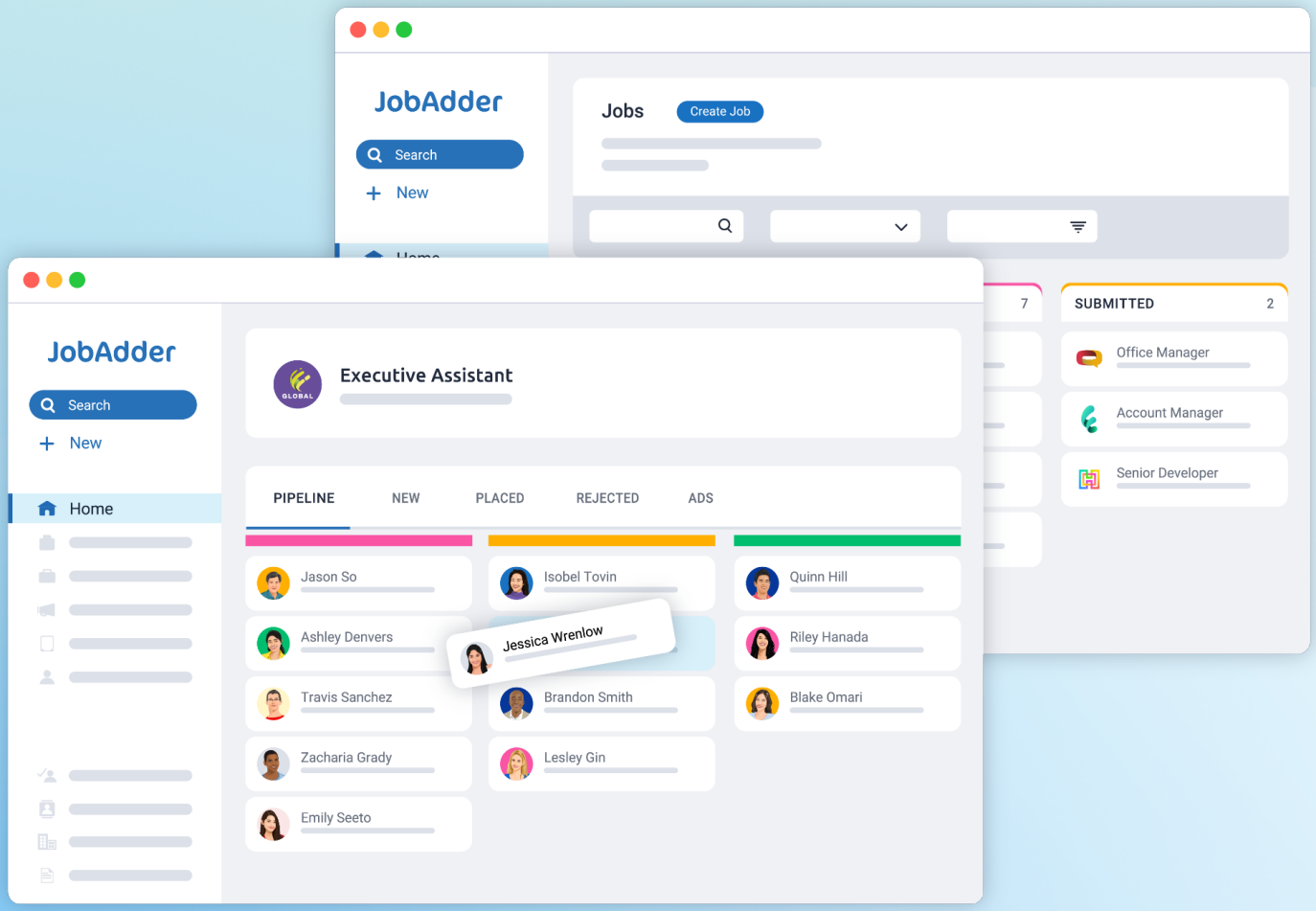
JobAdder

Security FAQs



June 2023

Commercial in Confidence

JobAdder

Company summary

Name of software vendor	JobAdder Operations Pty Ltd
ABN	39 167 597 953
Name of software product	JobAdder
Jobadder Compliance Certifications	ISO 27001:2013
Primary address	Level 1, 20 Bond Street Sydney NSW 2000
Security officer	Rhys Macfarlane (CPTO)
Contact email	Raise a ticket - https://support.jobadder.com/hc/en-us
URL of application or service	https://rms.jobadder.com
Marketing Site	https://jobadder.com
Operating Countries	Australia, New Zealand, UK, USA, Canada
Hosting Provider	Amazon Web Services - https:// www.aws.com
Privacy policy	https://jobadder.com/privacy
Terms of Use	https://jobadder.com/terms
# of Employees	~240
# of Customers	~4560

Introduction

JobAdder is a cloud-based recruitment management services system delivered to the end user via a web browser or mobile device. The purpose of this document is to provide an overview of common security questions.

