Filestack Statement of Security Practices

Cloud Infrastructure

Cloud Security

Filestack outsources hosting of its product infrastructure to Amazon Web Services (AWS) that guarantees between 99.95% and 100% service availability ensuring redundancy to all power, network and HVAC services. Filestack's AWS infrastructure resides in the US-EAST-1 region. AWS Data Centers are subject to various independent audits and assessments including for PCI, HIPAA, ISO 27001, ISO 27018, and SSAE-16 (SOC 1 and SOC 2). AWS compliance documentation is publicly available at the AWS Cloud Compliance Page.

Hosting in AWS allows Filestack to leverage AWS's security controls and along with the additional security controls implemented by Filestack (detailed below), provide a robust security posture to protect the confidentiality, integrity and availability of data (for more information about AWS security controls, please see Cloud Security – Amazon Web Services (AWS)).

Filestack does not host any production systems or store, process, or transmit production data in its corporate offices.

Network Security and Perimeter Protection

The Filestack infrastructure enforces multiple layers of filtering and inspection of all connections throughout the platform.

Network-level separation and stateful firewalls are implemented to prevent unauthorized network access to our internal product infrastructure. Firewalls are configured to deny network connections that are not explicitly authorized by default, and traffic monitoring is in place for detection of anomalous activity.

Changes to network security are actively monitored and controlled through the employment of a formalized change control process. Firewall rulesets are reviewed on an annual basis to help ensure that only necessary connections are authorized for access.

Encryption In-Transit and At-Rest

All sensitive interactions with the Filestack services, e.g. API calls, authenticated sessions, etc. are encrypted in transit with secure TLS version 1.2 and 2,048 bit keys. Filestack leverages several technologies to ensure stored data is encrypted at rest. Platform data is stored using AES-256 encryption. Following industry best practices, user passwords are hashed and salted, and are encrypted at rest.

Encryption keys for both in transit and at rest encryption are securely managed by the Filestack platform. TLS private keys for in transit encryption are managed through the Filestack content delivery partners Fastly and Cloudfront, both of which complete independent audits such as SOC 2 (Compliance - Signal Sciences Help Center and AWS Artifact - Amazon Web Services (AWS)). Volume and field level encryption keys for at rest encryption are managed by and stored in the AWS Key Management System (AWS KMS).

Availability & Continuity

Filestack is committed to ensuring the availability of our systems. Real-time updates and historical data on system status and security is provided by Filestack's status site at https://status.filestack.com/.

All Filestack services are built with full redundancy. Server infrastructure is strategically distributed across multiple distinct availability zones and virtual private cloud networks, and all web, application, and database components are deployed with a minimum of n+1 supporting server instances or containers with auto-scaling employed to respond to changing service demands.

Systems are backed-up daily to the local region with a rolling 7 days of data available for restoration. Additionally, the core database is replicated in real-time to a separate AWS region for recovery in the event of a primary region outage. To learn more about AWS regions and availability zones, please visit Global Infrastructure Regions & AZs

Network Monitoring and Alerting

The Filestack infrastructure is continuously monitored and when anomalies occur, configured to alert engineers, administrators, and the compliance team. In particular, error rates, abuse

scenarios, application attacks, and other anomalies are configured to trigger automatic alerts to the appropriate teams for response, investigation, and when required, remediation.

Technology Change Management & Software Development

Filestack adheres to formal policies and procedures to develop and deploy technology changes. These changes run the gamut from software enhancements to infrastructure changes.

Robust testing is employed during the various stages of development prior to deploying any changes to the Filestack Environment. At least annually, all Filestack developers are provided training to help identify and prevent common software coding vulnerabilities based-on the OWASP Top 10.

Change management includes controls that require reviews and approvals including communicating change notices to maintain awareness among personnel that manage the Filestack infrastructure and systems. Post deployment, the success of changes are confirmed and should it be necessary, procedures are in place to revert changes.

Vulnerability Management

The Filestack Security team manages a multi-layered approach to vulnerability management, using a variety of industry-recognized tools to ensure comprehensive coverage of the technology stack. A Defense in Depth approach is implemented in the environment.

Vulnerability scans are configured to scan for exploitable vulnerabilities on a daily basis. An industry-recognized third-party is employed to perform annual penetration tests. The goal of these programs is to iteratively identify vulnerabilities that present security risk and rapidly address any issues.

Filestack assets are protected against known vulnerabilities by the regular application of vendor-supplied security patches and updates. Assets that rely on the use of a base image and do not support live patching are cycled or refreshed to use the latest available base image to ensure that applicable security updates are implemented.

Identity and Access Management

User-level assignment and privileges

Unique user IDs are assigned to personnel that access Filestack systems and infrastructure. All such access is documented and approved prior to granting access. Filestack adheres to the industry standard of granting access based on the principle of least privilege. If personnel job assignments change, or their employment is terminated, access privileges are revoked in a timely manner. Periodic reviews are conducted to ensure that all access privileges granted are appropriate.

Multi-factor authentication, passwords and VPN

Access to the Filestack environment requires a VPN connection that is additionally protected by requiring multi factor authentication (MFA). Password policies exceed industry best practices for required length, complexity, and rotation frequency.

Organizational and Corporate Security

Background Checks and Onboarding

New personnel are screened as part of the hiring process. Screening activities depend on applicable local laws and may include, but are not limited to, criminal background checks, SSN Trace, address verification, and reference checks.

Confidentiality agreement.

All personnel are required to formally agree to safeguard the sensitive information they may view, process, or transmit as part of their job responsibilities.

Information security roles and responsibilities.

Information security duties are formally assigned to Filestack personnel. The Director of Compliance and Information Security works with other departments to ensure sensitive information related to the Filestack service is protected.

Policy Management

Filestack documents and maintains a number of written policies and procedures including a core Information Security Policy - the policy covers data handling requirements, privacy considerations, and responses to violations, among many other topics. Policies are reviewed and approved at least annually and stored in the company wiki. Policies that require personnel to formally acknowledge are incorporated into mandatory annual training.

Security Awareness Training

Security awareness training (SAT) that covers general security best practices is mandatory for all new Filestack personnel upon hire, and on a monthly basis thereafter. In addition to formal SAT, Filestack regularly brings to the attention of personnel applicable recent security news or initiatives.

Corporate Offices Physical Security

Filestack's offices are secured in multiple ways. US office door access is controlled using RFID tokens tied to individuals, which are automatically deprovisioned if lost or when no longer needed, e.g., employee termination, infrequent use, etc. Video surveillance, and many other protective measures are implemented across Filestack offices.

Workstation security

Filestack leverages best security practices and employs a Next Generation Anti-Virus platform to protect its workstations. This provides extensive visibility into anomalous system behavior as well as real-time alerting so that the appropriate action can be taken through either automated event triggers or manual containment of systems.

Incident Management

Filestack maintains a formal incident response plan that details, among other things, established roles and responsibilities, communication protocols, and response procedures. The plan is reviewed and updated periodically to adapt it to evolving threats and risks to the Filestack environment.

Representatives from key departments are employed to address security-related incidents. These personnel coordinate the investigation and resolution of incidents, as well as communication with external contacts as needed.

Upon confirmation of an unauthorized disclosure of customer confidential information, Filestack will notify affected customers within 72 hours (unless otherwise defined).

Vendor Management.

Filestack performs risk-based evaluations of the security controls for vendors. Due diligence includes performing the said review before engaging the services of a vendor. All vendor security measures are reviewed on a periodic basis thereafter, but at a minimum, at least annually.