AppsFlyer

APPSFLYER'S SECURITY POLICIES AND PRACTICES

February 2018

Security Organization and Program

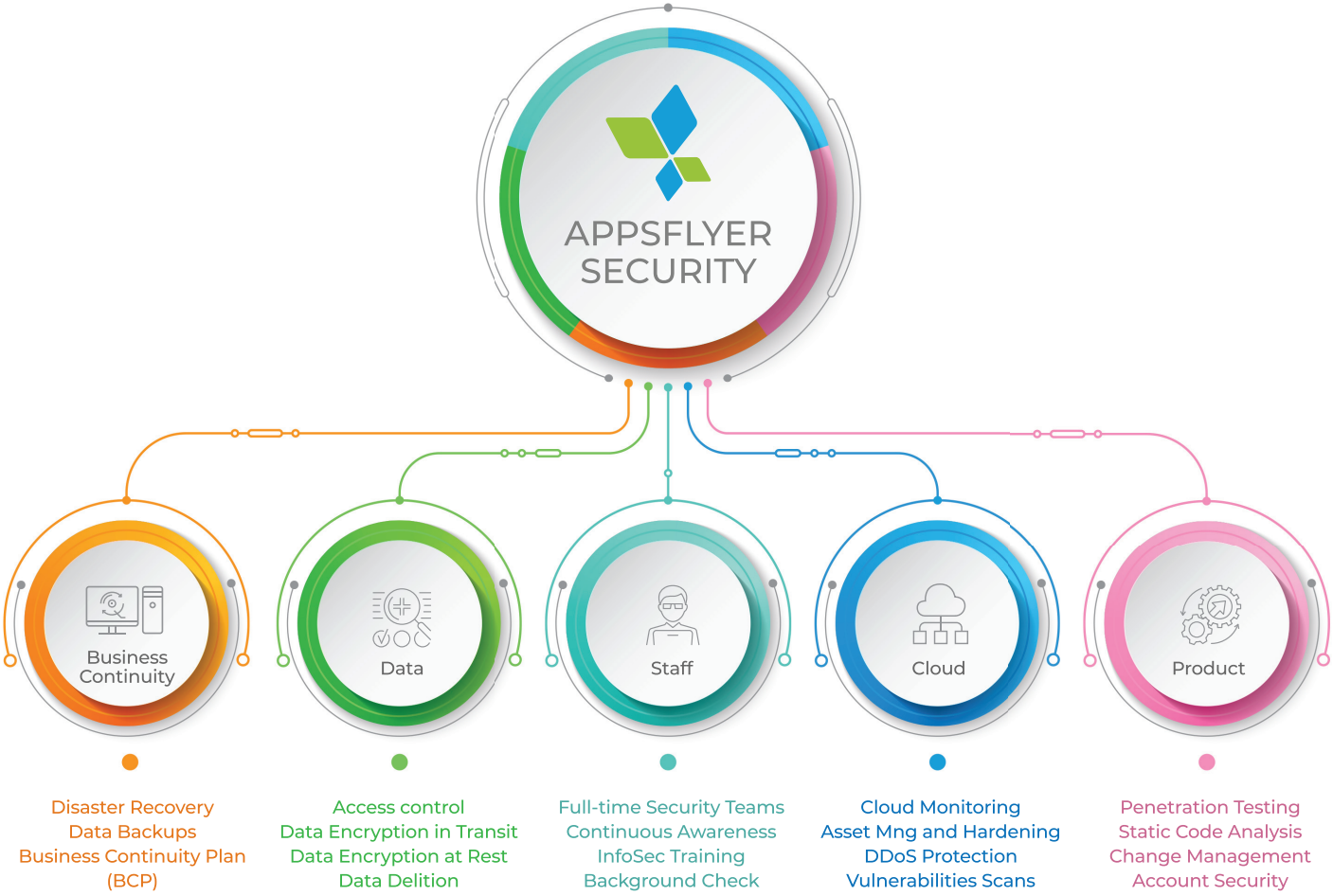
At AppsFlyer, data security, scalability and performance are our lifeblood.

