APPSPACE

Security Whitepaper

February 2022

Introduction

Appspace takes a risk-based approach to securing our platform. We take the viewpoint of assessing the Appspace platform based on the potential risks it poses based on our core Confidentiality, Integrity, and Availability principles. We know that security is essential and one of the core reasons to use Appspace for your communication and collaboration initiatives, so deploying a secure experience is a critical part of our internal standards.

Please view our Trust page here

Purpose

The purpose of this document is to provide a solid understanding of the security controls on the Appspace platform as well as our internal security programs. This document serves to inform the readers of both the technical and non-technical elements of our security programs to ensure a clear and solid understanding of how Appspace implements our Confidentiality, Integrity and Availability (CIA) principles. This document will additionally help Appspace partners to understand security during their third-party risk assessment process.

Our security culture

The Appspace internal culture is based on a pervasive desire to serve our customers. To ensure we do this consistently at a high level, we rely on an extensive set of policies, procedures, and internal standards. These range from constantly reviewing privileged access to encrypted endpoints and enforcing regular reviews of access, systems, and firewall rules.

Appspace promotes an engaging security culture for all employees. The influence of this culture manifests during the hiring process, employee onboarding, as part of ongoing training, and in company-wide events to raise awareness.

Human Resource Security

- Employment background checks are performed prior to hire; these include criminal, employment, and education. This includes OFAC (Office of Foreign Assets Control) background checks as well.
- All new employees/contractors are required to sign and agree to our security policies, acceptable use policy, and our confidentiality agreement.

- All new Appspace personnel are required to complete their security awareness training upon hire.
- New hires in our engineering teams are required to complete their OWASP training upon hire.
- All employees/contractors are required to complete our annual security awareness training as part of their terms of employment.

Production Support

Production support of the Appspace platform is predominantly based in the US with ad-hoc support available in Malaysia. This team is responsible for supporting, maintaining, and administering our production environment. These are the only Appspace employees who have access to managing our production cloud infrastructure. All access is logged and tracked, which follows our change management controls.

Change Management

Appspace uses internal tools to track all production incidents, including Problem and Change Requests. Separation of duties are adopted between the requester and implementer for production system changes. Specific processes in our change management process include rollback plans, test plans, back-up plans, and post-change reviews.

Security Management

The Appspace platform adopts TLS 1.2+ to protect data in flight with the adoption of strong cipher suites. For encryption at rest, Google Cloud enforces this control by default and Appspace does not have access to the AES-256 Data Encryption Keys. All keys and secrets are stored in a separate virtual FIPS 140-2 KMS, which is segregated from the platform and access is controlled and monitored through our IAM (Identity and Access Management) tools. In addition to these controls, we use an enterprise anti-malware and antivirus tool across all our systems and endpoints.

Security Monitoring

Monitoring the ingress of security threats is critical to our security team. To have a proactive understanding of incoming traffic and understanding whether this traffic is malicious in nature, we adopt an IDS/IPS (Intrusion Detection/Intrusion Prevention) solution. Our SIEM (Security Information and Event Management) consumes syslog events to enhance our visibility and ability to proactively react to threats by ingesting logs and performing threat correlation analytics based on known malicious signatures. This allows us to view our platform across the

board for suspicious activity. In the event a security incident arises, we would notify our partners within 72-hours upon confirming such an event.

Security Team

It is critical to have an experienced team of resources who understand security vulnerabilities, potential threats, attack surfaces, and can respond. In 2022, we have decided to invest heavily in security by significantly growing our security team. Our security teams are experienced professionals having worked at Fortune 500 companies in their past with an array of security certifications which builds confidence in their ability and skill set.

Privacy By Design

As part of our adherence to GDPR standards, we adopt a privacy-by-design approach to our product by performing data privacy impact assessments across our product features. This enables us to have a clear understanding of where sensitive information may reside or flow through as part of our processes. The security team works closely with our product team to develop these controls and processes.

During the development process of our product, the security team stays aligned with our engineering and product teams to ensure we adopt a data minimization approach by limiting areas to where personal data is required.

It should be noted the platform is not suitable to process, transmit, or store payment card information (PCI DSS) or healthcare information (HIPAA).

