AppsFlyer

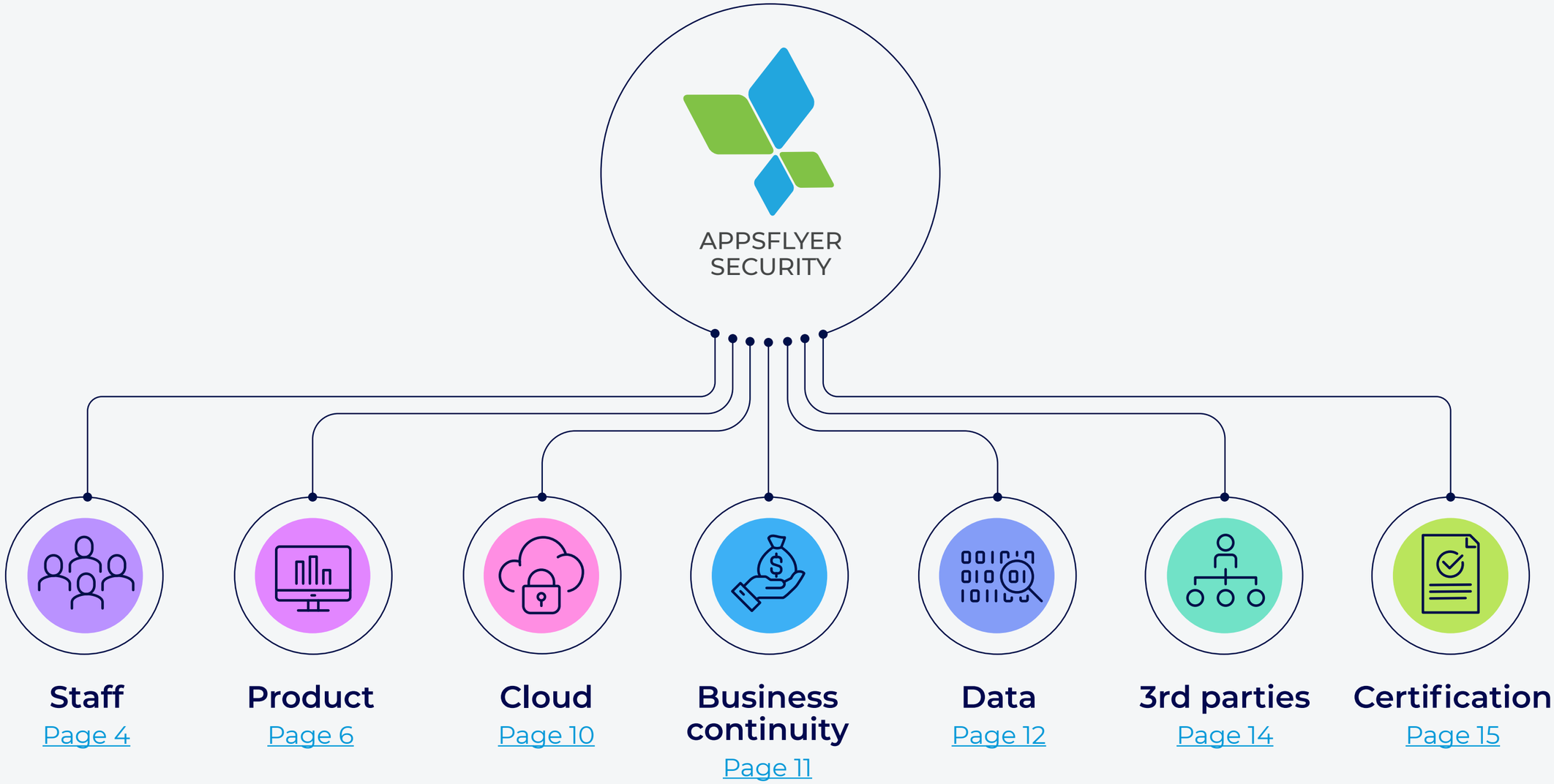
Security Policies and Practices

INTRODUCTION

At AppsFlyer, data security, scalability and performance are our lifeblood. Our state-of-the-art real-time infrastructure, advanced security and data protection, independent certifications and global regulatory compliance have earned the trust of the world's leading brands.
We strive to implement the highest level security processes and practices across all business units. To help ensure we attain this goal, our staff includes a full-time, in-house chief information security officer (CISO) and a growing dedicated security team.

Our security practices are based on industry-leading standards such as SSAE 16 SOC2, on which we are audited annually. Our security framework includes policies and procedures, asset management, access management, physical security, people security, product security, cloud and network infrastructure security, third-party security, vulnerability management, security monitoring, and incident response.

