FUEL CYCLE SECURITY WHITE PAPER

2021

Fuel Cycle Security Paper

1. **Audit & Compliance**
   - 1.1. SOC 2 Type 2
   - 1.2. HITRUST CSF
   - 1.3. GDPR
2. **Software Development Security**
   - 2.1. In-house Development
   - 2.2. OWASP
   - 2.3. Code Review & Merging
   - 2.4. Code Vulnerability Analysis
   - 2.5. Quality Assurance
   - 2.6. Development Environments
3. **Infrastructure Security**
   - 3.1. Amazon Web Services
   - 3.2. Patches
   - 3.3. Data Encryption
   - 3.4. Federated Multitenant Database
   - 3.5. Firewall
   - 3.6. Intrusion Detection & Intrusion Prevention
   - 3.7. Logging & Monitoring
   - 3.8. Backups
   - 3.9. Disaster Recovery
   - 3.10. Infrastructure Access
   - 3.11. Infrastructure Change Management
4. **Application Security**
   - 4.1. Manual Penetration Testing
   - 4.2. Password Settings
   - 4.3. Antivirus
   - 4.4. Account Creation MFA
   - 4.5. Single Sign On
   - 4.6. IP Filtering
   - 4.7. Data Segregation
   - 4.8. Data Retention & Destruction
   - 4.9. Application Change Management

Executive Summary

Fuel Cycle is a provider of data insights and a data operator which implicitly makes the data security a top concern.

Our Software Development Life Cycle (SDLC) is a mature process meeting or exceeding the latest industry security specs starting from the design process, through development, deployment, networking, to application access and availability.

Fuel Cycle applications are held to a very high standard of quality, by a dedicated in-house team of quality assurance specialists, ensuring the application performs as expected on a variety of devices and environments, including in high stress situations.

We are big believers in objective security testing, so we have several layers of 3rd party security test (Static Code Analysis, Manual Penetration Testing) and compliance auditing (SOC 2, HITRUST CSF).

Fuel Cycle uses AWS for a secure, fault-tolerant, highly available and scalable cloud infrastructure. Under the shared responsibility model, AWS is responsible for the underlying infrastructure that supports the cloud.

Our enterprise grade cloud solution is built with the right mix of innovative and proven technologies, taking advantage of the latest cloud and AI capabilities while resting on a stable Java and MySQL backbone.

1. Audit & Compliance

SOC 2 Type 2

Fuel Cycle goes through an annual SOC 2 Type 2 audit completed by Auditwerx, reviewing the Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy. The report covers the Fuel Cycle application, AWS & Office infrastructure and operations.

SOC stands for "system and organization controls," and the controls are a series of standards designed to help measure how well a given service organization conducts and regulates its information. It is an expensive and effort intensive process, requiring dedication and discipline and Fuel Cycle is one of the few in the Market Research industry that go through a SOC 2 Type 2 audit.

SOC 2 looks at five Trust Factors of secure data processing and storage. Demonstrating proficiency across one of more of these criteria is an attestation to the privacy and security controls:

1. **Security**: the system is protected against unauthorized access, both physical and logical
2. **Availability**: the system is available for operation and use as committed or agreed
3. **Processing Integrity**: system processing is complete, accurate, timely, and authorized
4. **Confidentiality**: information designated as confidential is protected as committed or agreed
5. **Privacy**: personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with the criteria set forth in Generally Accepted Privacy Principles (GAPP).

The latest Fuel Cycle SOC 2 Type 2 report can be made available upon request.

HITRUST CSF

The Health Information Trust Alliance, or HITRUST, is a privately held company located in the United States that, in collaboration with healthcare, technology and information security leaders, has established a Common Security Framework (CSF) that can be used by all organizations that create, access, store or exchange sensitive and/or regulated data. The CSF includes a prescriptive set of controls that seek to harmonize the requirements of multiple regulations and standards.

HITRUST is led by a management team and governed by an Executive Council made up of leaders from across a variety of industry. These leaders represent the governance of the organization, but other founders also comprise the leadership to ensure the framework meets the short and long term needs of the entire industry. Executive Council members represent the following organizations:

- Anthem, Inc.
- Express Scripts, Inc.
- Health Care Service Corporation
- Highmark
- Humana Inc.
- IMS Health
- Kaiser Permanente
- McKesson Corporation

- UnitedHealth Group

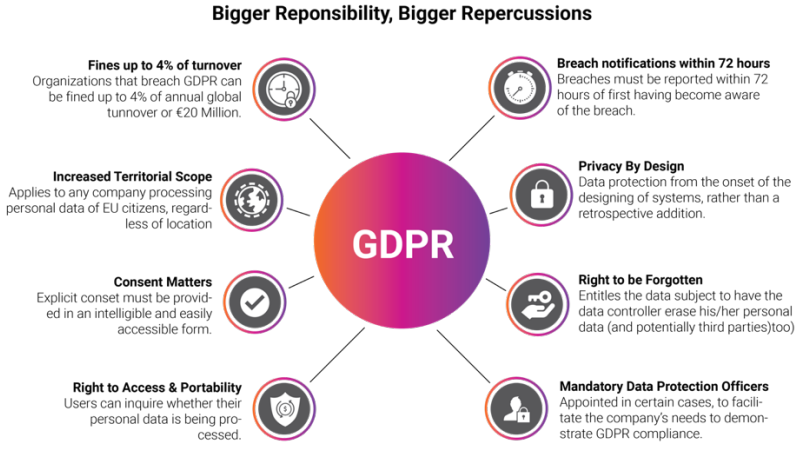
Building on top of SOC 2 controls, Fuel Cycle has implemented controls addressing HITRUST CSF version 9 requirements covering the TSC categories relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy.

GDPR Compliance

Fuel Cycle is both EU-US Privacy Shield and Swiss-US Privacy Shield Certified and has an enduring commitment to handling personal data in alignment with best industry practices.

As Data Processor we offer a very solid mechanism for GDPR compliance, but it's up to the Client (as Data Controller) to properly configure and enforce the available GDPR features:

- **Know Your Rights.** Fuel Cycle applications have a reserved page located atyourcommunityurl.com/privacy. This page is intended to be one-stop for all privacy-related information and data management for community members.
- **User Explicit Consent**. To ensure our customers are always in the right, we have automatically created a privacy trigger when a community member accesses your Fuel Cycle community for the first time from the European Union.
- **Customizable PII Designation**. In the Administration area, fields like first name, last name and email address are designated PII by default but the Researcher can designate any other fields as PII.
- **Least Privilege Access**. Access to PII is managed by the Researcher following the principle of Least Privilege which says that personally identifiable information should be accessible to the least number of people possible and those people must have a compelling business need to access this information.
- **User Data Export**. Members can anytime download the data they've provided to the platform, including algorithmically-defined data like many market research segmentation or typing tools.
- **The Right To Be Forgotten**. If members choose to be forgotten, their account will be closed and their data permanently removed.



California Consumer Privacy Act (CCPA)

Effective January 1st, 2020 the California Consumer Privacy Act ("CCPA") provides California residents with increased control in terms of how their personal information may be utilized by businesses, and also encompasses a number of specific rights that enable consumers to better control, understand and restrict the use of their personal information for business purposes.

With the introduction of CCPA, consumer privacy laws in the spirit of the General Data Protection Regulation are no longer exclusive to Europe. CCPA expands upon consumers' rights concerning their data and privacy, extends the definition of personal data requiring protection, and places additional requirements on businesses for acknowledging and satisfying consumers' data and privacy related requests.

As a general platform functionality, Fuel Cycle members will be able to invoke their CCPA-related rights in an automated and self-service process. The following is an overview of the general consumer rights and requests that community members may exercise under CCPA, and how Fuel Cycle can help support and process such requests.