Partnerships: Third Party Sub-processor

Appspace partners with Google Cloud. Your data is processed by Google Cloud but Google **does not** have access to your data. We perform third-party risk assessment against our cloud provider to ensure they adhere to compliance standards. Additional information can be found here: https://cloud.google.com/security/compliance

Vulnerability and Threat Management

The Appspace security team scans for potential security threats across our platform on a regular recurring basis. These may include open-source, internally developed code, or OS-related vulnerabilities. We adopt an internal standard to remediate vulnerabilities based on our CVSS rating of the vulnerability. Once the patch is commercially available, we adhere to the following patch cadence: Critical patches are applied in 0-7 days, while High patches are applied within 30 days. Medium and Low patches are reviewed and patched based on the

threat vector of the vulnerability and applicability to our cloud infrastructure. Our penetration testing team provides expertise and insight for the security team to better understand the vectors of attack as it relates to all security threats.

Our security team performs automated and manual software security testing, as well as network vulnerability testing on an on-going basis to identify and resolve potential security vulnerabilities and bugs in our software.

Malware and Antivirus prevention

Appspace implements anti-malware and antivirus real-time alerts across its cloud infrastructure and company-owned endpoints. The enterprise anti-malware and antivirus tool scans and quarantines files in real-time across our platform. Real-time updates are also enabled to ensure we receive the latest virus definition updates from our vendor. In addition to using these tools, we have hardened the OS to further secure the platform by disabling unnecessary services from running.

Incident Response Planning

Appspace conducts red team/blue team events on an annual basis as part of its Incident Response Plan policy and procedures. The scenarios are based on threat intel data that provide us key information of threats, vulnerabilities, and consequences which are then assessed to provide a prioritized list of risk-based table-top exercises which we conduct and refresh on an annual basis.

Security Enhancements

The zero-trust architecture model implemented by Appspace across our cloud infrastructure significantly reduces our attack surface. Our security team implements tools that encrypt the hard drive of all company-owned endpoints, enabling us to remotely wipe endpoints and mobile devices (through our MDM), locks endpoints after a period of inactivity, forces strong passwords, monitors suspicious activity and traffic through our IPS/IDS tools and receives enhancement threat correlation data from Google’s Security Command Center. These tools are supported by a robust SIEM which ingests threat intel feeds and provides advanced threat correlation data across our platform. These are just a few of many tools which we use to protect the confidentiality and integrity of our customers' data.

Application Security

Application Security

As a SaaS organization, Application Security is the cornerstone of our security program and we have controls in place to ensure the confidentiality and integrity of the platform. How do we do this? Here are some of our application security controls:

- Developers and QA team members undergo OWASP Top Ten training on an annual basis.
- We perform SAST scans for code-level vulnerabilities prior to each release.
- We leverage an industry-recognized security tool to perform DAST scans.
- We scan for open-source vulnerabilities and update the version of these libraries in the event a high vector of attack is found.
- We perform third-party penetration tests across our entire platform on an annual basis.
- A number of our features and services have been enhanced over the last 12 months to require an authenticated user with the required role-based access controls to be able to access these product features, which has reduced the vector of attacks.

Like most security-orientated SaaS organizations, we do not disclose specific information regarding the type of tools our security team uses to identify DAST, SAST and MAST related vulnerabilities.

Data Integrity

We implement data input and output integrity routines on all application interfaces and databases to prevent manual or systematic processing errors, or corruption of data. Appspace has also established policies and procedures in support of data security to avoid improper disclosure, alteration, or destruction of data. These processes and internal tools address change detection and FIM alerts on critical production systems.

Audit Assurance & Compliance

Audit Planning

Our security team drives our programs through our policies, procedures, and standards. Our policies build the framework to ensure we implement security controls to adhere to the latest security threat intel data and along the way ensure we are compliant across our organization with the latest compliance standards. You can find our compliance badges on the Appspace Trust Page

Across our ISO and SOC-2 Type II controls, our auditors have independently verified there are over 150 security controls in place, which are reviewed, managed, and administered by our security team to stay fully compliant year-round. In addition, in our independent audit, we perform internal security audits across our organization.

Independent Audits

Appspace undertakes independent third-party assessments of our platform, performing regular penetration tests of our cloud service infrastructure following industry best practices. Full penetration tests are conducted at least annually, while we conduct automated penetration tests more frequently. Subject to an NDA, we are happy to provide our Penetration Test summary report.