Information security policies and standards are approved by AppsFlyer management and are available to all AppsFlyer employees.


APPSFLYER
SECURITY
Staff
Page 4
Product
Page 6
Cloud
Page 10
Business continuity
Page 11
Data
Page 12
3rd parties
Page 14
Certification
Page 15

PEOPLE

The teams behind AppsFlyer products play an essential part in protecting our service on an organizational level.

SECURITY TEAM

AppsFlyer's business operation team includes top-notch security and privacy professionals who are experts in information, application and network security. The team is tasked with:

- Maintaining the company's defense systems
- Developing security review processes
- Building security infrastructure
- Implementing AppsFlyer's security policies

AppsFlyer's dedicated security team actively scans for security threats using commercial and custom tools, penetration tests, quality assurance (QA) measures, and software security reviews.

Members of the AppsFlyer information security team review security plans for all networks, systems and services. They provide project-specific consulting services to AppsFlyer's product and engineering teams. They monitor for suspicious activity on AppsFlyer's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments.

PEOPLE

HIRING

The AppsFlyer screening process is based on background checks and personal interviews with recruitment/HR managers and hiring managers. Where applicable, additional background checks are included based on local law.

INFOSEC TRAINING

New employees go through an on-boarding process that includes security guidelines, expectations, and code of conduct. All AppsFlyer employees undergo annual security awareness training.

ONGOING COMMUNICATIONS

The AppsFlyer security team communicates with all employees on a regular basis, covering topics such as emerging threats, phishing awareness campaigns, and other industry-related security topics.

PRODUCT

APPLICATION SECURITY

The AppsFlyer security development lifecycle (SDLC) standard helps ensure the delivery of a highly secure platform.
The following activities help us achieve this mission:

Change management
All changes are tracked, reviewed and approved to ensure alignment with our business objectives and compliance requirements.

Attack prevention
AppsFlyer utilizes Anti-DDoS protection, WAF and API protection tools.

SDLC
All products and features undergo thorough security reviews and code scanning.

Penetration tests
AppsFlyer conducts a variety of PTs using external vendors as well as scans using automated scanners.

Bug bounty
AppsFlyer offers a bug bounty program for detecting bugs in Application security.

PRODUCT

ACCOUNT SECURITY

AppsFlyer provides the most thorough authentication security measures in the mobile attribution industry. Among the available authentication capabilities, many settings are fully configurable to suit individual organizational standards and needs.

Full complexity passwords
All users must create full complexity passwords, which include a minimum of 8 characters, uppercase and lowercase letters, numbers and symbols.

SHA-2 + Salt password hashing
Customer passwords are not stored in clear text in AppsFlyer's servers. AppsFlyer uses SHA-2 hash standard for storing all passwords.

Failed logins
While the recommended setting is to block users after 10 failed login attempts, AppsFlyer blocks users after 5.
Customers can determine the duration of the lockout.

Temporary passwords
AppsFlyer requires new users to create a new password immediately after signing in with a temporary password.

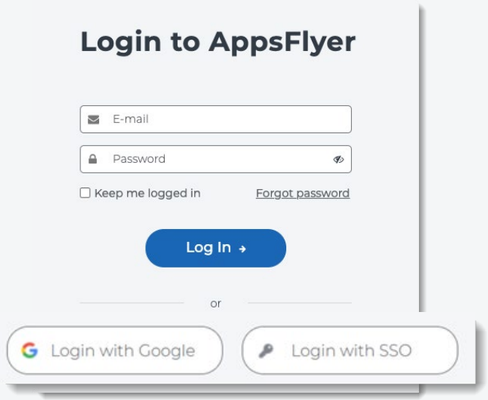
PRODUCT

ACCOUNT SECURITY

Self-serve

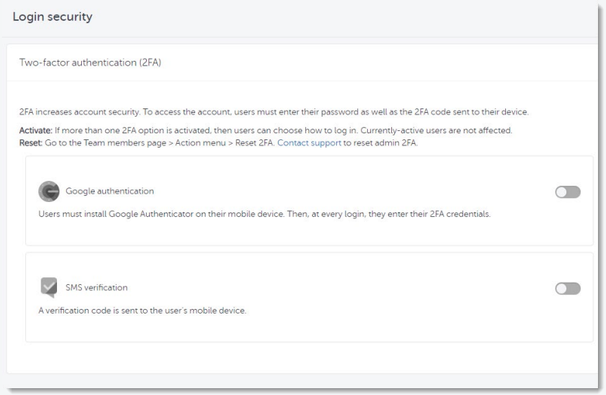
2-Factor authentication

Customers can choose to require 2FA when users log in to the dashboard. Available options are Google Authenticator or text message confirmation.