Right	**What does it mean?**	**How does Fuel Cycle help?**
Privacy Disclosure Notice	Businesses are responsible for ensuring that their members are provided with CCPA compliant disclosures, including information about the categories of personal information collected, the business purpose for collection, the categories of third parties that the information is shared with, and the methods by which consumers may submit requests.	Every Fuel Cycle community includes a dedicated and accessible landing page for providing your company's CCPA compliant disclosures. Each privacy landing page is customizable and can include a privacy policy drafted by you, an overview of the types of personal data collected, and a disclosure of your business's purpose of collecting and sharing members' data. Additionally, Fuel Cycle provide you with methods for allowing your members to self-request the deletion, access and export of any personal information in an automated fashion through the privacy landing page.
Right to Data Portability	Members have the right to receive a copy of their personal information collected by a business in a structured format that allows the member	Fuel Cycle provides you with a mechanism for allowing your members to self-request a data export file from your community's privacy landing page that which provides all

	to transmit the information without hindrance.	collected personal information in CSV format.
Right to Access	Members have the right to obtain information on the personal information held about them.	Fuel Cycle provides you with methods for allowing your members to self-request the specific pieces of personal information you maintain on them.
Right to Data Destruction	Members have the right to have their personal information permanently removed.	Fuel Cycle provides you with a mechanism for allowing your members to self-request account and personal information destruction from your community's privacy landing page. A requesting member must undergo an account verification process before the data destruction request is processed. Account and data destruction are permanent and irreversible. Members who request account and data destruction will no longer have access to their account, and all associated personal information will be destroyed and removed from the platform.

2. Software Development Security

In-house development

The entire engineering group is part of Fuel Cycle's team, we do not outsource our development to 3rd parties. This increasingly rare quality ensures maximum efficiency, security and minimizes response time.

Or development flow is based on an Agile framework, using Kanban for Sprints and project management. We have a mature Research & Development organization, with 6 engineering groups:

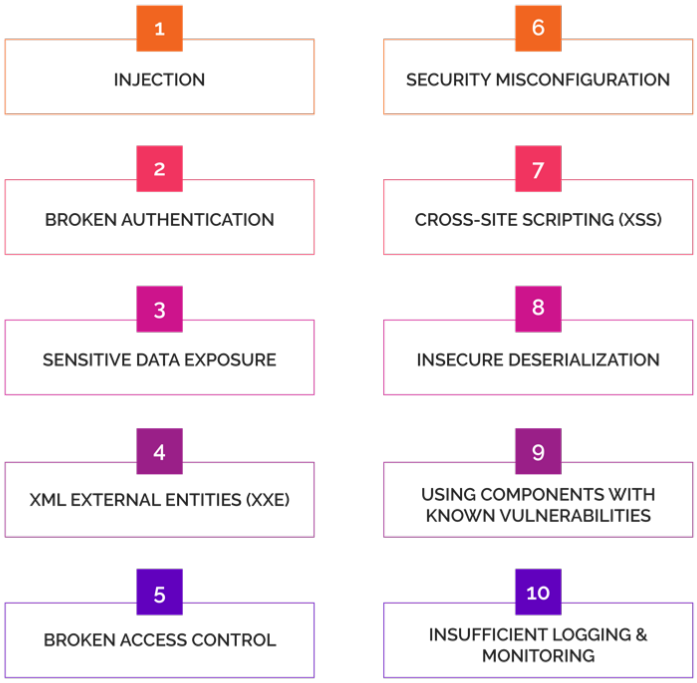
- Backend
- Frontend
- Mobile
- QA
- DevOps
- Advanced Analytics

OWASP

All engineers part of Fuel Cycle's development team are required to adhere to the OWASP top 10 standards:

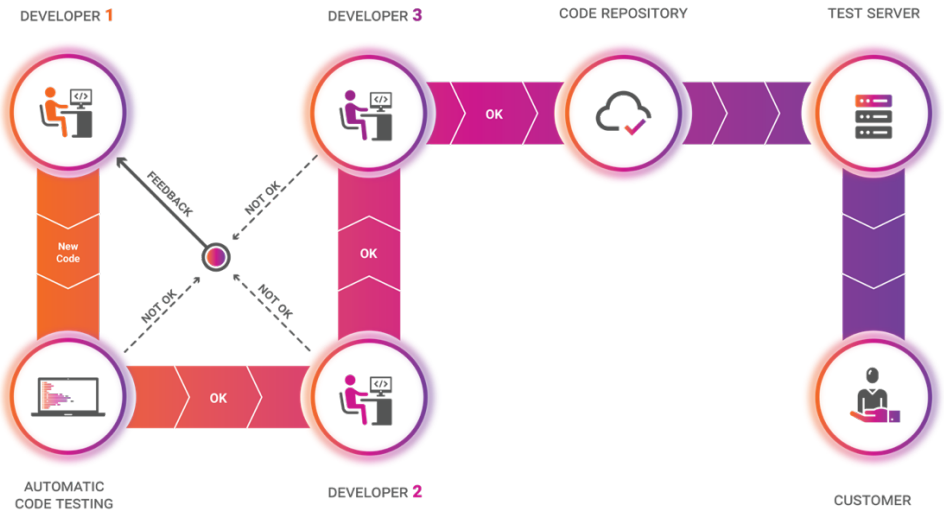
1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

The application is routinely tested for the OWASP standards by third party security providers and the vulnerabilities are addressed in real time.



Code Review & Merging

Every line of code is reviewed by one or more senior engineers, ensuring for best coding practices, efficiency, code reutilization, minimizing collaterals and visible flaws. This also helps spreading the know-how around, eliminating knowledge silos and single points of failure.
All branch merges are reviewed by the Director of Engineering, as a final measure of control.



Code Vulnerability Analysis

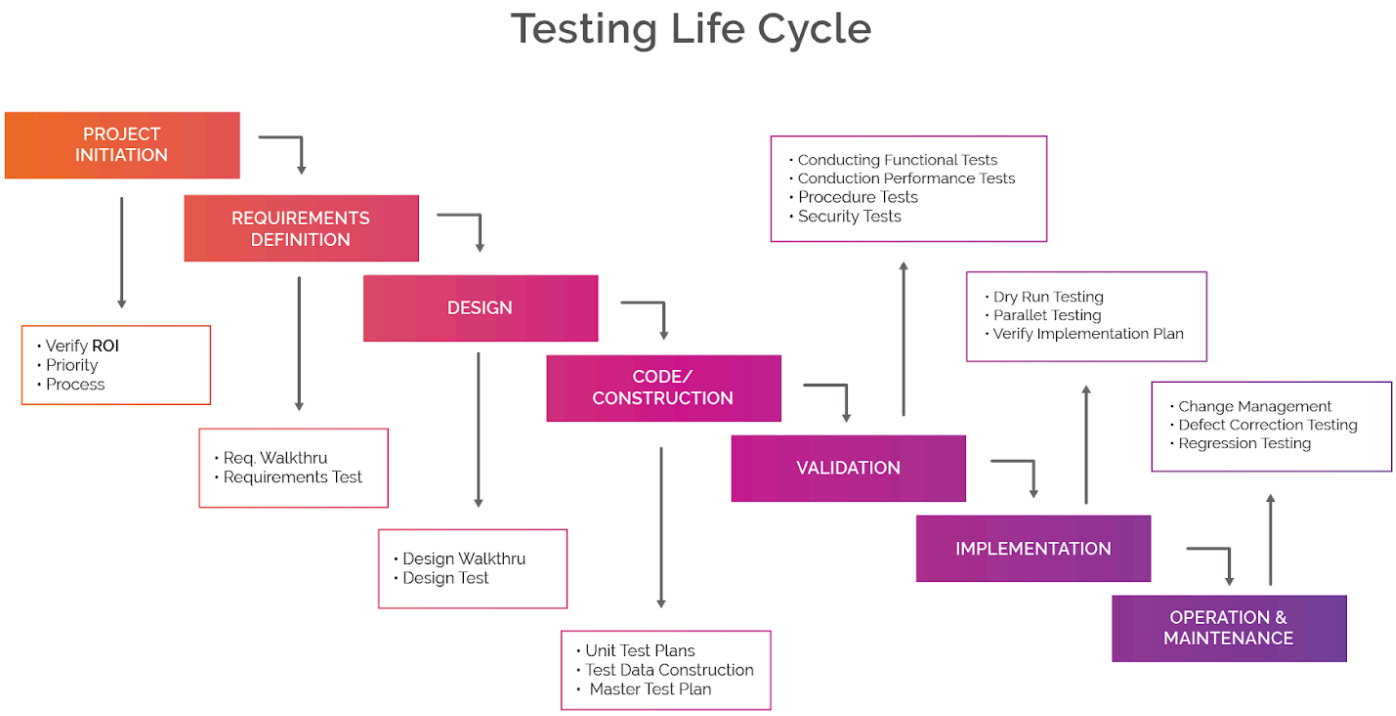
The Static Code Analysis is an integral part of Fuel Cycle security strategy and is performed on a quarterly basis by Micro Focus Fortify On Demand (ex HPE).

