A-LIGN

A-LIGN.com

Type 2 SOC 3

Prepared for:
Fluid Attacks

Year:
2026

fluid attacks

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

July 1, 2025 to June 30, 2026

Table of Contents

SECTION 1 ASSERTION OF FLUID ATTACKS MANAGEMENT 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 3

SECTION 3 FLUID ATTACKS' DESCRIPTION OF ITS FLUID ATTACKS APPLICATION SECURITY SOLUTIONS SYSTEM THROUGHOUT THE PERIOD JULY 1, 2025 TO JUNE 30, 2026 6

OVERVIEW OF OPERATIONS 7
Company Background 7
Description of Services Provided 7
Principal Service Commitments and System Requirements 7
Components of the System 8
Boundaries of the System 13
Changes to the System in the Last 12 Months 14
Incidents in the Last 12 Months 14
Criteria Not Applicable to the System 14
Subservice Organizations 14
COMPLEMENTARY USER ENTITY CONTROLS 15

SECTION 1

ASSERTION OF FLUID ATTACKS MANAGEMENT

ASSERTION OF FLUID ATTACKS MANAGEMENT

September 8, 2026

We are responsible for designing, implementing, operating, and maintaining effective controls within Fluid Attacks' (or 'the Company') Fluid Attacks Application Security Solutions System throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Fluid Attacks' service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Fluid Attacks' Description of Its Fluid Attacks Application Security Solutions System throughout the period July 1, 2025 to June 30, 2026" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Fluid Attacks' service commitments and system requirements were achieved based on the trust services criteria. Fluid Attacks' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Fluid Attacks' Description of Its Fluid Attacks Application Security Solutions System throughout the period July 1, 2025 to June 30, 2026".

Fluid Attacks uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Fluid Attacks, to achieve Fluid Attacks' service commitments and system requirements based on the applicable trust services criteria. The description presents Fluid Attacks' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Fluid Attacks' controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Fluid Attacks' service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Fluid Attacks' controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2025 to June 30, 2026 to provide reasonable assurance that Fluid Attacks' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Fluid Attacks' controls operated effectively throughout that period.

Aura Ximena Pabon O.

Aura Pabon
Administrative Director
Fluid Attacks

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Fluid Attacks:

Scope

We have examined Fluid Attacks' (or 'the Company') accompanying assertion titled "Assertion of Fluid Attacks Management" (assertion) that the controls within Fluid Attacks' Fluid Attacks Application Security Solutions System were effective throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Fluid Attacks' service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Fluid Attacks uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Fluid Attacks, to achieve Fluid Attacks' service commitments and system requirements based on the applicable trust services criteria. The description presents Fluid Attacks' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Fluid Attacks' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Fluid Attacks, to achieve Fluid Attacks' service commitments and system requirements based on the applicable trust services criteria. The description presents Fluid Attacks' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Fluid Attacks' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Fluid Attacks is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Fluid Attacks' service commitments and system requirements were achieved. Fluid Attacks has also provided the accompanying assertion (Fluid Attacks assertion) about the effectiveness of controls within the system. When preparing its assertion, Fluid Attacks is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Fluid Attacks' Fluid Attacks Application Security Solutions System were suitably designed and operating effectively throughout the period July 1, 2025 to June 30, 2026, to provide reasonable assurance that Fluid Attacks' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Fluid Attacks' controls operated effectively throughout that period.

The SOC logo for Service Organizations on Fluid Attacks' website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

A-LIGN ASSURANCE

Tampa, Florida
September 8, 2026

SECTION 3

FLUID ATTACKS' DESCRIPTION OF ITS FLUID ATTACKS APPLICATION SECURITY SOLUTIONS SYSTEM THROUGHOUT THE PERIOD JULY 1, 2025 TO JUNE 30, 2026

OVERVIEW OF OPERATIONS

Company Background

Fluid Attacks is a private company established in April 2001 that provides application security solutions. Fluid Attacks is a commercial company based in Garner, North Carolina has an office in Colombia under the name Fluid Attacks SAS.