Single sign-on

Customers using an IDP solution within their organization can connect it to the AppsFlyer dashboard.
AppsFlyer works with the SAML 2.0 standard for SSO.

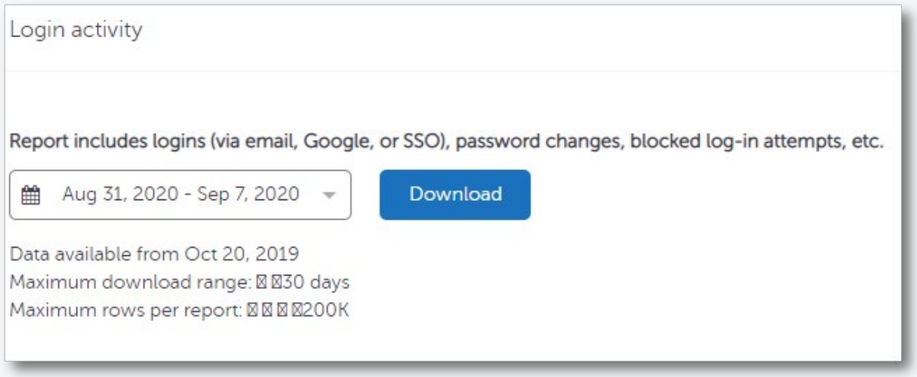


PRODUCT

MONITORING AND VISIBILITY

Our security team continuously monitors and assesses compliance, regulation and risk. Our vulnerability tests establish how we identify, respond, and triage vulnerabilities against the AppsFlyer platform. To ensure the security of our platform, AppsFlyer continues to improve and enhance its security capabilities: Continuous 24/7/365 monitoring and the implementation of a variety of security tools and other components to detect and mitigate any new vulnerabilities, incidents, and threats.

We want our customers to have complete visibility into what happens inside their account, giving them the freedom to monitor their own account activity. For this reason, we provide complete logs of all account activity, including failed login attempts and changes made to data exportation.



Audit Trail
Customers have full visibility into account activity: failed and successful logins, changes made and data exports.

24/7 Monitoring
AppsFlyer security team conducts 24/7 monitoring of the infrastructure and to application. Any alert triggers a clear process to mitigation.

CLOUD

The security of our infrastructure and networks is critical. Creating a safe platform for AppsFlyer application and customer innovation is the mission of our cloud security.

INFRASTRUCTURE COMPLIANCE

We use multi-layered controls to help protect our infrastructure, constantly monitoring and improving our applications, systems, and processes to meet the growing demands and challenges of security. In addition, we use AWS and GCP, highly-regulated and compliant data centers that meet stringent regional and international certification requirements.

ASSET MANAGEMENT & OWNERSHIP

All assets are assigned with a defined owner and accountability. Access to production infrastructure is limited to the minimal number of individuals based on a least-privilege and need-to-work basis.

DDoS PROTECTION

As part of the multilayered-protection approach, a dedicated DDoS mitigation ecosystem has been put in place. AppsFlyer utilizes Anti DDoS protection, WAF and API protection tools.

FULL REDUNDANCY

AppsFlyer utilizes a wide range of tools to monitor its environment across data centers on both the server and application level. Parameters are collected and aggregated at a central location using redundancy to detect anomalies, trends, threshold crossing, etc.

BUSINESS CONTINUITY

While we can't predict the future, we can ensure that we are fully prepared for it. That includes managing potential service interruptions and minimizing recovery time.

BUSINESS CONTINUITY PLAN (BCP)

AppsFlyer's BCP ensures that critical operations and services are continuously available to customers throughout the occurrence of any disaster or business interruption, from temporary outages to global-scale catastrophes.

DISASTER RECOVERY

AppsFlyer's services are hosted on AWS and GCP, enabling continuous global activity, even if one location fails. AWS and GCP span multiple geographic regions and provide multiple backups, allowing AppsFlyer servers to remain resilient in the event of most failure modes.

DATA BACKUPS

AppsFlyer performs regular backups of customer data and other critical data using Amazon S3 cloud storage. All backups are encrypted in transit and at rest using strong encryption.

DATA

DATA IN TRANSIT

Data is vulnerable to unauthorized access as it travels across the internet or within networks. For this reason, securing data in transit is a high priority for AppsFlyer. Our web servers support strong encryption protocols to secure connections between customer devices and AppsFlyer's web services and APIs. Any traffic transferred to AppsFlyer encrypted over https using TLS1.2 only.

DATA AT REST

Data is encrypted in our databases using AES256bit encryption by default.

DATA

MASKING

Our customers can choose to implement even stricter security measures, i.e., additional layers of protection to their account. We encourage customers to work with their account managers to make sure any specific security needs are being met, such as IP masking.