The Static Code Analysis (white-box testing) is an automated and repeatable scan within a non-running environment for a deep scan of the source code and the 3rd party libraries, detecting over 988 unique categories of vulnerabilities across 25 programming languages that span over 999,000 individual APIs.

This method of security testing has distinct advantages in that it can evaluate both web and non-web applications and through advanced modeling, can detect flaws in the software's inputs and outputs that cannot be seen through dynamic web scanning alone.

Quality Assurance

Fuel Cycle has a robust Quality Assurance framework, where people and machine work together to minimize the number of bugs and also perform manual security and privacy tests.



Permanently scanning reports, exports, listing pages, checking for correct PII handling, testing forms submission and other features prone to data issues, the QA group is an added layer ensuring flawless data segregation and privacy compliance.

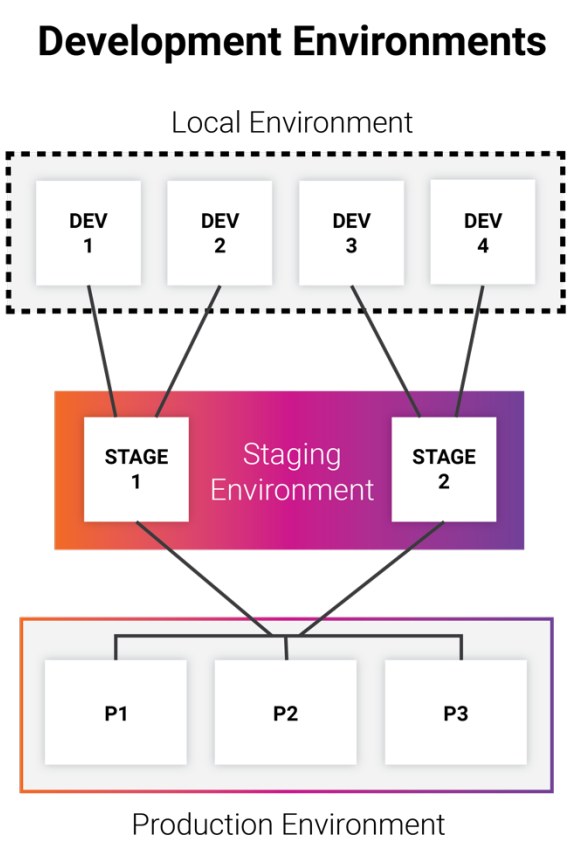
Development Environments

Fuel Cycle has three distinct environments where the code is being written, reviewed, merged into the stream, scanned, QAed, compiled and released to public.

The Local environment is the engineer's personal machine where the code is initially developed. Though the software replicates the Production (live) environment, the hardware is different so the testing capabilities are limited.

The Staging environment is a private replica of the Production environment, where the code is deployed and tested. Both software and hardware are exactly the same as in the Production environment, in order to create as close as possible replica in which to run as many test cases as possible.

The Production environment is where Fuel Cycle's application is used by clients and their members. Adhering to the Segregation of Duties principle, the code releases on Production are done by the DevOps Specialist only and the engineers do not have access to anything Production related.



3. Infrastructure Security

Amazon Web Services

Fuel Cycle applications are hosted in the cloud, using Amazon Web Services (AWS), the biggest cloud provider in the world, using a shared security responsibility model. AWS offers the necessary performance, reliability and security that a business like Fuel Cycle needs.
Fuel Cycle utilizes AWS for Infrastructure as a Service (IaaS) while AWS is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud.

For high availability and redundancy, Fuel Cycle instances are located in two separate data centers: North Virginia and Oregon.
AWS data centers are housed in nondescript facilities. Physical access is strictly controlled, both at the perimeter and at building ingress points by professional security staff, utilizing video surveillance, intrusion detection systems, and other electronic means.

Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
All physical access to data centers by AWS employees is logged and audited routinely.

AWS has all the compliance certifications and attestations Fuel Cycle requires from its infrastructure provider:

- AWS SOC 2 Security, Availability & Confidentiality Report
- AWS SOC 3 Security, Availability & Confidentiality Report
- ISO/IEC 27001:2013
- ISO/IEC 27017:2015
- ISO/IEC 27018:2014
- EU-US Privacy Shield

CUSTOMER:
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA		
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT		
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION		
CLIENT-SIDE DATA ENCRUPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORK TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS:
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

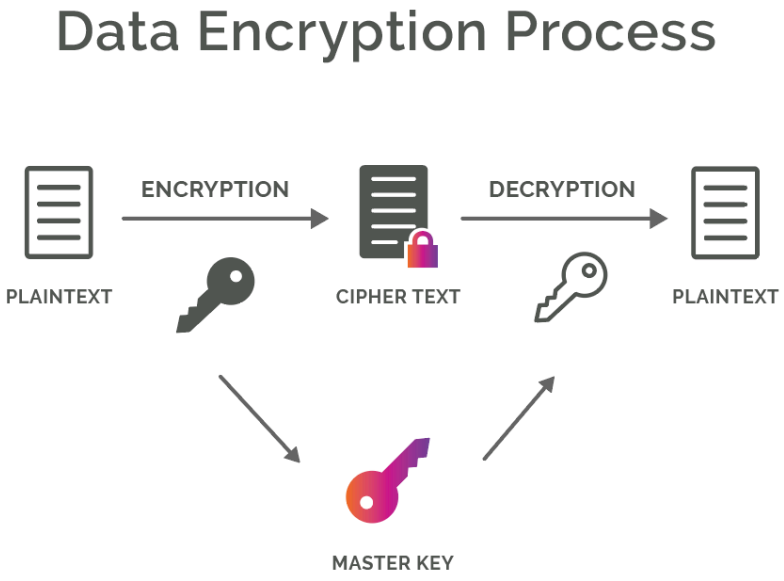
SOFTWARE			
COMPUTE	STORAGE	DATABASE	NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE			
REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS	

Patches

Infrastructure patches are applied monthly or as needed. The patch content is compiled and approved by the DevOps Specialist and the Director of Engineering for maximum compatibility with Fuel Cycle's software. The patch is then deployed by the DevOps Specialist at a time of very low traffic.