Description of Services Provided

Fluid Attacks' Application Security Solutions is an application that combines security testing tools, artificial intelligence (AI), and a hacking team to accurately find and help remediate security vulnerabilities throughout the software development lifecycle (SDLC) and ensure secure deployments.

Fluid Attacks reports risk exposure promptly to its clients and supports them to achieve high remediation rates and guarantee high-quality and safe products to their end users.

Fluid Attacks' security testing involves different automated and manual techniques, namely, static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA), cloud security posture management (CSPM), secure code review, manual penetration testing, and reverse engineering. Further, Fluid Attacks uses its own AI tool to sort files in a code repository by their probability of containing security vulnerabilities, thus informing Fluid Attacks' hacking team of which files to prioritize in their manual tests to start finding vulnerabilities faster.

Fluid Attacks helps its clients develop secure software and have secure deployments into production. To ensure secure development, Fluid Attacks performs tests during the entire SDLC. It reports all findings both by its tool and hacking team to its clients on Fluid Attacks' platform. There, its clients can learn about the specific lines of code affected, find links to documentation with examples of compliant code, control the remediation process, request retests to verify fixes and keep track of their progress in risk mitigation, among other vulnerability management tasks. To help developers easily incorporate vulnerability management into their workflow, Fluid Attacks offers integrations with several tools developers often use.

Fluid Attacks' support in the vulnerability remediation process is through custom and automated fixes generated by AI from Fluid Attacks' IDE extension. Additionally, Fluid Attacks' feature called "Talk to a Pentester," allows its clients to meet with Fluid Attacks' hacking team for guidance on remediation. Further, Fluid Attacks offers a CI agent to prevent the client's development team from deploying software versions with unmanaged vulnerabilities, thus helping to enforce its client's policies and urge the development team to fix the software security issues.

Principal Service Commitments and System Requirements

Fluid Attacks designs its processes and procedures related to the Fluid Attacks application security solution's system ("System") to meet its objectives. Those objectives are based on the service commitments that Fluid Attacks makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Fluid Attacks has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online and in the Fluid Attacks privacy policy and terms of use.