ACCOUNT SEGREGATION AND ACCESS

To keep data private and secure, AppsFlyer logically isolates each customer's account data from other customers and users, even when stored on the same physical server.

For AppsFlyer employees, access rights and levels are based on job function and role using the concepts of least-privilege and need-to-know. They are only granted a limited set of default permissions to access company resources. Additional permissions require a formal process that involves an approval from a manager as dictated by AppsFlyer's security policies. An employee's authorization settings are used to control access to all resources, including data and systems.

THIRD PARTIES

Every organization relies on other organizations – whether its an email provider, a server farm or the cafe that caters your Friday lunches. Vendor security must be addressed just like any other element in organizational security. Investing in internal security and ignoring the security vulnerability is like padlocking your front door but leaving a window open. Vulnerability is just that, a vulnerability; and third-party vendors can be a significant one.

AppsFlyer is a 3rd-party vendor for some of the world's biggest organizations. On top of that, AppsFlyer's products have third-party integrations and we employ vendors for internal services across multiple departments. We take 3rd party security as seriously as an other internal security measures:

VETTING PROCESS

Third parties used by AppsFlyer are checked before employment to validate that prospective third parties meet AppsFlyer's security standards. Customer data is not accessible to third parties or subcontractors.

ONGOING MONITORING

The AppsFlyer security team will conduct an annual review of applicable vendors. The review will conducted by AppsFlyer's security team or via a third-party report (e.g., SSAE 16 SOC2 report, ISO27001). The procedure takes into account the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal/regulatory requirements.

CERTIFICATION

AppsFlyer is committed to mitigating risk and ensuring AppsFlyer services meet regulatory and security compliance requirements. AppsFlyer complies with applicable legal, industry, and regulatory requirements as well as industry best practices.

While other attribution companies have been subject to repeated breaches, leaks and compliance failures, AppsFlyer has offered (and continues to expand) an unparalleled global compliance and certification program. AppsFlyer's compliance program is unmatched in the industry.

Compliance	AppsFlyer	Branch	Adjust	Kochava	Singular
SSAE16 SOC2	✓	✗	✗	✗	✗
TRUSTe	✓	✗	✗	✗	✗
ePrivacy	✓	✗	✓	✗	✓
ISO27001	✓	✗	✓	✗	✗
ISO27017	✓	✗	✗	✗	✗
ISO27018	✓	✗	✗	✗	✗
ISO27032	✓	✗	✗	✗	✗
ISO27701	✓	✗	✗	✗	✗
CSA STAR	✓	✓	✗	✗	✓

SSAE16 SOC2

AppsFlyer has obtained SOC2 certification, providing our customers with validation of our security controls and confidence in our security program. The Trust Service Criteria, which SOC 2 are based upon, are modeled around four broad areas: Policies, Communications, Procedures, and Monitoring. Each of the criteria have corresponding points of focus, which should be met to demonstrate adherence to the overall criteria.

TRUSTe

AppsFlyer meets all the privacy requirements established by TRUSTe and/or applicable regulatory bodies. Our continued TRUSTe certification demonstrates AppsFlyer's utmost commitment to transparency. TRUSTe reviews our website and its subdomains, software development kit {"SDK"), and API's.

ISO 27001, 27017, 27018, 27032, 27701

The ISO/IEC 27000 family of standards helps organizations keep information assets secure and manage security of assets. AppsFlyer has standard requirements for ISO 27001, 27017, 27018 and 27032 which verify that AppsFlyer has demonstrated (and even exceeded) the required measures for organizational security management, information security, PII cloud security and privacy.

CSA STAR

AppsFlyer’s commitment to data security extends to cloud services used by the company.
CSA STAR Certification is a rigorous third party independent assessment of the security of a cloud service provider. The STAR Certification is based upon achieving ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix.

ePrivacyseal

ePrivacy GmbH awards the data protection seal of approval following an in-depth audit of a company's online and mobile products. The certification covers the requirements of GDPR for digital products. Following a stringent evaluation process, AppsFlyer has been awarded the ePrivacyseal for compliance with all criteria outlined by ePrivacyseal.

SUMMARY

As a leading provider with vast experience in the industry, we realize that working in a cloud-based multi-tenant environment may raise concerns related to the confidentiality and protection of sensitive data. AppsFlyer's security mechanisms to protect physical, network and application components of the platform and our transparency with regard to security policies and processes let brands trust us with their most confidential data. This trust helps for the foundation on which our customers leverage the business benefits of our multi-tenant SaaS solution.

If you have questions or need more detailed explanations on topics covered in this whitepaper, feel free to contact our Security Team via the Support Team or your Customer Success Manager.

To learn more, visit www.appsflyer.com