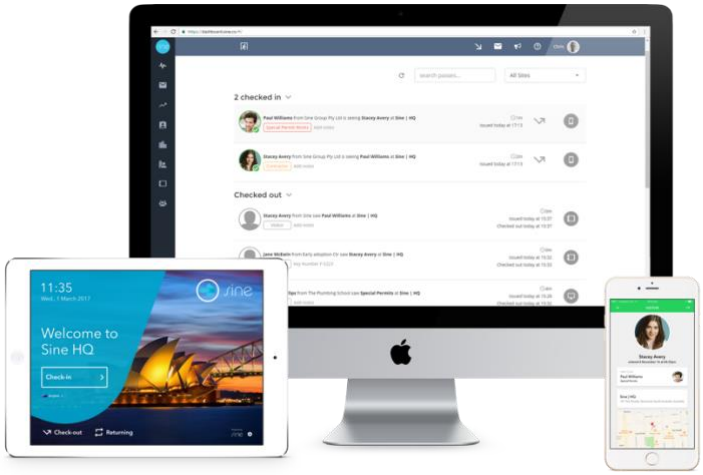
Workplace software



Privacy, hosting and security Whitepaper

Sine Group Pty Ltd

https://sine.co
support@sine.co

Company Background

Sine Group Pty Ltd (ABN 49167296219) is an Australian registered company based in Adelaide, South Australia. Sine Technologies Inc, is a US registered subsidiary based in Culver City, CA.

Sine operates in many countries globally and provides visitor and contractor management software and services. Our clients range from education, construction, industrial, office, medical and other client sectors.

Sine is trusted with global partners such as:

- Qantas, Comcast, Commonwealth government of Australia, GE, Lendlease, iag, QBE, Coles, Woolworths, Downer, Sydney Cricket Ground, Allergan, Visy, Stockland
- JLL, CBRE, Colliers – National contractor registration partner across Australia
- Private & public schools globally

Sine is backed by private investors and is well capitalised to invest in product and platform, continually improving and updating its products with aspirations to be a sustainable global visitor and contractor management technology group.

Our customers, and their sensitive data, are the central focus of our highly professional software engineering team, with customer requirements and industry best practices guiding our product roadmap. All our software engineering is conducted in Australia.

We are fully compliant with all legal and regulatory requirements in all jurisdictions in which we operate, including GDPR in the EU and CCPA in the US

Our address is:

Sine Group Pty Ltd
65 Magill Road, Stepney South Australia 5069

- Telephone +61881215956
- Email info@sine.co

Sine Technologies Inc
10000 Washington Blvd, Culver City, CA 90232

- Telephone: +19173103522
- Email info@sine.co

Privacy

Sine effectively protects all customer data and takes privacy very seriously. Our privacy policy is viewable to all parties at:. http://www.sine.co/privacy

Terms of use

Sine's terms of use are published at: http://www.sine.co/terms-of-use

EU Customers

As an organisation focused on earning our customers' trust and handling their information assets with care, Sine has developed a strong compliance culture and robust security safeguards. Sine's GDPR compliance efforts will leverage these assets. Sine has updated its terms of business, privacy policies and processes to comply with the GDPR. View our additional EU terms of service and EU privacy policy if you are from the EU or UK.

Cloud based visitor & contractor management

The benefits of cloud-based visitor management include:

- Central offsite data backup – Our reliance on global infrastructure ensures means you are not vulnerable to theft or damage of your visitor sign in information and is available from multiple devices in case of an emergency
- Visitor books display private information to other visitors when signing-in. Sine's iPad app is totally secure and never displays your visitors' details
- Costs of implementation and running are lower than on premise solutions
- Integrations with other services – safety, induction, access
- Consistency of service

Reliability

Sine uses a highly available cloud architecture and all Sine infrastructure (processing, storage and backup) is spread across three availability zones (ap-south-east-2a, b and c), consisting of 9 data centres within the AWS Sydney region. Production and non-production environments are logically separated and reside on separate AWS accounts.

iPad data storage

Sine does not store any visitor data on the iPad SinePoint Pro App. In the unlikely event of theft or loss of the iPad, no visitor data will be recoverable from the iPad. SinePoint devices can be remotely logged out using our dashboard.

Hosting

Sine is a cloud-based visitor management system, hosted with Amazon Web Services (Sydney Region, Australia). The Sine API is behind Cloudflare.

Sine uses AWS CloudFront, AWS S3, AWS EC2, AWS ECS, AWS ElastiCache (Redis) AWS RDS (PostgreSQL), and MongoDB Atlas hosted in AWS Sydney.