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

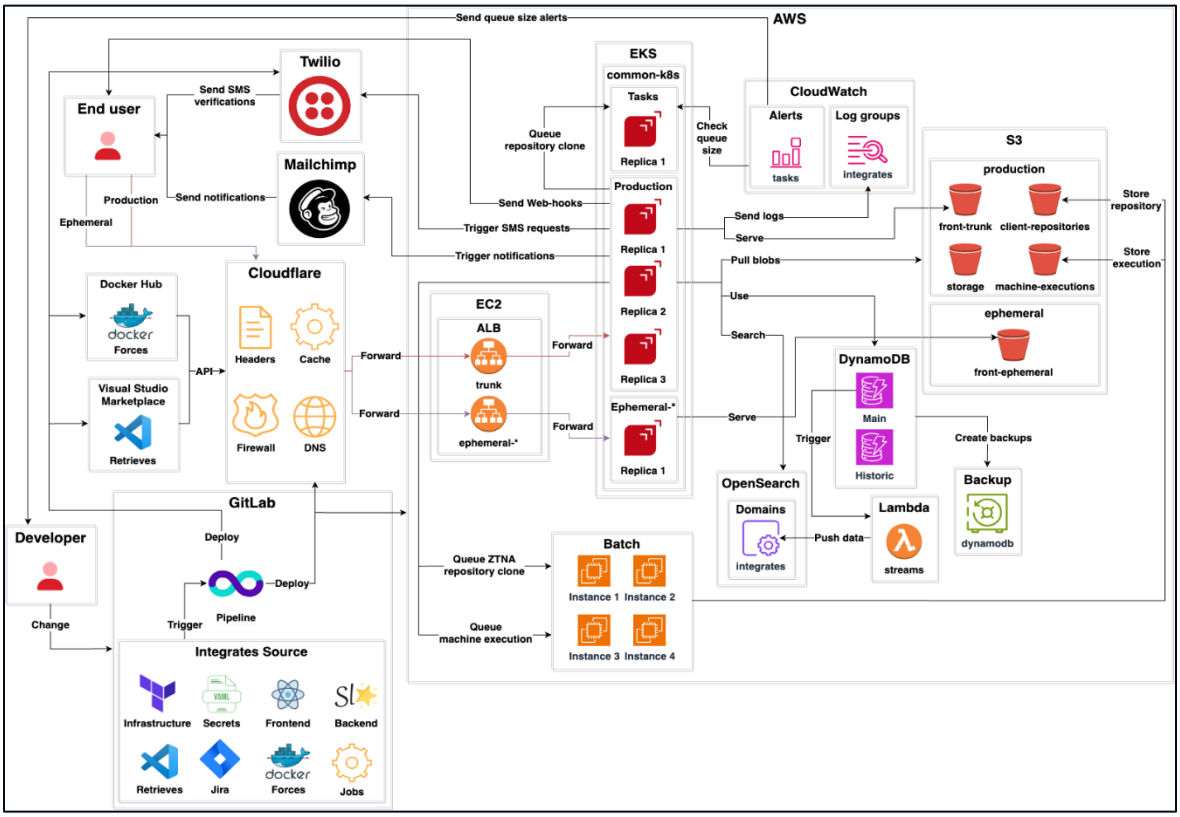
- Use of data retention and data disposal
- Uptime availability of production systems
- Secrets rotation
- Defined service recovery objectives
- Cloud infrastructure served from multiple zones
- Established backup policies
- Use of device formatting and data removal
- Use of a non-disclosure agreement (NDA) for personnel

Fluid Attacks establishes operational requirements that support the achievement of security relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies and/or procedures around how the service is designed and developed, how the system is operated, how the internal business systems and infrastructure are managed, and how employees are hired and trained. In addition, how to carry out specific manual and automated processes required in the operation and development of the System.

Components of the System

Infrastructure

Fluid Attacks maintains a system inventory that includes virtual machines (EC2 instances) and computers (laptops). The inventory documents device name, device type, vendor function, OS, location, and notes. To outline the topology of its system, the organization maintains the following architecture diagram:



The Fluid Attacks application infrastructure is located at the EE.UU. East Region (Northern Virginia) and UE Region (Ireland) data centers. Amazon Web Services (AWS) acts as a hosting subservice organization for the company. The subservice organization provides the physical security and environmental protection controls, as well as, managed services for Fluid Attacks' infrastructure.

AWS' network security uses software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules.

In addition to the firewall, Fluid Attacks exerts endpoint security through Mobile Device Management (MDM), which includes antivirus and antimalware, and forbids end-users from disabling or altering software.

Fluid Attacks' Information Security and Endpoint Security Policies ensure that all computer devices involved in the Fluid Attacks environment have proper virus and malware protection, current virus definition libraries, and the most recent operating system and security patches installed. The IT department verifies that all known and reasonable defenses are in place. In the event of a virus threat, the specific MDM function will remove or quarantine the infected file.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. Fluid Attacks performs continuous security testing to its own technology to detect potential vulnerabilities to the production environment and corporate data. E-mail is scanned at the gateway and in the hosted e-mail environment. All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on Fluid Attacks-owned computers, as enforced through the MDM. Fluid Attacks maintains several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible.