In addition to our penetration test assessments, we have been conducting SOC-2 Type II audits since 2020, and in 2021 we became **ISO 27001**, **IS27017** and **CSA STAR Level 1** certified. In 2022, we will continue to enhance our compliance standards based on the latest cloud standards to ensure our security controls are in place on our platform; and build confidence with our customers.

Our hosting partners hold certification reports, such as SOC1, SOC2, SOC3, & FedRAMP, thus requests for copies of those reports would need to be directed at them. You can do so here: https://cloud.google.com/security/compliance/

Information System Regulatory Mapping

Within our multi-tenant cloud, all customer data is logically and cryptographically segmented at the application and database level, making it possible to effectively audit and produce data for an individual tenant without accessing another tenant's data. Single-tenant cloud customers’ data is physically segmented.

Given Appspace's global infrastructure, it's possible for customers to create accounts in a preferred region at signup, which helps with regulatory compliance in relevant jurisdictions.

Business Continuity Management & Operational Resilience

Business Continuity Planning / Disaster Recovery

In late 2020, we introduced additional processes within our Business Continuity Plan to address global workforce changes due to a pandemic outbreak. During this time, we identified processes to automate our Disaster Recovery (DR) process as much as possible in order to reduce the potential downtime in the event of a DR.

As a SaaS-based organization whose services are hosted in a geographic-redundant cloud environment, we reap immense benefits of leveraging Google Cloud zones to allow us to enable a robust failover system. Our back-up model has now changed from 4 hours to 1 hour for database and content back-ups. These back-ups are held for no less than 90 days.

Our SLAs can be found here.

Business Continuity Testing & Documentation

We test our business continuity and failover plans at scheduled intervals to ensure their continuing effectiveness. Detailed documentation of these processes is available and used by authorized Cloud Operations and Security personnel. We review and test our failover and business continuity plans at least annually.

Environmental Risks

Our hosting partners deploy certified datacenters with countermeasures implemented against natural disasters, attacks, other environmental risks, equipment power failures, network disruptions, and outages. To learn more, visit https://cloud.google.com/security.

Retention Policies

Appspace has the technical control capabilities to enforce tenant data retention policies. We perform database and content backups at a minimum every hour and retain backups for no less than three months. All backup data is encrypted.

If requested, we can purge all customer data from their Appspace account, there's a procedure in place approved by our Data Protection Officer and part of our Data Processing Addendum. Data can be made available to customers via secure file transfer before being purged from Appspace systems.

Data Security & Encryption

Your Data

Our privacy policy and Data Processing Addendum can be found here. This will provide insight into how we handle customer data and your rights.

Data Classification

Appspace does not limit or control the types of content the customer loads onto the platform. Any content loaded falls under the customer's ownership and is considered confidential information by Appspace, subject to our Acceptable Use Policy and Privacy Policy.
View our policy at https://www.appspace.com/legal.

Data Flows

Data flows between endpoint devices and the Appspace cloud over TLS encrypted communications, meaning that Appspace does not have access to a customer's network; instead, all communications are initiated from the device side.

Entitlements & Key Generation

Appspace uses security tokens generated when a session starts to grant access within the platform. The lifecycle of these security tokens is each active session. Upon session expiry and a subsequent log in, a new security token will be generated. At no time are these security tokens surfaced within the platform interface. In the event of a security incident, security tokens can be revoked as a means of containment. The session tokens expire regularly.

In addition to session tokens, we have implemented OAuth 2.0 to enable integration with third-party applications using a unique set of refresh and access tokens. Additional information regarding our integration capabilities can be found here.

Additional information regarding required MS scopes can be found here.

As it relates to entitlements; we adopt a least-privilege and role-based access control strategy for users accessing the platform. Additional information can be found here.

Data Encryption and Ciphers

Appspace uses TLS to protect information while in transit across the Internet. We have implemented TLS 1.2+ to encrypt data in transit.

Working with Google Cloud, we have implemented disk encryption leveraging AES-256 as the encryption standard. As part of this process, we do not have access to the data encryption keys (DEKs) to decrypt this data.

Please review the platform's A+ rating on SSL Labs. In addition to implementing a strong cipher policy, we have ensured our top-level domain is on the HSTS Preload List.