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, we have hired a full-time chief information security officer (CISO) in house and have recruited a dedicated security team of professionals responsible for AppsFlyer's security.

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.



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, and 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 Security

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

Some of the controls we conduct include:

- **Background Checks**

  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 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:

- **Penetration Testing**

  AppsFlyer implements testing for security vulnerabilities on a regular basis both in-house and by independent security assessment service providers. Penetration tests are performed on an annual basis by a third party.

- **Change Management**

  AppsFlyer follows a strict change management process. Changes are tracked, reviewed and approved to ensure operational changes are aligned with AppsFlyer's business objectives and compliance requirements.

- **Encryption 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 such as TLS to secure connections between customer devices and AppsFlyer's web services and APIs.

- **Account Security**

  Beyond AppsFlyer's robust security controls, 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.

- **Accounts 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. AppsFlyer employees are only granted a limited set of default permissions to access company resources such as employee email and AppsFlyer's internal employee portal. Additional permissions require a formal process that involves a request and 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.

Support services are only provided to authorized customer administrators whose identities have been verified in several ways. This access is monitored and audited by our dedicated security, privacy, and internal audit teams.

Cloud Infrastructure

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.

- **Top-tier Infrastructure**

  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.

- **Asset Management and 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.

- **Monitoring**

  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.

- **Distributed Denial-of-Service (DDoS) Prevention**

  As part of the multilayered-protection approach, a dedicated DDoS mitigation ecosystem has been put in place.

Physical Security

The physical security of AppsFlyer facilities is an critical part of our security strategy.

Data Center Security

AppsFlyer's production environment is hosted in an AWS data center located in the EU. These facilities comply with the highest industry standards for physical, environmental, and hosting controls. Security measures at the data center include 24/7 security officers, facility access control, biometric hand readers, exterior security, interior security, annual audits, cages, alarm monitoring/intrusion protection, video imaging, CCTV, audio intercom and two way radio subsystem, ID requirements, intrusion testing, security personnel hiring/training, security policies, asset tracking, and video surveillance.

Business Continuity Plan and Disaster Recovery

Disaster Recovery

Hosting our services on AWS gives AppsFlyer the ability to be always up and running globally even if one location goes down. AWS spans multiple geographic regions and availability zones, which allows AppsFlyer servers to remain resilient in the event of most failure modes, including natural disasters or system failures.

Business Continuity Plan (BCP)

AppsFlyer has established a business continuity plan that enables the company to respond quickly and remain resilient in the event of most failure modes, including natural disasters and system failures.

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.

Third-party Security

In today's interconnected business environment, maintaining visibility into the software supply chain is critical. AppsFlyer has implemented the following procedures:

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

Once a relationship has been established, the AppsFlyer security team will conduct an annual review of applicable vendors. The annual review can be done by AppsFlyer's security team or by getting 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.

Security Compliance

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.

SSAE16 SOC2

AppsFlyer has obtained SOC2 certification, providing our customers with validation of our security controls and confidence in our security program.

EU / US Privacy Shield Framework

AppsFlyer has certified adherence to the principles of the EU-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. For more information about our EU/US Privacy Shield Framework certification click here.

GDPR May 2018

AppsFlyer is committed to the confidentiality, data privacy and security of its enterprise customers and their end-users. We are investing and will continue to invest extensive resources towards maintaining the highest levels of data protection, privacy and security standards. We are compliant with applicable laws and regulations, and are committed to compliance with the EU GDPR and related guidelines by May 2018.

TRUSTe

AppsFlyer meets all the privacy requirements established by TRUSTe and / or applicable regulatory bodies using a combination of technical and manual methodologies and company self-attestations. Our continued TRUSTe certification demonstrates AppsFlyer's utmost commitment to transparency. We work with TRUSTe to verify our data privacy policies and practices. TRUSTe reviews our website and its subdomains, software development kit (“SDK”), and API’s.

Monitoring and Vulnerability Tests

At AppsFlyer, the security and resiliency of our products and infrastructure is a top priority. 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

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. AppFlyer’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.