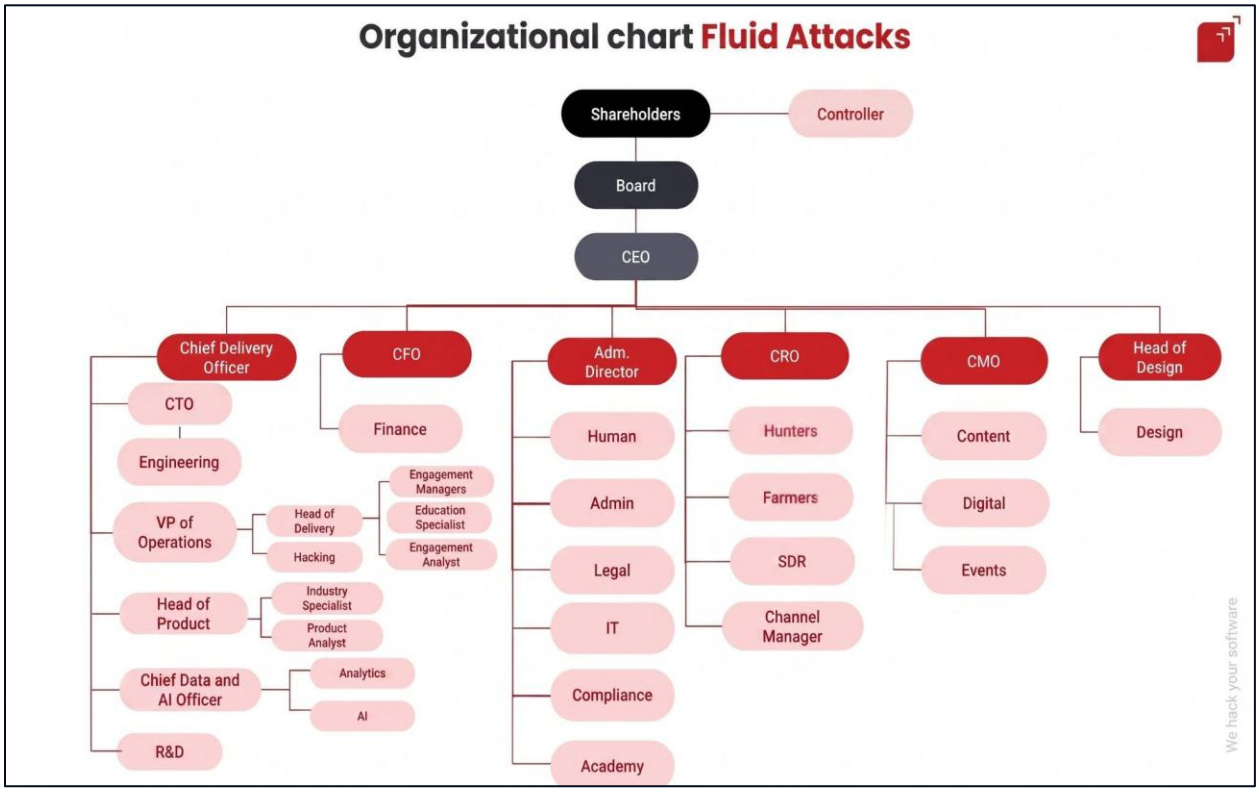
Software

Fluid Attacks maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation. Critical software in use includes the following: Amazon DynamoDB, Amazon S3, Amazon Simple Queue Service (SQS), AWS Batch, AWS CloudWatch, AWS Elastic Compute Cloud (EC2), AWS Elastic Kubernetes Service (EKS), AWS Identity and Access Management (IAM), AWS Key Management Service (KMS), Cloudflare, Datadog, GitLab, Nix, Okta, Google Workspace, Time Doctor 2, dbt Labs, among others.

People

The Fluid Attacks staff provides support to the above services. Fluid Attacks employs dedicated team members to handle all major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and recovery. The company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep Fluid Attacks and its data secure.

