System Architecture Document

V.2025.08

PowerHouse Hub
Building 6, 2440 Logan Road
Eight Mile Plains QLD 4113
www.powerhousehub.com
+61 (0)7 3518 4020

Version Information

Version	Date	Update	Author / Reviewers	Approved by
2020_AU	2020	Annual Review and update	Philip Atkinson	Tony Carrucan
2022	Feb, 2022	Annual Review and update	Philip Atkinson	Tony Carrucan
2022-1.1	Mar,2023	Additional update	Philip Atkinson	Tony Carrucan
2023-1	Jan, 2023	Annual Review and update	Philip Atkinson	Tony Carrucan
2023.4	Apr, 2023	Additional update	Philip Atkinson	Tony Carrucan
2024.10	Oct, 2024	Annual Review and update	Philip Atkinson	Tony Carrucan
2025.09	Sep, 2025	Annual Review and update	Philip Atkinson	Tony Carrucan

Contents

Purpose

The purpose of this document is to provide a structured framework that demonstrates how the system is designed, implemented, and protected. It serves both technical and governance and is essential for ensuring system integrity, performance, and security.

Architecture

Network Infrastructure

The applications network infrastructure is hosted on Amazon Web Services (AWS), leveraging its secure and scalable cloud environment. Core components—including firewalls, application servers, and database servers—are provisioned, configured, and maintained by internal technical staff to ensure full control, accountability, and adherence to our security standards.

The infrastructure operates within AWS's world-class data centres, which implement robust security controls, automated monitoring systems, and undergo regular third-party audits. AWS maintains key certifications such as ISO 27001, SOC 1, SOC 2, SOC 3, PCI DSS, and GDPR compliance, ensuring a secure and compliant hosting environment.

