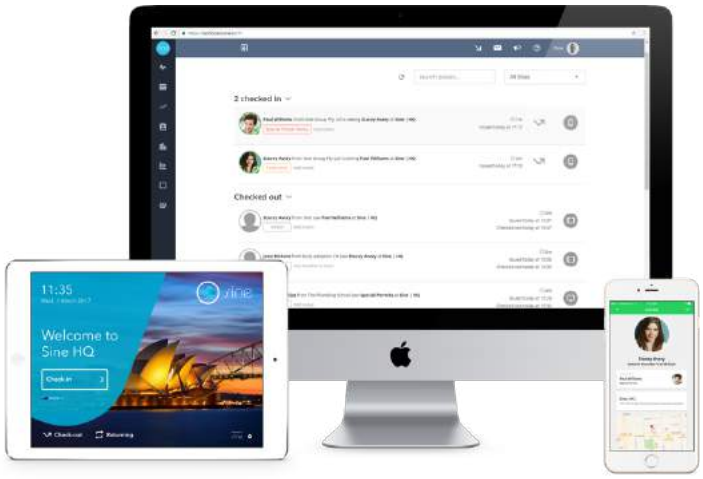
Honeywell sine

Workplace software



PRIVACY, HOSTING AND SECURITY WHITEPAPER

Sine, a Honeywell Company

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

Sine is part of Honeywell Connected Enterprise in Honeywell International, Inc. Honeywell is well capitalised to invest in product and platform, continually improving and updating its products with capability to be a sustainable global visitor and contractor management technology solution.

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

Here at Sine, we strive to understand and design solutions to address challenges our customers face today in managing their workplaces. Sine is designed to assist applying their internal policies and to assist them in addressing applicable regulations.

Our address is:

Sine Group Pty Ltd

100 Pirie Street, Level 1, Adelaide South Australia 5000

- Telephone +61881215956
- Email info@sine.co

Privacy

Sine recognizes the importance of privacy to our business and customer trust. We are committed to handling all customer data responsibly. Our privacy policy explains our approach to privacy and how individuals may exercise their rights: http://www.sine.co/privacy.

As an organisation focused on earning our customers' trust and handling their information assets with care, Sine strives to develop a strong compliance culture and robust security safeguards. Sine has updated its terms of business, privacy policies and processes with GDPR and other relevant privacy laws in mind. Our terms of use incorporate Data Processing Terms, which are published at: http://sine.co/terms-of-use/data-processing.

Terms of use

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

Cloud-based workplace software

The benefits of cloud-based workplace software solution include:

- Central offsite data backup – our reliance on global infrastructure is done with the goal of reducing your vulnerability to theft or damage of your information and is available from multiple devices in case of an emergency
- Secure, private storage – paper and pen sign-in books display private information to other visitors when checking-in. Sine's iPad app is designed to provide secured access to a private system of record for your visitors' details without exposing details to future visitors.
- Cost effective implementation - our cloud-based solution enables you to save on the costs of deploying and maintaining an on-premise solution
- Integrations with other services – safety, induction, access and others
- 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 centers 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 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 workplace management system, hosted with Amazon Web Services (Sydney Region, Australia). The Sine API sits behind Cloudflare.

Sine uses AWS CloudFront, AWS S3, Amazon 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.

AWS continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. AWS' data center operations have been accredited under numerous compliance certifications, including:

- ISO 27001SOC 1,
- SOC 2 and SOC 3
- PCI DSS Level 1
- IRAPSarbanes-Oxley (SOX)

AWS maintains a cloud security resource with further detail on the security posture and AWS practices of AWS's infrastructure and services at https://aws.amazon.com/security.

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 are designed to 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 managed by a secrets manager with 2-factor authorization and encryption enabled. Access to databases is strictly controlled by security groups limiting access to authorized personnel.

We have policies that require employees to never store any production data on their laptops. Production environments are segregated from non-production environments and access to production data is limited to authorized users.

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. All connections are made with TLS, which enforces TLS 1.2 as a minimum.