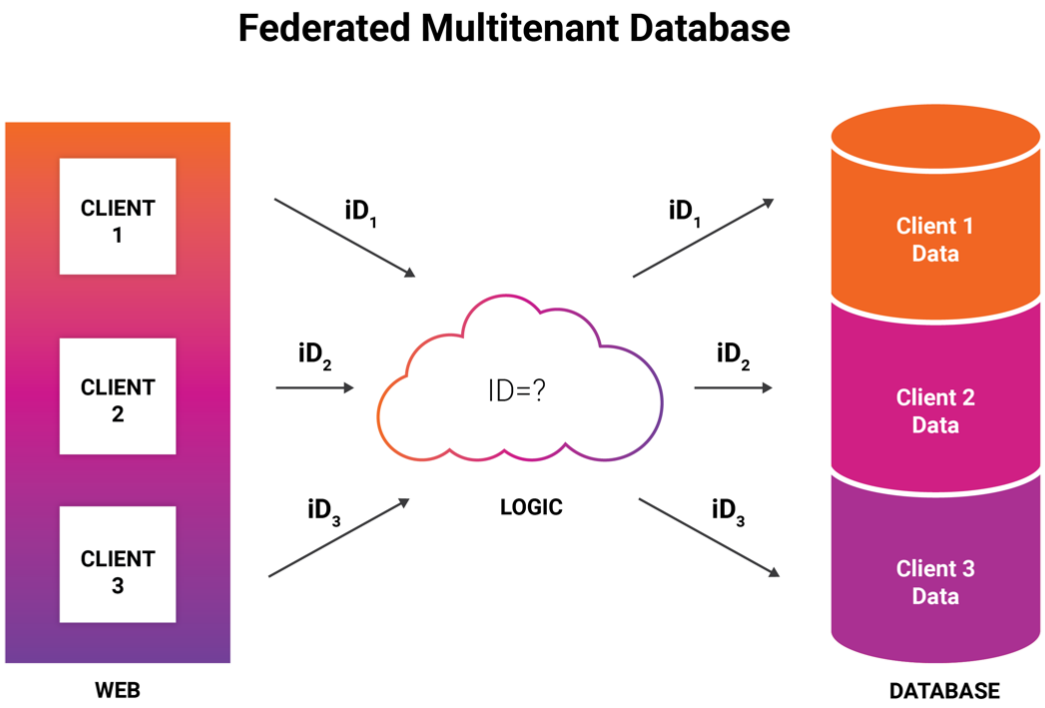
Data Encryption

All Fuel Cycle data is encrypted at rest and in transit. At rest, the data is encrypted at disk level (files and database) and it resides in a private subnet that is only accessible via our web application. Fuel Cycle application can only be accessed via HTTPS and the data in transit is encrypted at all times using TLS.



Federated Multitenant Database

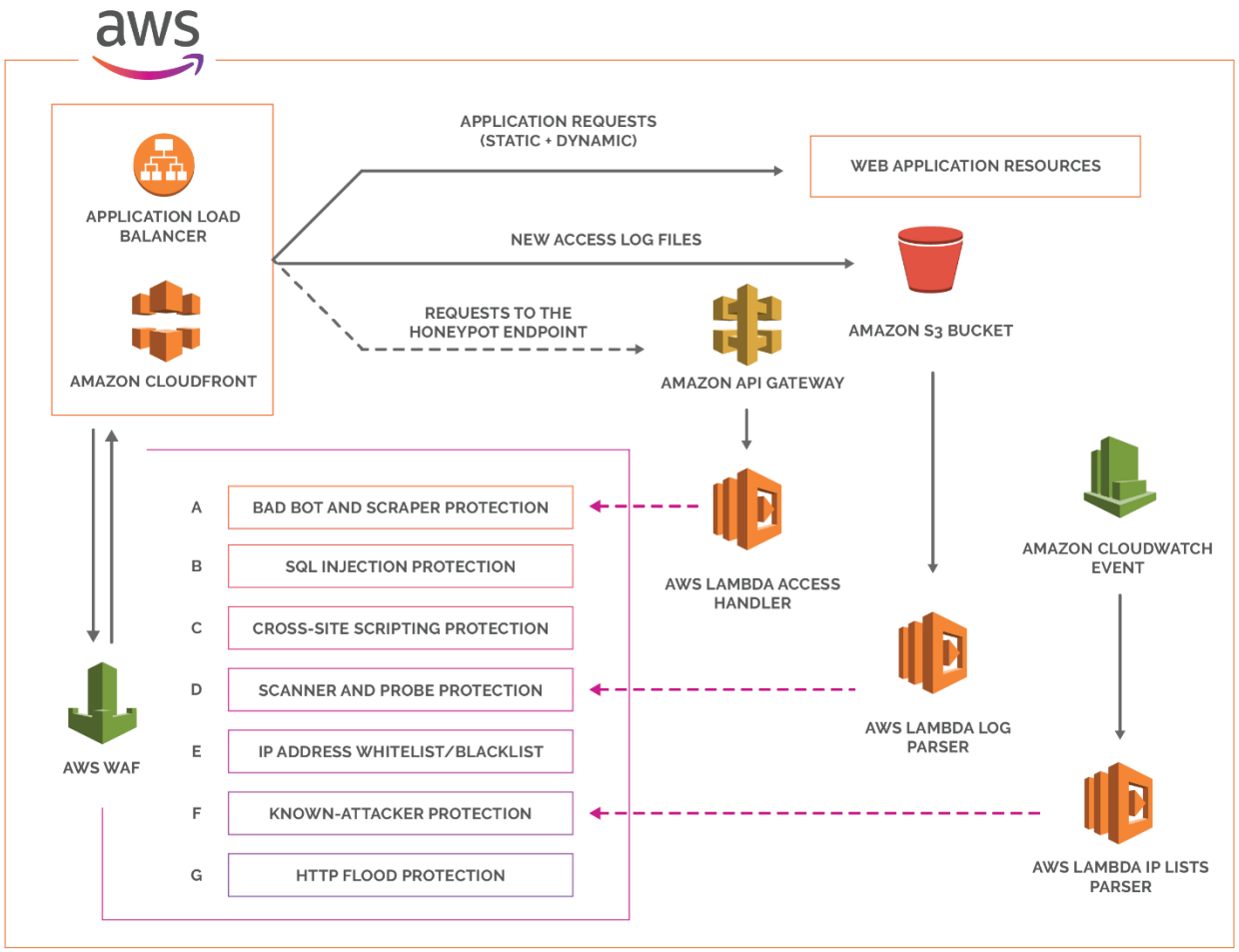
Data segregation, security and availability is paramount in the Fuel Cycle application. We logically separate the data of our clients using unique client IDs for each record in the database and we have redundant layers of logic in the controllers to ensure cross-talk never happens.



Firewall

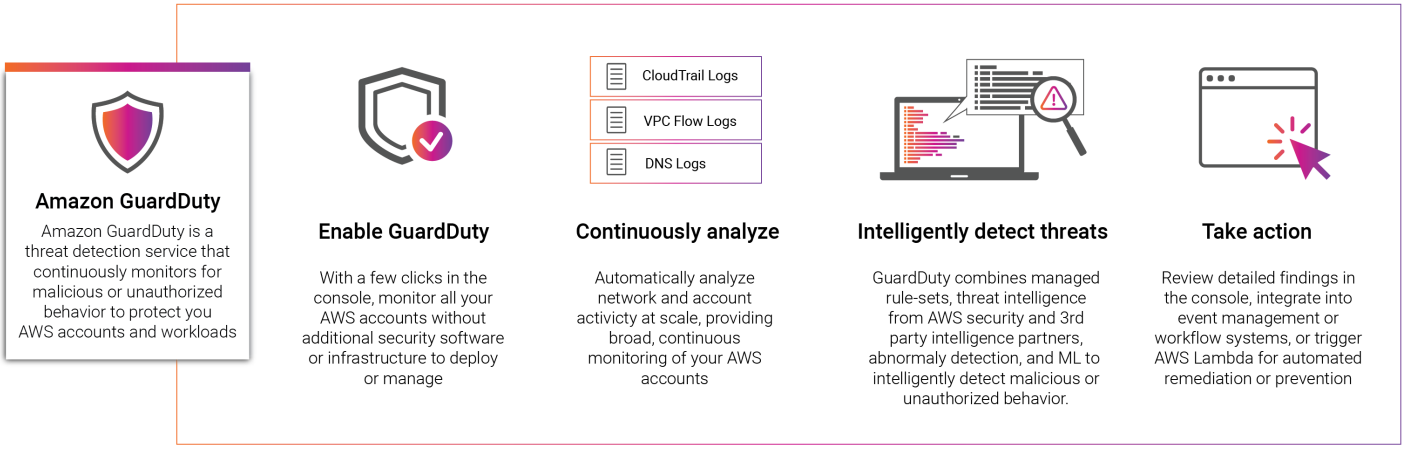
AWS WAF (Web Application Firewall) is a web application firewall that helps protect our application from common web exploits that could affect application availability, compromise security, or consume excessive resources.
The firewall restricts traffic by protocol, by service port, and by source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block). By default, WAF is in deny-all mode, and we only opened the minimum ports necessary for inbound calls.

The AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors have no more access to that instance than any other host on the Internet. They can be treated as if they are on separate physical hosts.



Intrusion Detection & Intrusion Prevention

We are using Amazon GuardDuty in combination with Amazon WAF to permanently monitor, asses, alert and prevent any malicious activity and unauthorized behavior. GuardDuty uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats by analyzing tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs.



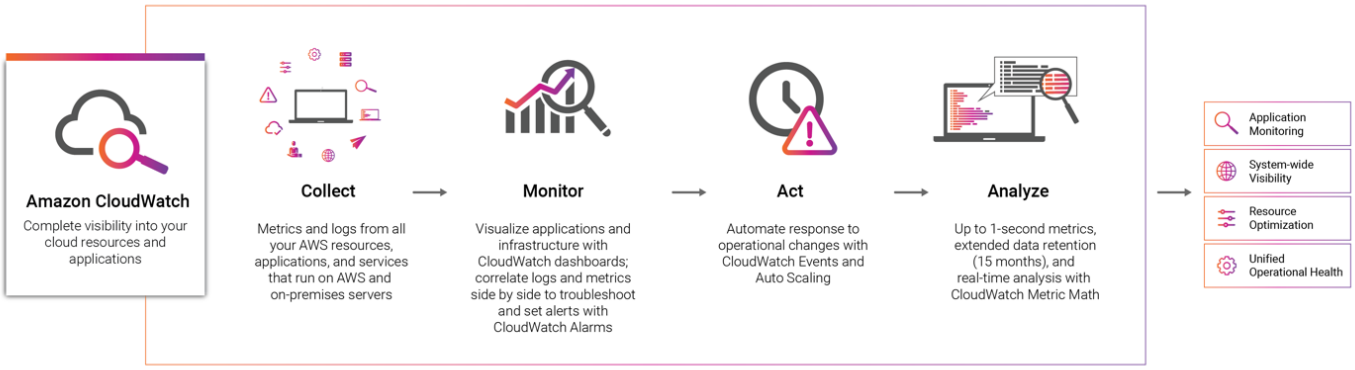
Logging & Monitoring

Fuel Cycle logs important events across its applications and infrastructure that provides us with data and actionable insights to monitor, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.

We are using AWS CloudWatch for infrastructure monitoring, AppDynamics for application related events, custom database logs for user actions, and we pull everything in Splunk.

Our database logs captures entries that contain the date, time, client information, user information, operation performed, and source IP address for most of the actions performed by the public.

If there is suspicion of inappropriate behavior, Fuel Cycle can provide user log entry records to assist in forensic analysis. This service is provided on a time and materials basis.

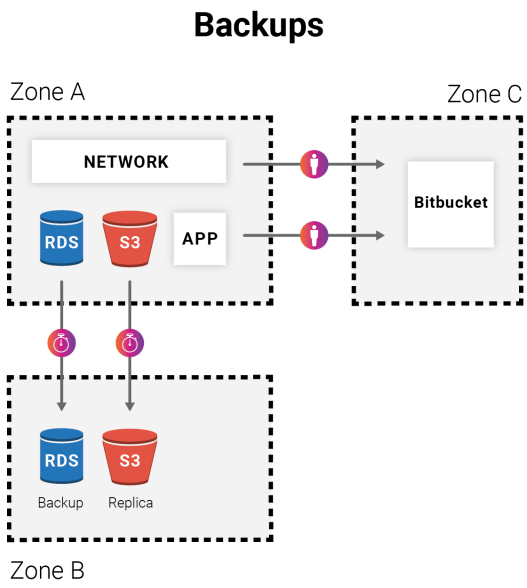


Backups

We back up the data in real-time (delta) and in daily full-backups, with a trail of 30 days. The backups are then saved in a different AWS region from where we have our Production environment.

Component	Backup Process	Owner, Frequency
Network (VPC, routing tables, LB, etc)	Terraform code stored in Bitbucket	DevOps, manual, ad-hoc
EC2 (Web, API, Jobs, Search)	AMI's copied in Oregon	DevOps, manual, ad-hoc
RDS	Snapshots copied in Oregon	Lambda, automated, daily
S3	Real-time replication in Oregon	SaaS, automated, real time
Codebase	Bitbucket check-in	Developer, manual, ad-hoc

If the backup fails, we get alerted. If the backup saving/copying to a different region fails, we get alerted as well. We regularly test the backups as part of our Disaster Recovery exercises, to ensure data and infrastructure can be properly and swiftly recovered if disaster strikes.



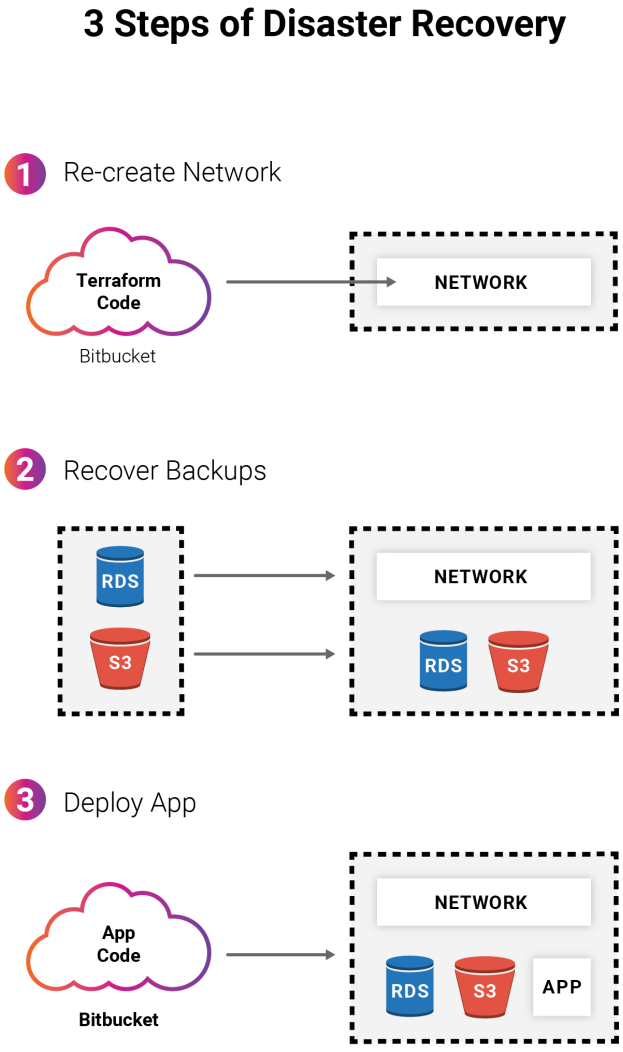
Disaster Recovery

A well-rehearsed disaster recovery plan makes the difference between going out of business and just having an ugly downtime. Despite AWS native redundancy, sometimes disaster strikes and an entire region goes dark for an indeterminate period of time, or with significant data loss.

In such extremely rare cases, Fuel Cycle is able to quickly spin up a new infrastructure in a completely different AWS region and resume operations with minimal or no data loss, in no more than 20 hours.

That is possible because the multi-region real-time data replication and full backups that we do for every bit of data in our platform, including infrastructure architecture. We also use Terraform (Infrastructure As Code - IsC) to create a code blueprint of the entire AWS backbone.

Recovery Time Objective (RTO) is 20 hours, and represents the time needed to recreate the environment from scratch. This does not include the time necessary for setting up the domains that are managed by the Client. Recovery Point Objective (RPO) is 24 hours and represents the time since the oldest backup.



Infrastructure Access

The access to Fuel Cycle's infrastructure is highly restricted and has multiple layers of security. Based on the principle of Least Privilege, only the DevOps Specialist has access to AWS console and servers, only via Virtual Private Network (VPN), Secure Shell (SSH) and Multifactor Authentication (MFA).

