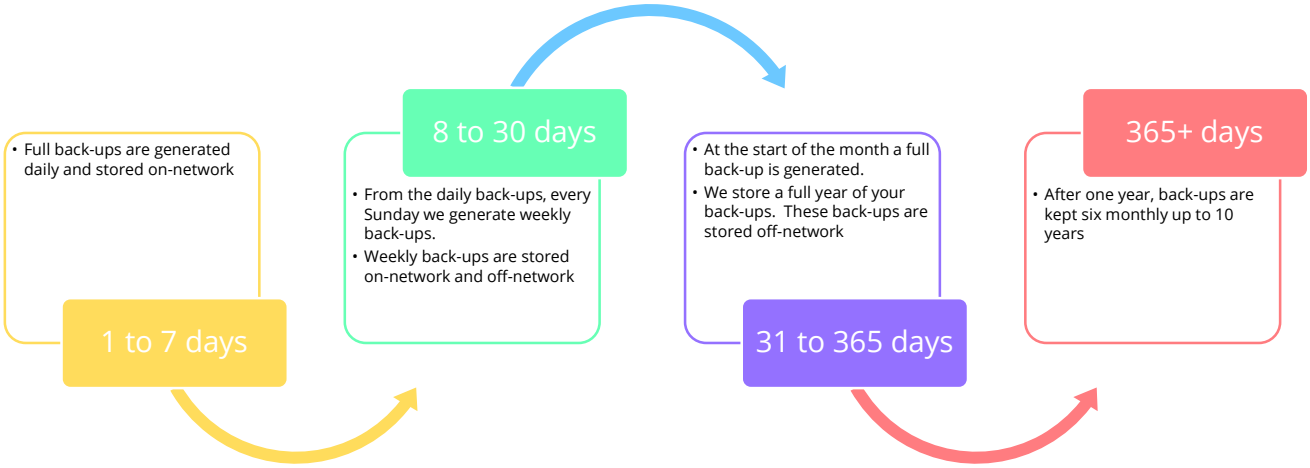
All sites are hosted in the client's chosen country and meet compliance standards such as Privacy and Data Protection, GDPR standards and guidelines. For more information, please see our GDPR documentation and privacy compliance clauses in the Customer Agreement.

Backup and Recovery

A core deliverable in our hosting services is the commitment we make to data back-ups. Rotational data back-ups are a crucial part of our solution. All back-ups are completed and hosted in the country of choosing. In Australia all customer data for production and back-up systems are located at AWS in Sydney.

Your website or portal utilizes our custom backup / recovery technology which stores a complete copy of your site and data for up to 10 years.

The data back-up workflows include the following:



Technical FAQs

What are your data backup and recovery processes?

The PowerHouse application and client data are hosted within an AWS datacentre. Each client's data stays in the country of origin for compliance privacy legislation and local compliance.

As part of the hosting and support services, Powerhouse Hub offers an extensive back-up and Disaster Recovery Program as part of the standard Service Level Agreement.

All Production workflows abide by privacy legislation with strict protocols assigned to client database access.

What functionality is included in APIs/web services?

Database Integration: API and Web Services

The agility in the technical design of the platform provides the ability for clients to access the PowerHouse API to integrate specific datasets with their existing employee or contractor database. The most common web services we offer:

- Synchronization of learner accounts
- Synchronization of training groups
- Update training records
- Integration with HRIS, Payroll or client CRM systems

The web services can deliver the calls you require to match your business requirements.

What authentication methods does your system support?

The PowerHouse platform has been developed to operate a complete hosted solution that delivers all of the required induction program functions and stores all reporting data in the system database.

The following authentication methods are available:User/password

- SSO via SAML
- LDAP integration
- 2FA

Active Directory Integration

PowerHouse is LDAPs (Lightweight Directory Access Protocol) compliant and supports integration with Active Directory to streamline learner data and access protocols.

End User Data Integration

The PowerHouse API delivers data calls and offers content import. The platform provides a wide range of ways to add or link learners to your platform. Your options include:

- Integration with the PowerHouse API to external databases (CRM, Payroll, HRIS)
- CSV import and export functionality in the administration portal
- Self-Registration forms to create automatic accounts
- Activation key module to self-register large groups accessing your training
- Single-Sign-On (SSO) functionality between existing systems

How and where is the data stored?

Your PowerHouse deployment includes your own separate and secure database. The data in your database is stored at our Tier 1 Hosting Provider – AWS.

How can data be extracted in bulk?

The platform has the inbuilt capacity to export your entire user database in CSV format. We can also customise this export, to export data in XML format. This standard export features allows your administrators to export specific groups or the entire database in bulk.

As part of our termination conditions, we provide the offer to export all database records and files if required.

What limitations does the system have regarding total users, concurrent users, number of records, size of uploads and volume of storage?

The PowerHouse platform caters for up to 200,000 users on the one database iteration. The number of users can be extended with load balancing with aligned deployments. The platform has been optimized to cater for 10 simultaneous users per second.

The platform has a prescribed limit of 128Mb file upload – usually to cater for SCORM or html5 objects. This can be varied upon request. We also assist clients by uploading large assets at database level.

What is your data retention policy with regards to records for these activities?

Powerhouse Hub data retention policies include the following tenets:

1. Our master agreement states all data collected is considered the client's intellectual property and this data retention is determined by the client and/or sector.
2. The system will automatically archive the previous year's data for all users and record new data that relates to training and annual re-induction courses
3. User data records can be bulk exported by the client at any time
4. We offer corporate annual licenses of 12 months in duration and the data retention relates to this term. At termination, the client may request a copy of all data in CSV or XML format and then instruct PowerHouse Hub to destroy all records
5. All client data is protected by privacy legislation.

Please refer to the Customer Agreement and SLA for more specific terms and conditions.