In July 2022, we will cease supporting TLS 1.0/1.1 on all legacy display devices.

Non-production Data

Appspace maintains separate production, staging, and development environments. All code is tested and reviewed by the Quality Assurance team before being deployed to a staging environment or production. At no time is production data (customer data) used within the development environments.

Secure Disposal

In partnership with our cloud provider, we have implemented a secure data sanitization approach that is executed in the event a customer requests this method of deletion upon the end of their contract. Further information can be found on Google Cloud's Media Sanitization page.

Controlled Access

Only senior Cloud Operations and Security personnel have access to Appspace production environments. Two-factor authentication is required through company-issued computers. No other Appspace personnel have permissions to handle customer data unless ad-hoc access is required to resolve support issues.

Logging & Tracking

All actions within the Appspace platform are logged and tracked. CRUD, session, and data transfer action logs are kept for up to one year for all Appspace personnel. As a SaaS-based platform, we review and alert on event logs.

Data Usage

Appspace philosophy

Cloud Platform customers own their data, not Appspace. The data that customers put into our systems is theirs, and we do not scan it for advertisements nor sell it to third parties. We offer our customers a detailed data processing amendment that describes our commitment to protecting customer data. It states that Appspace will not process data for any purpose other than to fulfill our contractual obligations. Furthermore, if customers delete their data, we commit to eliminating it from our systems within 180 days. Finally, we provide tools that make it easy for customers to take their data with them if they choose to stop using our services, without penalty or additional cost imposed by Appspace.

Law enforcement data requests

The customer, as the data owner, is primarily responsible for responding to law enforcement data requests; however, like other technology and communications companies, Appspace may receive direct requests from governments and courts around the world about how a person has used the company's services. We take measures to protect customers' privacy and limit excessive requests while also meeting our legal obligations.

Respect for the privacy and security of data you store with Appspace remains our priority as we comply with these legal requests. When we receive such a request, our team reviews the application to make sure it satisfies legal requirements and Appspace's policies. Generally speaking, for us to comply, the request must be made in writing, signed by an authorized official of the requesting agency, and issued under an appropriate law. If we believe an application is overly broad, we'll seek to narrow it, and we push back often and when necessary. It is Appspace's policy to notify customers about requests for their data unless expressly prohibited by law or court order.

Governance & Risk Management

Documented Procedures and Training

Appspace takes care that internal teams are aware of security and privacy guidelines and procedures. Through detailed documentation and recurring security training, we can maintain awareness of and compliance with our security standards for employees' areas of responsibility. As new employees are onboarded, they are required to read and agree to our Information Security policies and our Acceptable Use Policy in addition to our Confidentiality

Agreement. Developers and QA team members are required to complete their OWASP Top Ten training in addition to their security awareness training, as stated previously.

Policy Enforcement

All employees are made aware of the actions that will be taken in the event of a violation of our policies and procedures. Formal disciplinary and sanction policies are in place for employees who violate security protocols.

Policy Changes & Reviews

As a result of recurring risk assessments and the general evolution of technology, Appspace may need to adjust existing privacy and security policies. When making changes to any of our published policies, we take care to inform our tenants of the changes to these policies, procedures, standards, and controls through our third-party audit reports.

Identity & Access Management

Auditing & Logging

All access into an Appspace instance is logged and tracked. Every user requires their own unique login credentials, whether using local Appspace credentials or integrating with a SAML2.0-compatible IdP for SSO. Additional information regarding our SAML 2.0 capabilities can be found here. Additional information regarding configuring SSO can be found here.

Roles

Appspace employs a role-based permissions system within the platform, which means that every user can be assigned a specific role, or multiple ones, which grant access to different areas of the software, as well as allow them to perform tasks tied to each role. We perform quarterly access reviews for these roles. Additional information was provided earlier regarding the platform's role-based access controls.

Privileged Access

Appspace presents browser-based access to cloud servers. We do not surface any internal server functionalities of an Appspace account, which means that no customer has access to any data, configuration options, or source code. Only senior Cloud Operations and Security personnel have 2FA access to production environments within the Appspace hosted cloud. All admins access production systems through a password-less process (one-time password generator) in addition to 2FA controls.

