Client Name :	Document ID : 2BP	Version 1.0
BuildPan Tech Document		18/12/2020

Security Doc | BuildPan

Contents ::

1. BuildPan CI/CD SECURITY MEASURES

At BuildPan, we take security very seriously and handle all customer data with utmost care. Our infrastructure and software architecture have multiple layers of security mechanisms in place to ensure the security and integrity of your data.

2. SECURE INFRASTRUCTURE

The underlying infrastructure for BuildPan builds is secured with SSH, TLSv1.1 or HTTPS protocols for all the networking. It means that all the data you send to BuildPan or receive from BuildPan is fully encrypted. Your builds are run on virtual machines in a private network. Our Mac infrastructure is also physically secured in data centers and the vendors are ISO27001 certified.

Each build runs in a separate environment where it boots a new virtual image. The build agents are not visible to the public network due to firewalls. Only our internal virtual private network can be used to make connections from backend services to the build machines.

3. SECURITY OF SOURCE CODE

BuildPan uses your source control system, such as GitHub, Bitbucket to get access to the CI/CD features. Once you grant access to your source code management tool, we will keep the tokens encrypted in our database. These tokens can only be used to check out the source code on virtual machines.

When your app is hosted on GitHub, Bitbucket. We use OAuth tokens or GitHub app tokens to perform various other tasks too: list branches, set webhooks, get latest commit information, update commit/PR statuses, etc. The source code checked out during the build is deleted from the virtual machine after the build and never stored on BuildPan. If you ask for our assistance with investigating a possible issue with your build, we can take a look at the build logs which are retained after the build, but only if you share your build link with us.

BuildPan protects the integrity of your source code and doesn't alter the code unless you have explicitly specified so in the build scripts. The only exceptions here are some platform-specific files that would have to be modified for successful building. For example, BuildPan modifies the project files for iOS to specify code signing settings during the build and injects a Gradle plugin to the Android component to gather build information and information about the artifacts to be generated.

4. **ENCRYPTION OF SENSITIVE DATA**

You can have BuildPan automatically deploy iOS and Android apps to App Store Connect and Google Play Store. However, in order to deploy apps, we need your login credentials, certificates with private keys, provisioning profiles, keystore files. This information is extremely sensitive and we understand the importance of keeping this data safe.

Sensitive data is kept securely in an access-limited GCloud bucket in AES-256 encrypted form at rest with no backtrace to the original owner on the bucket. Our backend has no read access to the data.

During read and write operations the data travels via TLSv1.1 and HTTPS protocols. Additionally, the data is transmitted in encrypted form and decrypted during build time in the virtual machine that the build is running. Once the job is finished the virtual machine is destroyed.

BuildPan also enables users to encrypt sensitive information in order to use them in configuration files or during build scripts as environment variables which, unless you expose them in a custom script, are available only to a specific virtual machine during the build.

5. **HOW WE STORE DATA**

Your app's builds take place in virtualized environments. At the end of each build, the virtual environment is destroyed and rebuilt when a new build is initiated using a snapshot that has no knowledge of your app's source code. All the build data, including your source code, sensitive information, build artifacts and test reports, are cleaned once the build finishes. The only build artifacts that are kept are the ones that are shown in build logs and are available for download.

We use cookies on our website and that data is shared with third parties. We have 3 main cookie categories: functional, advertisement and performance/analytics. See our privacy policy here.

During active use of BuildPan, your data will be retained. Once an account is deleted all data about the customer is deleted. Build history is kept up to 6 months, anonymous usage information is kept until it is deleted by the customer. For information about

cookies and their retention see our privacy policy.
Customers can delete their account in which case all data about the customer will be removed from our database in 14 days. You can also delete workflows, applications that you have connected and other information that you have shared and these take effect immediately. See our documentation.
For the purposes of security, our data is segmented into 2 groups - sensitive information and not sensitive information. Sensitive information is kept separate from non-sensitive data and it is encrypted.

6. **ACCESS CONTROL**
   We support account creation via email login , OAuth via GitHub, BitBucket, GitLab and also GitHub app.
   To add repositories customers can use SSH keys or basic authentication via HTTPS protocol.

7. **CHANGE MANAGEMENT**
   We keep the software versions up to date on our machines and share it via release notes. When there is a new Xcode version we will update our machines and point the latest stable version to the one Apple has announced for example.
   We may update our IP address in which case we notify the customers ahead of time.
   We use industry standard practices to test and deploy our code.
   We keep database backups and continuously monitor our service.

8. **BUSINESS CONTINUITY**
   We have redundancies in our data centers and cloud providers.
   We periodically create database backups.
   We do not have a documented recovery plan.
   Our CTO is in charge of disaster recovery and technical support is available via email, phone and in our web app.
   We create database backups every 8 hours and retain them up to 1 month.

9. **MONITORING AND INCIDENT MANAGEMENT**
   Our CTO is in charge of incident management and we provide the following service level objectives in our service level agreement for enterprise customers:
    1. response to an incident query - 6 hours;
    2. problem classification (non-critical problem, user error, service error, third-party dependency related issue) - 8 hours;
    3. provision of an interim solution - 3 days;
    4. provision of a fix to a problem related to BuildPan internal service errors. A fix can only be provided for internal service errors - 7 days.

10. After we identify an incident we will notify our customers via in-app message, twitter, public Slack announcement and possibly email depending on the severity of the incident.

11. **VULNERABILITY MANAGEMENT**
    Vulnerability Assessment (VA) and penetration test (PT) is available on request, but we do not perform them on a regular basis at the moment.

12. **LOG MANAGEMENT**
    1. We have build logs available for customers in BuildPan web app.
    2. Product usage is tracked anonymously for analytics.
    3. System logs are used internally, which have information about internal services without user data.

13. We have an audit in case user requests to remove data. We do not review it regularly, build logs are retained along with build history and are available 6 months by default.

14. **COMPLIANCE**
    We are not ISO27001 certified and have not gone through a SOC2 audit. We have completed and kept our security procedures up to date with Cloud Security Alliance CAIQ form which describes our security procedures in depth with an accepted industry standard. Please contact us at hello@buildpan.comto request the latest version.

15. **INFORMATION SECURITY RESOURCES**
    Our CTO manages information security and we have a dedicated data protection officer. We do regular risk assessments and use reasonable measures appropriate by law when hiring and train our staff on security and handling confidential information if their role requires it.
    Our Vendors are ISO27001 certified and we make all efforts to ensure that sensitive information is secure and access to it is limited and there is appropriate control.

16. **SAFE PAYMENTS**
    BuildPan doesn’t process, collect or store any data related to payments. We have no knowledge of your credit card information and are not directly involved in making the transactions. Instead, we use the Stripe payments platform for all payment actions which is integrated into BuildPan by use of designable iframes. Stripe is used and trusted by numerous companies all around the world, including Amazon, Google and Microsoft.

17. **STRONG LEGAL AGREEMENT**
    In compliance with the EU's General Data Protection Regulation, we are committed to keeping your sensitive data and private information safe. We protect your personal

information and private data by encrypting all the network traffic between you and our servers and storing your data in an encrypted format, as also stated in our privacy policy.

CONCLUSION

As a CI/CD service provider to both individuals and businesses, we consider security one of our key concerns. Now that you know more about the security measures we have in place, we hope you can rest assured that your sensitive data, intellectual property and source code are safe with us. If you have additional questions about security on BuildPan, do not hesitate to reach out to us on Slack or at hello@buildpan.com.