FAQs

Where are JobAdder's data centres located?

JobAdder's data centres are hosted with AWS. Depending on the location of a client, production/live data will be stored in one of the following AWS regions:

- Asia Pacific (Sydney)
- US West (Oregon)
- Canada (Central)
- EU (Ireland)

This architecture ensures that live data does not migrate beyond a geographic boundary. Compute is spread across multiple availability zones in each region.

How can customers check the status of the JobAdder platform?

Customers can visit https://status.jobadder.com to quickly determine if the JobAdder platform, or any related services, are experiencing any degradation.

Does JobAdder provide tenants with separate environments for production and test processes?

There are pre-production environments available for integration and testing. These environments do not have any production data. If production data is required for testing then a separate UAT environment can be created per customer.

Does JobAdder have an API?

Yes. All available services, along with documentation, are located here: https://developers.jobadder.com/docs.

What platforms can the system be accessed from? E.g. Windows, Mac, etc.

JobAdder is a pure web application, running on any device that supports a web browser. JobAdder is built for the browser and utilises all native browser functionality out of the box, such as forward and back buttons, ctrl+click to open a record in a new tab and so on.

JobAdder is a SaaS solution and supports the latest versions of all major browsers.

How do customers authenticate?

JobAdder provides two options for authentication to the platform, JobAdder local accounts or SSO using customers' own IDP (via OIDC or SAML2).

Local accounts must have a minimum 15 character password. A word blacklist exists for common phrases. A user cannot reset their password to be one of their last five passwords. After five unsuccessful attempts, a user will be blocked from logging in for five minutes.

OTP based MFA (multi-factor authentication) is available either via individual user opt-in or can be enforced by the account administrator for all users.

SSO can be implemented using either OIDC or SAML 2.0, this provides customers the convenience of SSO and the ability to define their own password/authentication and session requirements.

How is authorisation / role-based access control implemented in the JobAdder Application?

There are two major classifications of user (Admin & Standard). There are also more granular function based roles that can be applied a) Add contact as hiring manager, b) Approve placements, c) Manage placement credit, d) Delete records, e) Delete and Edit notes, f) Merge candidates, g) Export spreadsheets, h) Edit interview evaluation, i) Grant API access to integration partners, j) Manage financial custom fields.

Does JobAdder Maintain any Security/ Compliance Certifications

Yes, JobAdder was certified to ISO 27001:2013 by Lloyd's Register Quality Assurance (LRQA) in July 2022.

Does JobAdder implement Compliance and Risk Management Programs?

Yes JobAdder is certified to ISO 27001:2013 and implements an associated risk management program.

Are External Audits Performed?

Yes, at minimum an independent audit of JobAdder's ISMS is performed by Lloyd's Register Quality Assurance (LRQA) as part of ISO 27001 certification. Penetration testing by CREST certified (NCC Group) penetration testers is also performed on a minimum annual basis and for any significant architectural change.

How does JobAdder store payment information?

JobAdder does not store any credit card information. All card subscriptions are processed using Recurly: https://recurly.com/security.

Recurly is integrated with Stripe as a payment gateway to initiate and charge transactions on behalf of JobAdder. Both Recurly and Stripe are PCI-DSS Level 1 compliant.

Does JobAdder have documentation that describes scenarios in which data may be moved from one physical location to another?

Production data does not leave JobAdder's AWS data centre except where a customer requests a data export upon terminating their JobAdder subscription. This is outlined in the JobAdder Terms of Use.

How secure are JobAdder's data centres?

JobAdder's data centre provider (AWS) is ISO 27001 & ISO 9001 compliant.
https://aws.amazon.com/compliance/iso-27001-faqs
https://aws.amazon.com/compliance/iso-9001-faqs

A current list of its compliance programs and standards can be found here:
https://aws.amazon.com/compliance/programs.

Physical access to AWS data centres is restricted to AWS employees:
https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf.