In general, access to various applications and services used in Fuel Cycle is given only when is absolutely required for an individual to perform their tasks, and it's reviewed monthly or as needed, as per Access Management Policy.

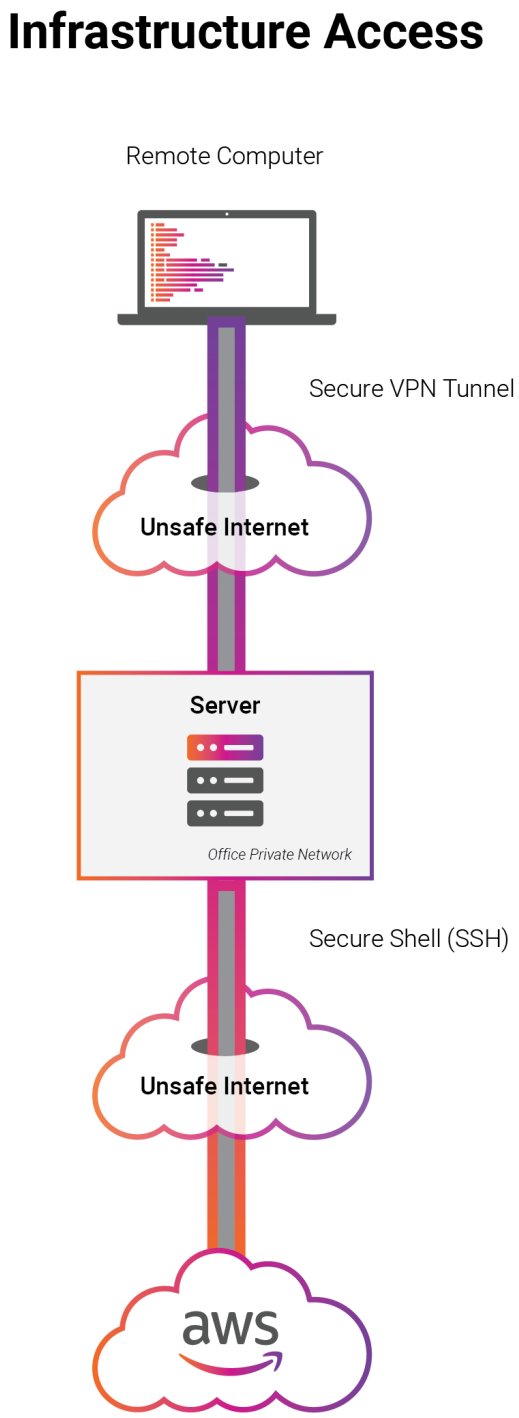
We also have a quarterly review of the access logs of the critical applications, to spot any unauthorized events that might have escaped all other controls.

Infrastructure Change Management

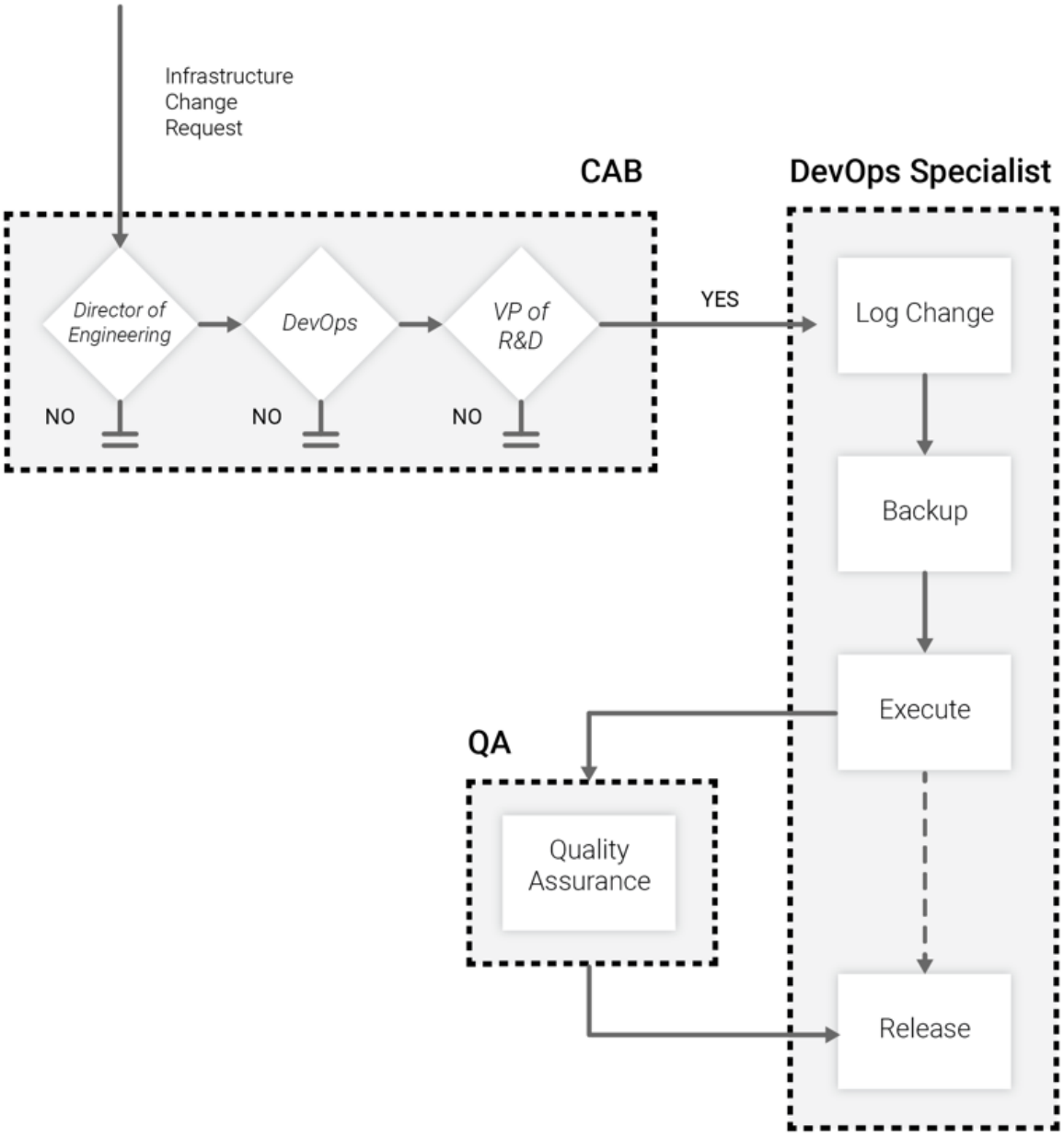
Infrastructure changes range from simple configuration updates to adding new servers or technologies.

All infrastructure changes follow the Infrastructure Change Management Policy: they have to be approved by the Director of Engineering, VP of R&D and executed by the DevOps Specialist.

The changes are logged and tracked into JIRA and backups are performed before the change is applied. Based on the type of change, QA might be performed on Stage and after the change was applied in Production.