AWS data centers are secure by design and have a defence-in-depth approach to the protection of data within each availability zone. Logical, personnel, physical and environmental controls include load-balancing, capacity planning, physical access control, CCTV, intrusion detection, redundant power supply, fire detection and suppression, and water and temperature detection.

Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data centre operations have been accredited under:

- ISO 27001

- SOC 1/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)
- PCI

Amazon security policies https://aws.amazon.com/security

"The AWS cloud infrastructure is housed in AWS's highly secure data centers, which utilize state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. All personnel must be screened when leaving areas that contain customer data. Environmental systems in the data centers are designed to minimize the impact of disruptions to operations, and multiple geographic regions and Availability Zones allow you to remain resilient in the face of most failure modes, including natural disasters or system failures."

MongoDB Atlas is SOC 2 Type II compliant. Further information can be found here https://www.mongodb.com/cloud/trust

Data Security

Sine is a multi-tenanted SaaS platform. Customer data is segregated by Access Control Lists maintained by the Sine application. All interactions within Sine are bound to a security context which respects these ACLs. Security contexts prevent unauthorized access of data between customers.

Data is encrypted at rest using AES-256 encryption. Encryption keys are managed by AWS KMS, where keys are never transmitted outside of the AWS region in which they were created. Database connection strings are kept separate from the codebase within an encrypted S3 bucket with a strict access policy, audit logging, and mandatory 2FA. RDS security groups have strict ingress and egress rules to prevent unauthorized database connections.

We have policies that require employees to never store any production data on their laptops. Production data is never used in test environments.

Encryption

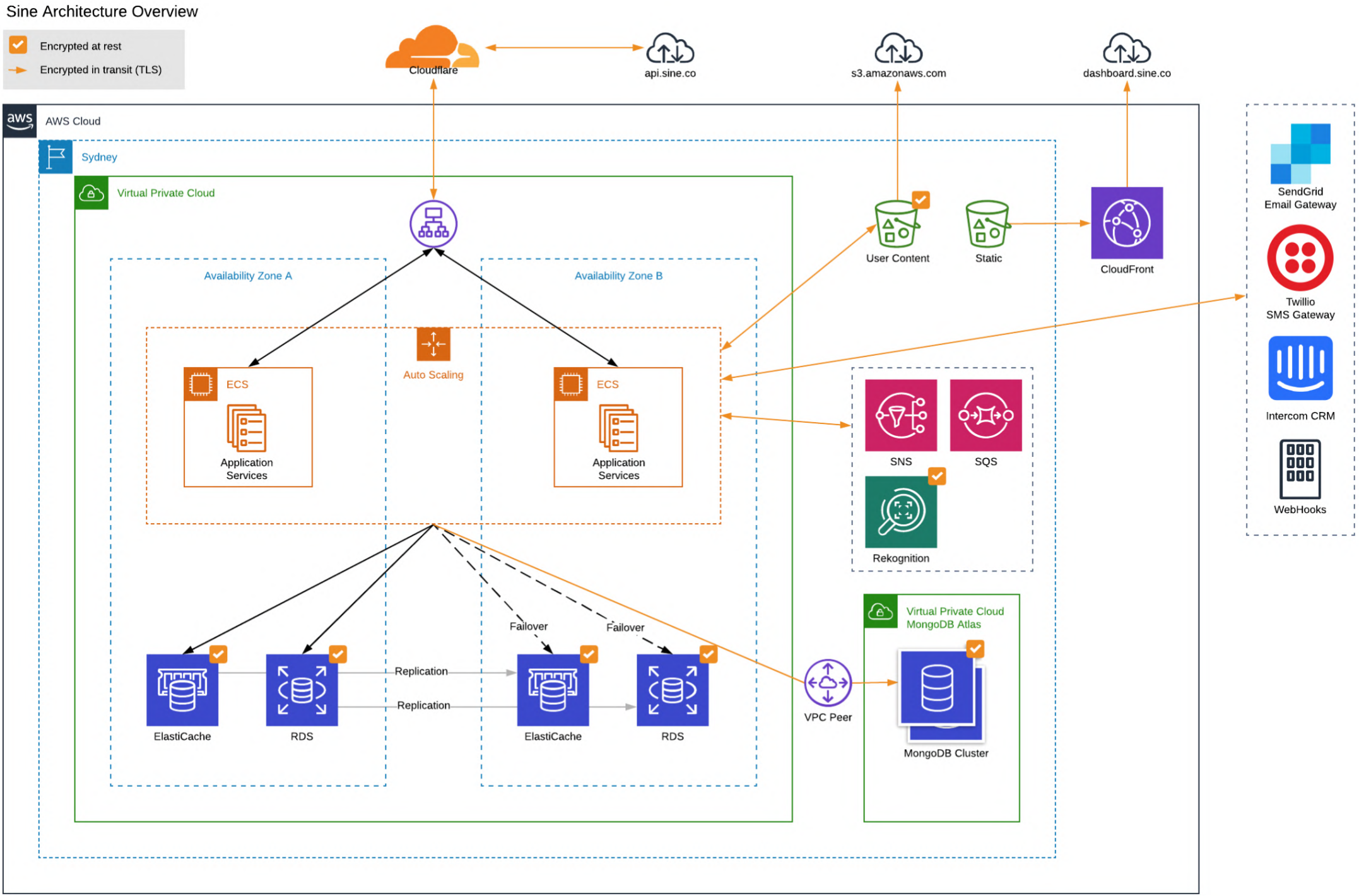
All data is encrypted at rest on AWS RDS, MongoDB Atlas, and S3 using AES-256 encryption. We host assets such as signed agreements and photos on S3 and core application data on RDS. Workflows and Connect data is hosted on MongoDB