Granting Access

Once an Appspace cloud account is set up, access to a customer's account is granted via email invitation, which would create a local set of credentials for each user. Alternatively, when using SSO or AD/LDAP integration, the handling of access to Appspace is done by the customer's system, which would merely grant permission for a security token to be generated once credentials are validated, initiating the login session. It's important to note that roles within Appspace must be assigned independently.

User Access Revocation

If needed, a user may be deleted from the Appspace user list by an authorized individual with access. For customers using SSO, account access is revoked through their IdP (Identity Provider).

User ID Credentials & Passwords

By supporting open standards to delegate authentication capabilities to tenants, Appspace users may deploy Single Sign-On in their Appspace cloud (SAML2.0). When implementing SSO, credentials are not stored within the Appspace database.

If local Appspace credentials are preferred, passwords are stored in a one-way salted hash within the database. When creating a password for your Appspace account, the password composition must follow ALL these rules:

- A minimum of 8 characters.
- Must be a combination of:
    - uppercase letters (A-Z)
    - lowercase letters (a-z)
    - numbers (0-9) or special characters (!@?#$%&*)
- Does not contain the current username.
- Does not contain more than 3 consecutive repeating characters.

Password Expiry, Session Logout & Account Lockout

Appspace passwords do not have expiry configurations. Sessions that become inactive are logged out automatically after a configurable amount of time. Any user that becomes locked out of their account has the option to recover/reset their password via email.

Interoperability & Portability

APIs

Appspace makes available an API list for developers to integrate customized solutions, facilitating interoperability with other applications. Additional information can be found here.

Network Protocols

Appspace uses secure, standardized network protocols for the import and export of data, and to manage its service. All communications are encrypted during transit and at rest. The Appspace cloud always uses HTTPS over TLS 1.3 and higher and AES 256-bit or higher encryption. More details on the ports that Appspace uses are found here.

Virtualization

Appspace uses an industry-recognized virtualization platform and standard virtualization formats to help ensure interoperability. We partner with Google Cloud to provide our multi-tenant cloud offering. Single tenant cloud deployments can occur with Google Cloud, Microsoft Azure or BYOL within Google Cloud.

Penetration and Vulnerability Testing

Testing report availability

We are working on determining the best way to share reports and be open about our internal testing results in a way that is secure and makes sense for our customers and us.

Customer-initiated security testing

In line with our End User Agreement, we currently do not allow customer-initiated testing for our hosted service. We are committed to being open and will endeavor to share such information when we've determined the best course for doing so.

Reliable hosting partners

Appspace partners with Google Cloud, a technology platform that is conceived, designed, and built to operate securely. Google is an innovator in hardware, software, network, and system management technologies, presenting custom-designed servers, and geographically distributed data centers. Using the principles of "defense in depth," Google has created an IT infrastructure that is more secure and easier to manage than more traditional technologies.

State-of-the-art data centers

Appspace chose Google Cloud as a hosting partner for Google's focus on security and protection of data. Google data centers' physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter.

Powering the data centers

Google's data centers feature redundant power systems and environmental controls to keep things running 24/7 and ensure uninterrupted services. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment help prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks.

Custom server hardware and software

Appspace uses Google's data centers' energy-efficient, custom, purpose-built servers, and network equipment to power the Appspace global cloud platform. Unlike much commercially available hardware, Google servers don't include unnecessary components such as video cards, chipsets, or peripheral connectors, which can introduce vulnerabilities. Server resources are dynamically allocated, allowing for flexibility in growth and the ability to adapt quickly and efficiently, and adding or re-allocating resources based on customer demand.

Hardware tracking and disposal

Google meticulously tracks the location and status of all equipment within their data centers from acquisition to installation to retirement to destruction, via barcodes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from the inventory and retired. Google hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect data at rest.

When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the disc contains no data. If the drive cannot be deleted for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy, and any variances are immediately addressed.

Questions

If you have additional questions which have not been answered in this document, we encourage you to review our CAIQ (Consensus Assessments Initiative Questionnaire) on the CSA STAR site here. In the event, your security team needs additional information regarding our security posture and controls as part of a third-party risk assessment, please ask your customer representative for a copy of our SIG Lite documentation. We also will provide a copy of the latest SOC-2 Type II report and Penetration Test report under a fully executed MNDA. Finally, if your security team performing the third-party risk assessment has additional questions; please ask your customer representative to schedule a call with our security team.

