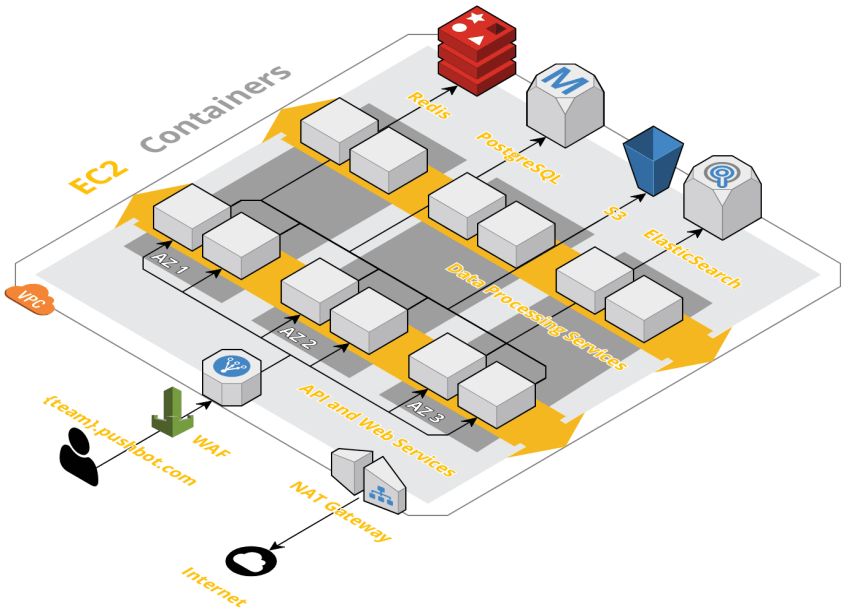
Catalytic Security Guide

Catalytic Security Fundamentals

Catalytic is built for enterprise-level security to protect your users, data, and business processes from threats.

Secure Cloud Platform

Catalytic is a cloud-based enterprise web application, hosted on Amazon Web Services (AWS). The architecture includes multiple layers of security to protect your data.



Certifications & Audits

As of June 30, 2019, Catalytic has achieved successful completion of the following attestation examinations, performed by an independent CPA firm:

- SOC 2 Type 2
- HIPAA

Penetration Testing

On a quarterly basis, a third-party auditor performs penetration tests. Any critical or high severity vulnerabilities are resolved within 7 days.

Encryption
All data is encrypted both in transit and at rest using enterprise-grade security standards. Cryptographic keys are randomly generated by OpenSSL. All data, snapshots, and logs are encrypted when at rest using the AES-256 encryption algorithm. In addition, data is encrypted in transit between services using the transport layer security (TLS) version 1.2 encryption protocol. Encrypted web communications sessions are used for the secure transmission and exchange of ePHI over public networks. Whitelisted IP addresses are utilized to grant access to production systems.

Encrypting data at rest provides a foundational level of security which ensures that the data is useless without the keys needed to decrypt the information. Our master keys are stored in AWS Key Management Service (KMS), and access to decrypt the key material is restricted to only those backend services which need key access via AWS Identity Management Service (IAM).

Database Backups
We have automated backup systems in place to perform scheduled backups and alerting notifications. In addition, offsite storage of backup data is different than production storage. We have automatic failover across three geographically separated data centers in North Virginia. Additionally, customer data is backed up at least daily to AWS data centers in the Oregon region. Restorations of backups are tested quarterly.

AWS has built-in redundancies for backup data as the data is deployed using multiple availability zones and regions. If one availability zone or region were to fail, AWS has built-in redundancy to another zone or region.

Infrastructure Security Standards
References to AWS security in this document have been included based on information from the AWS Security Whitepaper. The IT infrastructure that AWS provides is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1

- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

Infrastructure Auditing
Every deployed application image is saved and can be audited. All changes to our infrastructure are recorded in a read-only audit trail.

Logical Data Separation
With AWS multi-tenant hosting, the data for your Catalytic team is separated from other Catalytic teams by a logical layer. Each Catalytic team has a unique domain name, and in order to access data or perform Catalytic actions for a team, a user must be logged in as a member of that team.

More details on our AWS environment are found below:

	AWS Multi-Tenant Environment
AWS account	Shared, logical separation
Database	Shared, logical separation
Compute	Shared, logical separation
Encryption	Full, in transit & at rest
On-prem connectivity	White-listed IPs
Throughput	10 actions per second
Managed by	Catalytic

Physical Security

Catalytic Offices

Our offices are secured with keycards, automatic locks, alarms and security cameras. All visitors to our offices must be escorted, and we have policies and procedures in place for granting and revoking access to appropriate personnel. We also enforce a clear desk and clear screen policy.

Data Centers

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. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Internal Control Environment

Compliance Team

We have a dedicated Compliance Team that implements and monitors security-related controls, which are based on a security framework that aligns to SOC 2, HIPAA, and GDPR requirements.

Policies and Procedures

We maintain written policies and procedures relating to several key areas, including: Change Management, Asset Management, Workstations, System Access, Risk Assessment, Incident Response, and Disaster Recovery. Our employees also attend Security Awareness Training at least annually (and as a new hire), and all are required to adhere to our Code of Conduct.