The following links provide more information on the AWS Compliance Programs

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

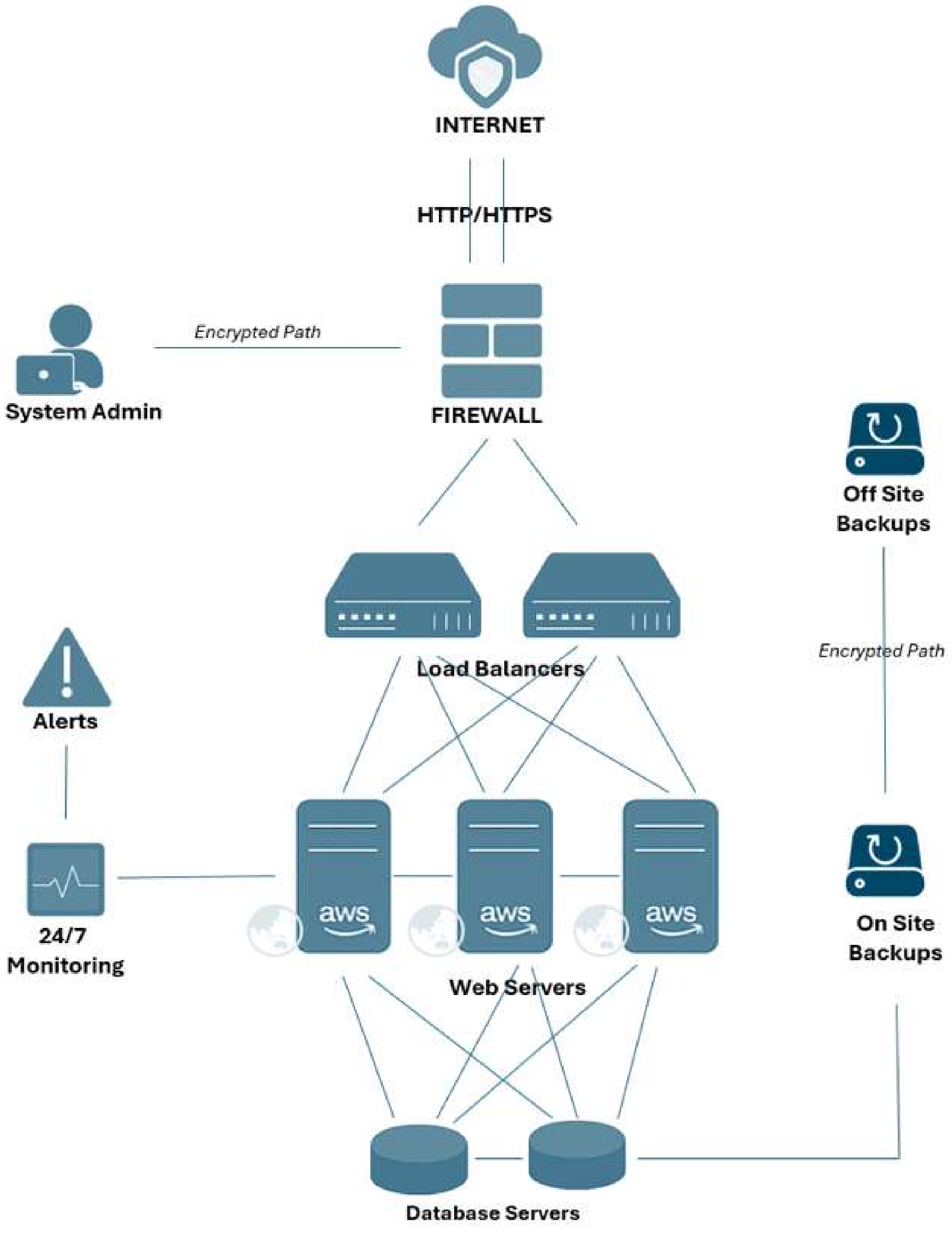
Network Topology

The following elements form the backbone of our secure infrastructure:

- Secure Firewalls
- HTTPS Gateways to the Internet
- Load Balancers
- Multiple Web Servers (Shared and Dedicated)
- 24/7 Monitoring and Alerting Systems
- On-Site and Off-Site Encrypted Backups
- High Level Encryption for all data in Transit and at Rest

Redundancy and high availability are fundamental design principles across the ecosystem to ensure uninterrupted access and data protection.

Topology Map



Firewalls, Load Balancers, and SSL

Each hosted service is protected and optimised using AWS-managed infrastructure layers:

1. Firewalls
   - Strict policies allow only approved traffic, primarily on ports 80 (HTTP), 443 (HTTPS) and 37822 (Maintenance).
   - AWS security groups and network ACLs are used to enforce access restrictions.
2. DDoS Protection
   - Cloudflare and other network monitoring tools are used to mitigate Distributed Denial of Service (DDoS) attacks and ensure service availability.
3. Load Balancing
   - AWS Load Balancers distribute incoming traffic across multiple application instances, ensuring high availability and fault tolerance.
4. HTTPS and SSL
   - All data is transmitted securely using SSL certificates, enforcing HTTPS-only connections and TLS encryption to safeguard data in transit.

Application Servers

The platform leverages a hybrid architecture to accommodate a wide variety of solutions and use cases. It operates across multiple environments, including:

- Operating Systems: Debian Linux and Windows Server
- Web Servers: Apache2 and Microsoft IIS
- Technologies: PHP and .NET frameworks

To ensure scalability and performance, the application stack is deployed on AWS burstable instance types, which dynamically allocate compute resources based on system load. This setup ensures a responsive and resilient user experience, even during high traffic periods.

File Storage

Application files and user-generated content are stored using encrypted AWS S3 Buckets. All storage solutions provide a minimum durability of 99.999%, ensuring high resilience and data integrity.

To safeguard against data loss, all data is backed up regularly to an external network located within the same country. This approach ensures geographic redundancy while maintaining compliance with local data residency requirements.

Database Storage

The application utilises two database technologies: MySQL and MongoDB. Both databases are backed up at regular intervals to ensure data availability and integrity.

For redundancy, backups are maintained in two locations:

- On-network: for fast recovery and minimal downtime in the event of data loss or corruption.
- Off-network: securely stored in an in-country AWS S3 Bucket to provide geographic redundancy while complying with local data residency requirements.

Security Measures

Administrative Access

All access to the applications infrastructure is secured using SSH2 encryption, with each system administrator assigned unique credentials to ensure traceability and accountability. Administrators are thoroughly vetted, undergo comprehensive security training, and are granted access strictly based on the principle of least privilege.

All activities involving production servers or data are performed only by authorised personnel. Actions are subject to prior approval and are logged to maintain an auditable record of administrative operations, supporting both security and compliance requirements.

Platform Hardening

The company follows a robust platform hardening policy aligned with industry standards and best practices, including the Center for Internet Security (CIS) Critical Security Controls, the NIST Cybersecurity Framework, and the OWASP Top Ten Project. These guidelines are applied across key infrastructure components to minimise vulnerabilities and strengthen system resilience.