JobAdder stores documents on Amazon Simple Storage Service ("S3") and uses Amazon EventBridge, Simple Notification Service ("SNS") and Simple Queue Service ("SQS") for internal messaging. Amazon has a commitment to availability and provides an SLA of 99.9% and an SLA of 99.9% uptime for EventBridge/SNS/SQS.
https://aws.amazon.com/s3/sla/ https://aws.amazon.com/messaging/sla/

Technology controls

How does JobAdder protect data in transit?

HTTPS using TLS 1.2 or above with approved secure ciphers is required for all web applications. Certificates are 2048-bit RSA.

How does JobAdder protect data at rest?

- All data is encrypted at rest using AES256.
- Database data is stored on AES256 encrypted EC2 volumes.
- S3 buckets are AES256 encrypted using S3-managed keys.

What Network Security controls are in place?

- JobAdder uses Cloudflare for WAF (web application firewall) and DDOS mitigations.
- AWS Network Load Balancer, restricts access to only required ports/services.
- AWS Security groups are utilised for network segmentation on a least access model
- Application Server Operating systems are hardened to provide only necessary ports, protocols, services and applications as part of the baseline standard build.

What Operating System controls are in place?

Web and Application servers run on the latest version on a hardened Windows Server and Linux AMI.

- Windows Updates, hotfixes and service packs are applied promptly
- Port blocking is set at the network setting level
- Unnecessary services are disabled
- Anti-malware and Enhanced Detection Response (EDR) is deployed on all infrastructure and updates continuously
- Logs are shipped to New Relic for monitoring and alerting

What measures does JobAdder have in place with regard to Infrastructure Security?

- A synchronised time-service protocol (NTP) is in place to ensure all systems have a common time reference
- Server and system requirements are reviewed regularly to ensure current and anticipated capacity can meet customer needs
- Files uploaded by users to JobAdder like documents, images etc are validated against a whitelist of allowed file types/extensions.
- Automated encryption key rotation and secrets management is implemented

What anti-malware / threat mitigation controls are in place?

At the operating system level, anti-malware and EDR (enhanced detection and response) software is used across the environment and kept up to date on all systems.

This software analyses both files for malware as well as behaviour patterns associated with indicators of attack or suspicious activities.

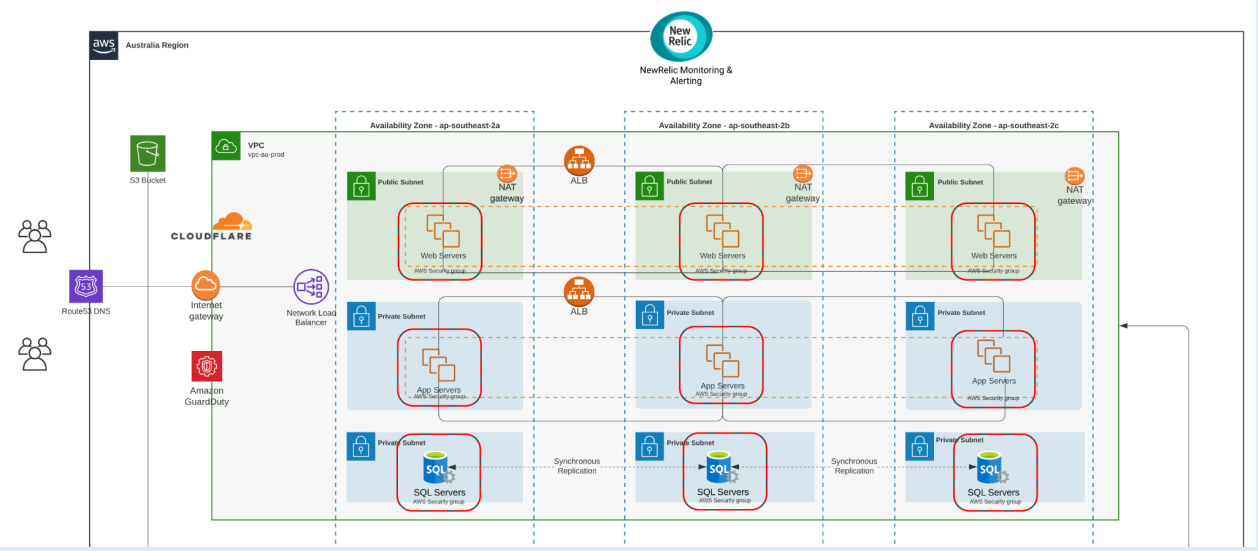
What logging / monitoring, SIEM / threat detection controls are in place?