Infrastructure Change Environment



4. Application Security

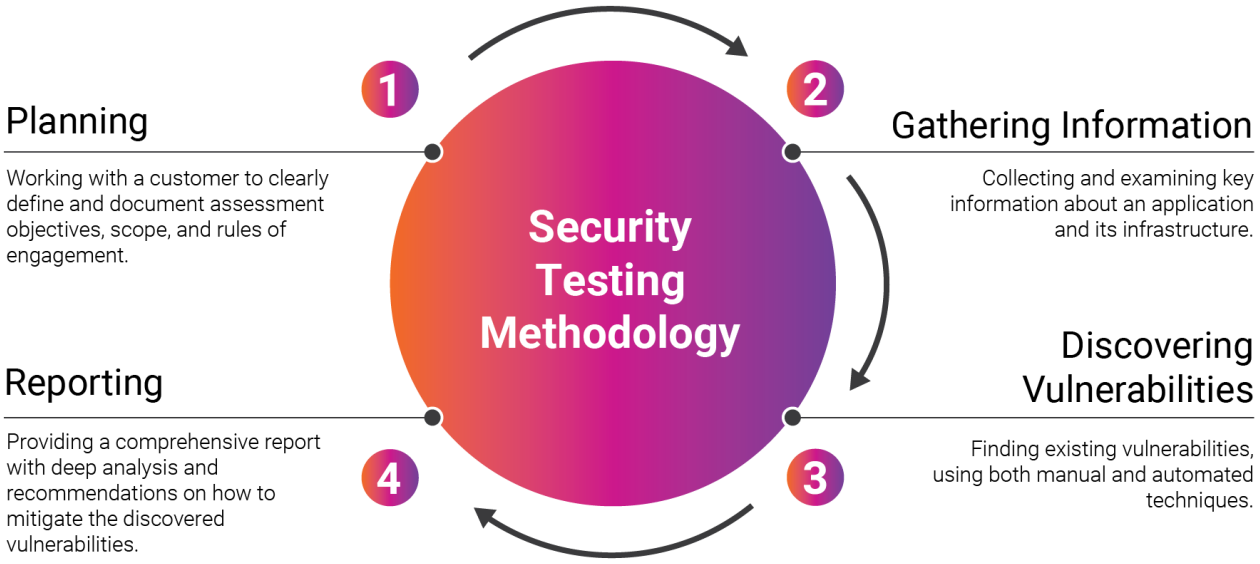
Manual Penetration Testing

Application Manual Penetration Testing is the most comprehensive test a web application can go through. It's a combination of Black Box and White Box testing, dynamic scans, and ethical hackers trying to find vulnerabilities and exploit them in a safe and controlled environment.

Fuel Cycle performs bi-annual MPTs using Microfocus' (ex HPE) Fortify On Demand service in the Production environment on a test instance of the application that can be safely abused during the test.

The test takes up to 5 days to complete, the list of vulnerabilities is reviewed by the VP of R&D and the Director of Engineering, prioritized and put in development. The vulnerabilities are addressed based on criticality:

Vulnerability Type	Remediation ETA
Critical	1 business day
High	2 business days
Medium	5 business days
Low	20 business days
Info	As needed



After all the vulnerabilities are addressed, the test is executed again to verify that the all issues have been fixed. The cycle repeats until all Critical, High and Medium vulnerabilities have been fixed. Low and Info are spread out over a longer period of time, depending on the resources available.

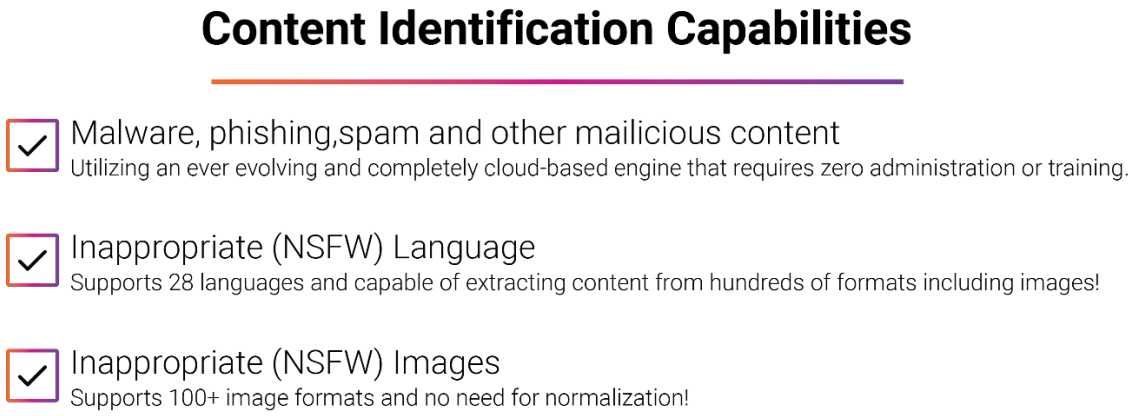
Password Settings

Fuel Cycle has a very robust and highly customizable password settings feature in its application:

- **Password Strength Policy**. Can be customized by each client in their instance of the application:
  - Normal: Minimum of 6 characters, Lower case, Upper case
  - Strong: Minimum of 8 characters, Lower case, Upper case, Number
  - Very Strong: same requirements as Strong with the addition of a Special Character
- **Password History Policy**. Can be set to 1, 2, 3 or 5 past passwords, basically how many previous passwords the user is prohibited from reusing.
- **Password Expiration Policy**. Can be set to 30, 60, 90 or 120 days.
- For manually created new accounts, passwords need to be reset before first login.
- **Account Lockout Policy**. Can be configured to lock the user out of their account if the password and/or username has been entered incorrectly more than 1, 2, 3 or 5 times.
- **Password Reset Policy** follows a very secure flow:
  - User requests password reset
  - System emails a link
  - User follows the link to a page where they enter the Current Password and the New Password.
  - User is redirected to the Login page

Antivirus

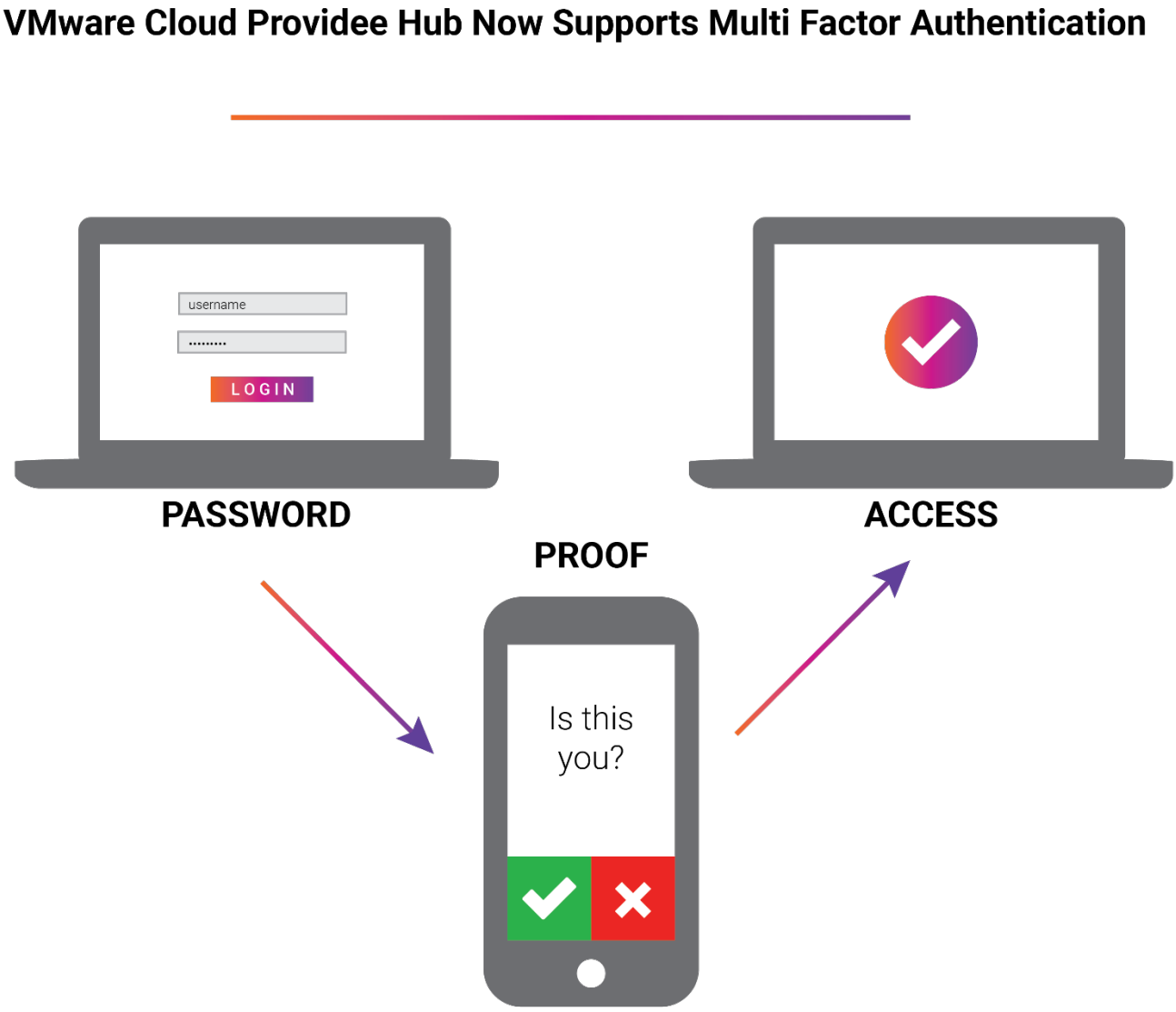
We are using Scanii as a cloud antivirus solution to analyze all the files uploaded or downloaded inside the application.