The platform hardening approach includes the following areas:

a) **Operating System (OS) Hardening**
Operating systems are configured to reduce the attack surface by disabling unnecessary services, removing unused software, and applying security patches promptly and consistently.

b) **Network Security**
Network infrastructure is protected through layered security measures such as firewalls, Intrusion Detection and Prevention Systems (IDPS), and Virtual Private Networks (VPNs), implemented as appropriate based on risk assessments.

c) **Access Control**
Access to systems and data is governed by the principle of least privilege. Strong authentication methods, including Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC), are enforced to ensure only authorised users can perform specific tasks.

d) **Application Security**
All applications are developed using secure coding practices and are subject to regular

security assessments, including vulnerability scanning and penetration testing, to proactively identify and address potential threats.

e) **Encryption and Key Management**
Sensitive data is protected using strong encryption algorithms for both data at rest and in transit. Proper key management practices are followed to securely generate, store, rotate, and revoke encryption keys.

f) **Logging and Monitoring**
Comprehensive logging and monitoring are enabled to ensure timely detection and response to security incidents. Logs are reviewed regularly, and anomalies are investigated in accordance with the incident response plan.

Platform Authentication Methods

The application supports a range of secure authentication methods to meet the diverse needs of users and organisations. These methods include:

- **Username and Password**
  Each user account is secured with a unique username and password combination. Password policies are enforced to promote strong credential hygiene.

- **Multi-Factor Authentication (MFA)**
  MFA enhances security by requiring users to provide a second form of verification, such as a one-time code sent via email, SMS, or generated by an authenticator app.

- **Single Sign-On (SSO) via SAML 2.0**
  SAML 2.0-based SSO enables users to log in once and access multiple integrated systems without re-entering credentials. The platform supports integration with identity providers such as Google Workspace, Microsoft Entra ID (formerly Azure AD), and other SAML-compliant services.

- **LDAP and Active Directory Integration**
  Organisations can integrate Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory to manage authentication centrally, streamlining user access control within enterprise or educational environments.

These authentication options provide flexibility and enhanced security, enabling organisations to align with their internal identity and access management (IAM) policies.

Cryptographic Controls

The company implements comprehensive security measures to protect data to the highest possible standards. These measures span across all layers of the platform and include:

- **Web Requests**
  All web traffic is secured using HTTPS with a minimum 2048-bit RSA encryption. SSL/TLS certificates used by the platform are rated **A+** by Qualys SSL Labs, ensuring strong encryption and secure communication.

- **File Storage**
  All stored files are encrypted at rest using **AES-256**, a widely recognised standard for secure data storage.
- **Database Encryption**
  Databases are encrypted at rest using **AES-256**, providing robust protection for structured data stored within the platform.
- **Sensitive Information**
  Sensitive user data, such as passwords, is encrypted using the **bcrypt** hashing algorithm, ensuring secure and irreversible protection against unauthorised access.

These security controls are part of a layered defence strategy designed to ensure confidentiality, integrity, and availability of all data managed by the application.

Cloud & Service Monitoring

The company employs an automated monitoring system that continuously tracks the health and performance of all critical services. This proactive approach enables the rapid detection of potential issues, ensuring minimal disruption to platform operations.

When an anomaly or performance issue is detected, immediate alerts are dispatched to on-call system administrators. These administrators respond in accordance with established incident response protocols to investigate and resolve the issue without delay.

In the event of a disruption, the company's top priorities are data protection and maintaining the integrity of customer information. Service accessibility and availability are core commitments of our platform, with a minimum of 99% availability assured through cloud service level agreements.

Cloud Monitoring Tools

The company employs a multi-layered cloud monitoring strategy to ensure system health, performance, and service continuity:

1. **AWS Monitoring**
   AWS provides native monitoring services that track the health of underlying infrastructure. These services proactively detect potential or active issues with instances and automatically trigger alerts via SMS and email to notify system administrators.
2. **Site24x7 (Off-Network Monitoring)**
   As a secondary and independent monitoring solution, the company uses Site24x7 to monitor service availability, performance, and overall quality of service. When Site24x7 detects any issue, alerts are immediately sent via SMS and email to on-call administrators for prompt resolution.

3. **Application Performance Monitoring**
   Site24x7 also provides detailed insights into application-level performance, including the identification of software-level issues, helping to ensure responsiveness and reliability.