- 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

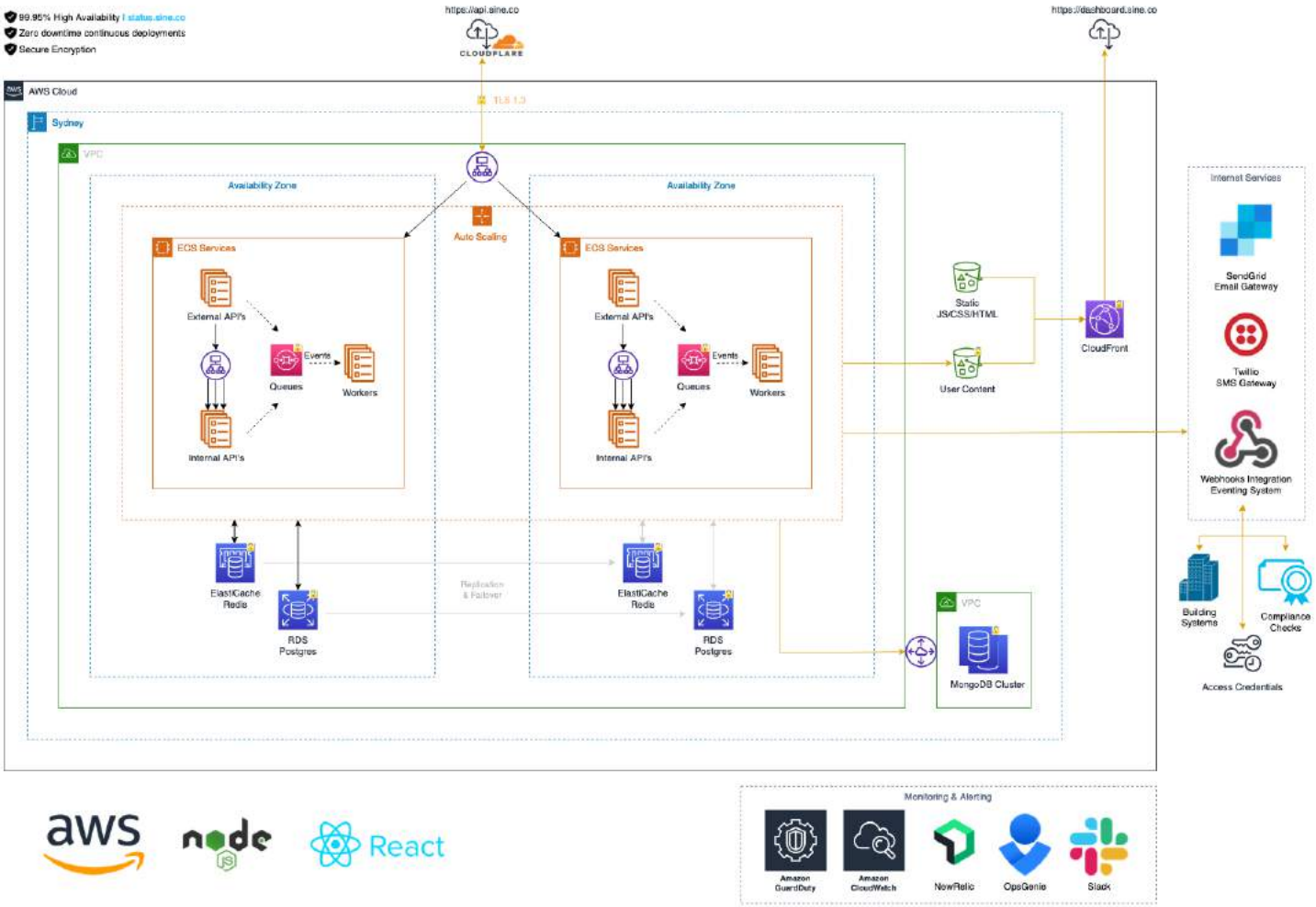
TLS is terminated at the load balancer.

Web Application Firewall (WAF)

All Sine web applications and APIs exposed to the public internet behind the Cloudflare web application firewall (WAF). This provides configurable protection against malicious patterns of requests using Cloudflare's best-in-class detection heuristics. This additional layer of protection protects against DDoS attacks, certain types of potentially malicious request payloads, and bot-like behaviour.

Bot protection

In addition to Cloudflare's algorithmic bot protection, Sine uses Google's Recaptcha service for certain critical user interactions on the web client. As well as this, sensitive API calls from native applications are protected using OS-level device attestation: Apple's DeviceCheck for iOS and Google's Play Integrity API for Android.


99.95% High Availability | status.sine.co
Zero downtime continuous deployments
Secure Encryption
https://api.sine.co
CLOUDFLARE
https://dashboard.sine.co
AWS Cloud
TLS 1.3
Sydney
VPC
Availability Zone
Availability Zone
Auto Scaling
ECS Services
ECS Services
External API's
Queues
Events
Workers
Internal API's
External API's
Queues
Events
Workers
Internal API's
ElastiCache Redis
RDS Postgres
Replication & Failover
ElastiCache Redis
RDS Postgres
Static JS/CSS/HTML
User Content
CloudFront
Internet Services
SendGrid Email Gateway
Twilio SMS Gateway
Webhooks Integration Eventing System
Building Systems
Compliance Checks
Access Credentials
VPC
MongoDB Cluster
aws
node
React
Monitoring & Alerting
Amazon GuardDuty
Amazon CloudWatch
NewRelic
OpsGenie
Slack

Third-party providers

Third-party, downstream providers are used to provide certain services on our behalf and a limited set of data is shared with these providers as part of provisioning the service. A list of third-party sub-processors for the services they provide and the countries where they are located can be found here: https://sine.co/subprocessors. Please note that this list may be updated from time to time as our services develop, so please check back regularly.

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. We recommend using 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 our PCI compliant provider or via invoice.

Administrator access

Sine Administrator accounts are managed in AWS IAM and are private, password-protected accounts only accessible by the chosen administrator. Your 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.

Auditing

We log the following:

- All HTTP requests, not including request bodies. IP address, user ID, device ID, method, endpoint, response code, and time are all included
- AWS interactions, logged with AWS CloudTrail
- AWS Guard Duty is enabled on all accounts
- Logs are centralized for monitoring

Help desk and support

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

Sine Support Center 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

Honeywell Connected Enterprise

715 Peachtree Street NE Atlanta, Georgia 30308
https://www.honeywellforge.ai/

Sine Whitepaper | October 2021