Fluid Attacks' corporate structure includes the following roles:



- Board - Provides strategic oversight, guidance, and accountability, ensuring that Fluid Attacks operates in the best interest of its shareholders and stakeholders. The Board's responsibility includes oversight of Fluid Attacks' cyber risk management.
- Chief Executive Officer (CEO) - Handles the strategic direction of Fluid Attacks. The CEO assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments:
    - Chief Delivery Officer (CDO) - Responsible for the technological direction and advancements of the organization. Directs the product, engineering, analytics and service teams to efficiently create/present new services, maintain existing ones, and help support the Fluid Attacks customer base using the service.
    - Chief Technology Officer (CTO) - This role is responsible for the development of Fluid Attacks' platform as well as for enhancing and augmenting the capabilities of Fluid Attacks' vulnerability scanner.
    - Chief Data and AI Officer (CDAO) - Responsible for the organization's data and artificial intelligence strategy and governance.
    - Engineering Team - Responsible for the design, development, deployment, and maintenance of the Fluid Attacks platform and its supporting cloud infrastructure.
    - VP of Operations: Responsible for driving operational efficiency across Engagement Managers, Education Specialists, and Engagement Analysts to ensure seamless security service execution and client engagement.
    - Service - This area is responsible for the activities of Fluid Attacks' hacking team and managing client relationships to ultimately achieve the client's objectives in alignment with Fluid Attacks'.
    - Analytics - This area is responsible for all of Fluid Attacks analytics, providing the information for the company to make decisions supported on reliable data. Moreover, they are responsible for the ideation of the charts and metrics that are presented to end-users on Fluid Attacks' platform.

    - R&D - This area is responsible for Fluid Attacks' research of vulnerabilities in open-source software projects.
- Chief Financial Officer (CFO) - Responsible for overseeing all financial activities and strategies to ensure Fluid Attacks' financial health and stability. Their role involves managing financial planning, budgeting, and forecasting.
- Administrative Director - Responsible for administrative support, human resources procedures, legal and compliance aspects. It is also responsible for daily IT support aspects, including support to end-users with day-to-day issues.
- Chief Revenue Officer (CRO) - Primary role for outbound reach to prospects and completing sales. They are also responsible for the maintenance and renewals of existing customer contracts.
- Chief Marketing Officer (CMO) - Responsible for the outward communication of company initiatives. Primary role responsible for exposing new programs to prospects and existing customers and furthering the public reach of Fluid Attacks.
- Head of Product - This role is responsible for the strategic vision and roadmap of Fluid Attacks' software products, guaranteeing compliance with quality, and therefore security, standards.
- Head of Design - Responsible for developing an intuitive user experience for the Fluid Attacks platform as well as visually appealing designs for Fluid Attacks' products' user interfaces and branding.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements or within the Fluid Attacks Knowledge Base website. Customer data is captured which is utilized by Fluid Attacks in delivering its application security solution.

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. All employees and contractors of Fluid Attacks are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are, subject to limited exceptions confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to Fluid Attacks' business and finances are, as a matter of Fluid Attacks policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, applications and systems is shared by the IT department. Fluid Attacks engineers are responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under their control, moreover, every Fluid Attacks personnel is required to sign a non-disclosure agreement (NDA).

Fluid Attacks has policies and procedures in place to ensure prior retention and disposal of confidential and private data. The retention and data destruction policies define the retention periods and proper destruction procedures for the disposal of data. These policies are reviewed at least annually. The destruction of data is a multi-step process. Client accounts and data are deleted upon termination of the contract.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Cloud networks are protected by enterprise-class firewalls and appropriate enterprise-class virus protection is in place. Passwords protection with assigned user rights is required for access to the applications and databases. Access to the cloud's network, applications, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

Data is categorized in the following major types of data used by Fluid Attacks:

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Fluid Attacks	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Fluid Attacks. Fluid Attacks must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information	• Customer operating data • Customer PII • Customers' customers' • PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Fluid Attacks to operate the business. Fluid Attacks must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information	• Legal documents Contractual agreements • Employee PII • Employee salaries

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe logical access, computer operations, change management, incident management, and data communication standards in order to obtain the stated objectives for system and data security, data privacy, and integrity for both the company and its clients and define how services should be delivered. These are communicated to employees and located within the organization's intranet.