JobAdder deploy's NextGen AV and Enhanced Detection and Responses (EDR) with a proactive threat hunting service across its infrastructure.

New Relic is used to ingest AWS infrastructure, WAF and server application logs and push alarms for unusual activity.

AWS Guard Duty is enabled for anomaly detection and alerting.

How is JobAdder's Application Architected for Resilience/ Availability?



(1) CloudFlare WAF

Cloudflare WAF provides web application firewall and DDOS mitigation services.

(2) Elastic Load Balancer

AWS Elastic Load Balancer distributes traffic across redundant servers hosted across 3 separate availability zones.

(3) Document Storage

Documents (resumes, cover letters, etc) uploaded are stored in encrypted S3 buckets which have a 99.999999999% (11 9's) of durability.

(4) Database

Database data is stored on encrypted EC2 volumes and on Amazon RDS. Data is mirrored asynchronously to a redundant server. Backups are managed and securely stored in AWS.

(5) Backups

While JobAdder's focus is on resiliency and to prevent data loss, in the case of failure, data can be restored from backup. Backups are managed and securely stored in AWS. The SQL database is backed up according to the following schedule; weekly full backup, nightly differential backup & 15min log backups.

RTO is 2 hours. RPO is 15 minutes, the maximum duration of a DB transaction log backup.

(6) Monitoring and metrics

Cloudwatch and New Relic are used to monitor and provide application and server metrics.

Process controls

How does JobAdder ensure production data is not replicated or used in non-production environments?

Personally Identifiable Information (PII) does not exist in non-production environments. Production and Non-Production environments are located in separate data centres on separate networks.

How does JobAdder detect security defects in code prior to production?

- Architecture Design Reviews (ADR) are performed prior to the development of new significant features to assess both function and security.
- JobAdder uses a Pull-Request model for software development changes requiring at least three separate people to approve code before it reaches production.
- There are both automated and manual checks for security vulnerabilities and issues are addressed prior to deployment.
- JobAdder uses automated static code analysis (SAST) and Software Composition Analysis SCA to review source code for production applications.
- Dynamic Application Security Testing (DAST) Web Application Scanning is performed across Jobadder applications checking for OWASP Top 10 vulnerabilities.
- JobAdder has controls and standards in place to ensure standards of quality are being met for software development. These include, but are not limited to: Authentication, Authorisation, Input/Output validation, Session Management, Exception Management, Logging, Encryption & Cryptography.
- When issues are reported in production, there is a procedure in place to remedy these as soon as they are identified.

What procedures & policies are in place to govern change in employment and/or termination?

There are a number of controls in place including:

- All employees are required to accept the confidentiality provisions of the JobAdder employment agreement as a condition of employment
- Onboarding and offboarding tasks for each employee are stored and logged in JobAdder's HRMS

How do JobAdder Administrators Authenticate?

JobAdder requires a minimum 15 character password and MFA is mandatory for all systems used by JobAdder infrastructure administrators.

Where are JobAdder's development and infrastructure administration teams located?

While core software development and administration is predominantly undertaken in JobAdder's Sydney office. JobAdder also engages a small team of developers in Vietnam. JobAdder has the global infrastructure and processes in place to be able to support developers anywhere. For core

software development projects, JobAdder enjoys a highly collaborative, mission-oriented development team which works closely with other functions in the business. JobAdder sees the interaction between Developers, Sales and Customer Success teams as essential. Close collaboration between development teams and business teams ensures all teams intimately understand how products are being used, and the experiences customers are having. This point of difference plays a huge part in JobAdder's 99% customer satisfaction ratings.

The Support and Sales functions have teams based in AU, the UK, USA and Canada, however, they do not have direct access to data. Support can only view a customer's account with that customer's permission. Access can be granted for 3 days, 1 week, 2 weeks or 4 weeks.

Is privileged access across Information Systems reviewed on a periodic basis?

Yes – Privileged access reviews are performed on a monthly basis.

What processes does JobAdder have in place to manage identity and access?

- Staff access to internal and 3rd party systems is managed using JobAdder's Corporate SSO Identity Management platform
- Multifactor authentication is required for employees to access production systems
- Information Management systems (e.g. application servers, firewalls, APIs) have logging and monitoring enabled
- The detail and levels of access of personnel who have access to IT infrastructure changes are managed and stored with individual accounts
- Access to logging and monitoring reporting is restricted to appropriate personnel
- Password changes are forced upon first logon to systems

We follow access management policies in line with ISO 27001 requirements and record approvals and collect artefacts for audits.