Passwords are salted and hashed with SHA-512.

At the transport layer, all data is encrypted. TLS connections are strictly enforced, with support for TLS 1.2. All connections are made with TLS.

- TLS from client devices to Cloudflare
- TLS from Cloudflare to Sine API load balancer
- TLS from application servers via private VPC peer to MongoDB Atlas
- Webhooks can be configured to use HTTPS

TLS is terminated at the load balancer


Sine Architecture Overview
Encrypted at rest
Encrypted in transit (TLS)
Cloudflare
api.sine.co
s3.amazonaws.com
dashboard.sine.co
AWS Cloud
Sydney
Virtual Private Cloud
Availability Zone A
Availability Zone B
Auto Scaling
ECS
Application Services
ECS
Application Services
User Content
Static
CloudFront
SendGrid Email Gateway
Twillio SMS Gateway
Intercom CRM
WebHooks
SNS
SQS
Rekognition
Failover
Failover
Replication
Replication
ElastiCache
RDS
ElastiCache
RDS
VPC Peer
Virtual Private Cloud MongoDB Atlas
MongoDB Cluster

Third-party providers

Third-party, downstream providers are used for SMS and Email delivery, and Customer Relationship Management and a limited set of data is shared with these providers as part of provisioning the service.

SendGrid - Email delivery
https://sendgrid.com/policies/security/
Data centres are in undisclosed locations

Twilio - SMS delivery
https://www.twilio.com/security
Data centres in the US, Ireland, Brazil, Singapore, Tokyo and Sydney

Intercom - CRM software
https://www.intercom.com/security
Data centres in Amazon Web Services (AWS) facilities (us-east-1) in the USA

Passwords

Sine uses the Dropbox password strength estimator, zxcvbn. Passwords must be a minimum of 8 characters and contain a satisfactory level of entropy. The minimum password strength is defined as “somewhat guessable: protection from unthrottled online attacks. (guesses < 10^8).'' The Sine API is rate limited to prevent brute force attacks.

All passwords are salted and hashed with SHA-512. You can only reset a password, not retrieve it. Additionally, users are notified when their password is reset or changed. Good passwords are hard to guess. Use uncommon words or inside jokes, non-standard uppercasing, creative spelling, and non-obvious numbers and symbols.

Payments

We do not store your credit card information in any database, you directly communicate with PayPal (PCI compliant) or via invoice.

Administrator Access

Sine Administrator accounts are private, password-protected accounts only accessible by the chosen administrator. Your visitor data is securely held in the cloud and is your private data. We also utilise TLS and encrypt all data transmitted between devices and our server.

Access to Customer Data

Sine staff do not access or interact with customer data or applications as part of normal operations. There may be cases where Sine is requested to interact with customer data or applications at the request of the customer for support purposes or where required by law. Sine may also inspect customer data to debug and troubleshoot platform issues. All access to accounts with elevated permissions is granted on principle of least privilege and reviewed quarterly

Staff Access

We have a strict policy that Sine staff only access our customer's data when absolutely necessary to ensure account functionality. Employees are required to use strong passwords. Elevated access is limited to 30-minute sessions which timeout automatically.

Auditing

We log the following:

- All HTTP requests, not including request bodies. IP address, userId, deviceId, method, endpoint, response code, and time are all included
- AWS interactions, logged with CloudTrail
- Deployments and who committed what code
- Peer review records. All code in production is peer reviewed by at least two other staff members.

Help desk and support

Sine enterprise customers enjoy online, live chat and telephone support during normal business hours in your region.

Sine Support Centre details are:

info@sine.co

AU +61 8 8121 5956 | 1800 007 463

NZ +64 9 887 5531

UK +44 20 7097 8866

US +1 917 310 3522

CA +1 647 946 5609