Reviews and changes to these policies and procedures are performed annually and are approved by senior management.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system.

Logical Access

Fluid Attacks uses an IAM platform for managing access to applications across the company. Logical access to Fluid Attacks' applications and data is limited to properly authorized individuals. Further, Fluid Attacks' infrastructure components always grant minimum privileges only to the applications and personnel that need to use them. Distributed firewall is behind the Fluid Attacks domain that implements full DDoS protection, browser integrity check, hotlink protection, rate limiting, browser integrity check, and anti-bot capabilities. Appropriate firewall rules, managed by top cybersecurity experts, are in place to restrict access to customer data and to limit the possibility of disruptions to customer operations from unauthorized users.

Computer Operations - Backups

Customer data is backed up and monitored by the Engineering Team for completion and exceptions. If there is an exception, Engineering Team will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations - Availability

Fluid Attacks maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

Fluid Attacks internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Fluid Attacks utilizes its own vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

Change Control

Fluid Attacks runs an Application Build Process for every change any one developer wants to introduce to Fluid Attacks' source code in the continuous integration and continuous delivery (CI/CD) system via a merge request. Developers also need to ask a peer to review their code changes before their merge requests can go into production. Peer-reviewers usually evaluate code quality, commit message coherence, and other semantic properties of the change.

CI/CD helps to maintain source code versions and migrate source code through the development process to the production environment. The CI/CD maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Fluid Attacks has a Change Management and Software Development Policy in place to define requirements for establishing and maintaining baseline protection standards for the company's applications and infrastructure, and to ensure that a standard set of minimum requirements are established for changes that are made to production systems and supporting infrastructure across the organization. The Fluid Attacks Change Management Policy applies to all individuals performing software development tasks and system administration within the organization, as well as to production systems and supporting infrastructure across the organization.

Boundaries of the System

The scope of this report includes the Fluid Attacks Application Security Solutions System performed in the Garner, North Carolina and Medellin, Colombia facilities.

This report does not include the cloud hosting services provided by AWS from multiple facilities.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

On October 20, 2025, Fluid Attacks experienced a service disruption caused by a widespread outage affecting multiple AWS services on which its infrastructure relies. Although AWS issues began around 12:11 a.m. (GMT-5), the platform continued operating until approximately 9:15 a.m., when service degradation began impacting the platform, agent, and API-dependent services. The incident was detected within 15 minutes by automated monitoring, and full recovery took approximately 8.4 hours, resulting in a total exposure window of 8.6 hours. While AWS worked to restore service availability, Fluid Attacks implemented infrastructure adjustments and redeployment activities to ensure systems could reconnect and resume normal operations once AWS stabilized. The company determined the root cause to be a third-party provider failure rather than an internal operational or security issue, and reported no indication of data compromise. As a corrective action, Fluid Attacks is pursuing more self-contained infrastructure architectures to reduce dependency-related risks and improve overall service resilience.

Criteria Not Applicable to the System

All Common/Security criteria were applicable to the Fluid Attacks Application Security Solutions System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at multiple facilities.

Subservice Description of Services

The cloud hosting services provided by AWS support the physical infrastructure of the entities services.

Complementary Subservice Organization Controls

Fluid Attacks' services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Fluid Attacks' services to be solely achieved by Fluid Attacks control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Fluid Attacks.

The following subservice organization should be implemented by AWS and included in this report to provide additional assurance that the trust services criteria are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Physical access points to server locations are managed by electronic access control devices.
		Electronic IDS are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Fluid Attacks management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Fluid Attacks performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the

COMPLEMENTARY USER ENTITY CONTROLS

Fluid Attacks' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Fluid Attacks' services to be solely achieved by Fluid Attacks control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Fluid Attacks'.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Fluid Attacks.
2. User entities are responsible for notifying Fluid Attacks of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Fluid Attacks services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Fluid Attacks services.
6. User entities are responsible for providing Fluid Attacks with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Fluid Attacks of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.