We have tens of thousands of files (images, videos, documents) that are being transitioned daily by the platform users and administrators. Every file is being scanned on the fly before reaching the servers or the user's computer. If there is any suspicious payload, the transaction is blocked and we get alerted to inspect the file.

Account Creation MFA

Clients can enable an extra layer of security for account creation, by choosing to map each user to a mobile phone.



During recruitment and account signup we can enable mobile pin verification so that we can verify that the member signing up is an actual person and not a bot, and to prevent account fraud. If this is enabled, it will ask the user for their mobile phone number and will ask them to type in the code they receive over SMS.

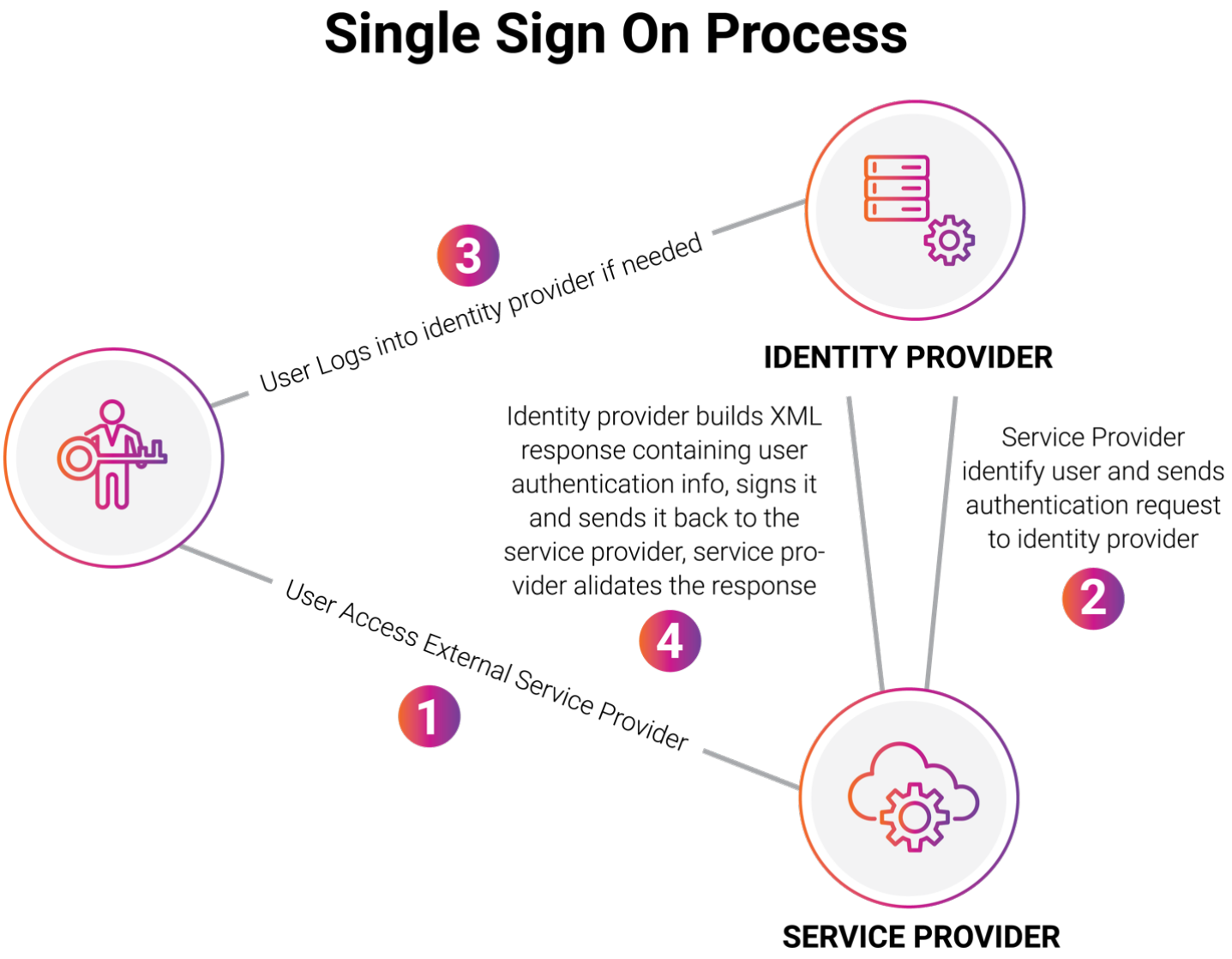
Single Sign-On

Fuel Cycle offers Single Sign-On (SSO) SAML 2.0, with direct integration or via Okta.

SSO increases security and simplifies access because as long as the user is authenticated in a designated 3rd party application, they can access the Community seamlessly without having to log in again. Other benefits include:

- Mitigate risk for access to 3rd-party sites (user passwords not stored or managed externally)

- Reduce password fatigue from different username and password combinations
- Reduce time spent re-entering passwords for the same identity
- Reduce IT costs due to lower number of IT help desk calls about password



IP Filtering

We offer the option of IP filtering by either allowing traffic only from specific IPs (Whitelisting), or only denying traffic from specific IPs (Blacklisting).

Whitelisting is widely used by our clients for protecting their Administration area where they would want to block all IPs except a handful - usually their office IPs.

Blacklisting comes in handy in the Member area where we might want to allow traffic from everyone, minus a few certain IPs that have been flagged as nefarious.

IP Filterting

Blacklist

Reactive

Blocks specific IPs

Lets everything else in

Less secure

Flexible

Whitelist

Proactive

Allows only specific IPs

Blocks everything else

Most secure

restrictive

Data Segregation

For increased data security and segregation, Fuel Cycle application offers a range of role-based account types, depending on the needs of the user. All accounts are created by the client or at the direction of the client.

Account Type	Privileges
Super-Moderator	Usually there is just one Super-Moderator account per client, used at the very beginning as a "parent" account for all the other types. This is the most powerful account type capable of accessing every corner of the application.
Moderator	A role that access to the Fuel Community and Moderation Platform, can create content, members and view member profile data.
Client	Same as Moderator but cannot create content or members.
Member	A role that has access to log into the Fuel Community Platform to participate in the community, but they don't have access to any data or reports.
Read-Only	An extra layer of restrictions that can be combined with other account types.

Data Retention & Destruction

Upon completion of the contract period, the Client can elect to have their data removed from the Fuel Cycle systems. This process will remove all of the panelist data, activity data and survey response

data. The data will be deleted or scrambled in the database, file storage and all copies and backups.

Application Change Management

An application change can be a simple copy update or a 6-months in the work new feature. We categorize the changes according to their scope (Bug, Improvement, New Feature) and to their size or impact on the application (Small, Medium, Large).

All changes falling into the categories below, will follow the Application Change Management Policy where they have to be approved by both the Product Manager and the VP of R&D:

- All New Feature
- Medium & Large Improvement
- Large Bug

The changes are logged and tracked into JIRA and backups are performed before the change is applied. All changes goes through a thorough QA process in Stage and after the change was applied in Production.

Fuel Cycle Contact:
Alireza Soukhakian, VP of Research & Development
asoukhakian@fuelcycle.com
(310) 408-0594