Catalytic Internal System Access Controls

The AWS management console uses two-factor authentication that requires a unique user account, password, and mobile token. Furthermore, predefined access groups are

utilized to restrict access based on job responsibility. User access reviews, including privileged users, are performed by Catalytic on a quarterly basis to ensure that security groups and roles are appropriate.

Network Security

HTTPS

Catalytic requires Secure HTTP access (HTTPS) for greater security for communication and data transmissions. HTTPS uses the SSL/TLS protocol, which uses public-key cryptography to prevent eavesdropping, tampering, and forgery.

Restrict Login IP Ranges

Organizations can opt to define trusted IP address ranges that prevent login to Catalytic by users attempting to enter from outside those ranges.

Outbound API Request IP addresses

All outbound API requests from Catalytic actions are made from a static list of IP addresses. Those addresses are:

- 34.239.242.199
- 34.198.36.194
- 34.203.5.188

Secure Network Architecture

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, are established on each managed interface, which manage and enforce the flow of traffic. These policies are automatically pushed using AWS's ACL-Manage tool, to help ensure these managed interfaces enforce the most up-to-date ACLs.

Network Monitoring and Protection

Various tools are utilized to monitor the security and availability of the Catalytic system. These tools collectively monitor access, resource utilization, availability/uptime, and performance metrics from system infrastructure components and endpoints and are configured to send alerts to IT personnel when predefined thresholds are exceeded, or

certain events are triggered. Identified issues are logged in the workflow management system, which is used to manage, record, and track identified system changes.

The cloud hosting services provided by AWS are automatically monitored on a regular basis as part of day-to-do operations, as automated alarms are set to alert our security team of specific events. Our logs record every action within AWS, and we have many event filters for suspicious or high-risk activity.

AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used so personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

Our intrusion detection system (IDS) is utilized to analyze and report network events. The IDS system is configured to alert engineering personnel when certain security events are detected. In the event that a potential or actual security incident is encountered, the engineering team works to identify the cause and remediate the issue as soon as possible. We also have processes in place that would allow us to communicate information related to confirmed security incidents to customers as soon as possible.

Catalytic also maintains a System Status page that customers may access at any time for information and updates about the Catalytic system.

Authenticate Users

Single Sign-On (SSO)

Catalytic has built-in user authentication, but companies also have the option to use an existing SSO capability to simplify and standardize user authentication, including password complexity and 2-factor authentication (2FA). Catalytic supports authentication using SAML 2.0, enabling you to let your users log in to your Catalytic team using their login credentials from an external identity provider, such as Microsoft

Active Directory (AD), Google, and Okta. When SSO is enabled for a Catalytic team, users will be redirected to the identity provider login when they reach the Catalytic login page.

Passwords
User passwords are required to be at least 8 characters long and include at least 3 out of these 4 character types:

- Lowercase letters
- Capital letters
- Numbers
- Symbols

With Single Sign-On enabled, organizations are able to enforce more complex password rules and a password timeout period.

Passwords are hashed with Scrypt which offers strong protection from both brute-force and rainbow table attacks. Passwords themselves are never stored by Catalytic.

Cookies
Catalytic issues a session cookie to record encrypted authentication information for the duration of a specific session. The session cookie does not include the username, password, or any confidential session information.

Session Security
Upon login, a user establishes a session with Catalytic. Session security limits exposure if a user leaves the computer unattended while still logged in. It also limits the risk of internal attacks, such as when one employee tries to use another employee's session. The default session timeout is after 24 hours of inactivity when SSO is enabled or 1 week of inactivity without SSO. Organizations can configure the session timeout period for their Catalytic users.

When the session timeout is reached, users are prompted with a dialog that allows them to log out or continue working. If they don't respond to this prompt, they are logged out. Users can also manually log out at any time.

Data & User Permissions

At the application level, permissions can be configured, including features designed to limit access to processes and data. For example, by marking fields of information 'Highly Confidential,' this will ensure that only pre-approved users can see that data. Groups can also be set, which will give only select users access to certain processes and information. Management of users and their permissions is handled by your company's Admin team member.

Field Level Security

Automation builders can set the level of data permission for each field. Catalytic has 4 levels of data permissions:

- **Public**: Anyone interacting with this automation
- **Internal**: Hidden from non-team members
- **Confidential**: Hidden from everyone except for admins and designated users
- **Highly Confidential**: Hidden from everyone except for designated users

When a user attempts to view information that exceeds their permission level, the sensitive data is redacted and replaced by a CONFIDENTIAL tag. This redaction occurs at the API layer, not the UI layer, for increased security.

Automation Level Security

Automation builders can define the users that can view and interact with automations with 3 levels of permissions:

- **None**: Users at this level cannot view or interact with the automation unless explicitly assigned a task within it
- **Standard**: Users at this level can start the automation and view it in lists and reports.
- **Admin**: Users at this level can do everything Standard users can do, plus these users can edit and configure the automation, as well as change user permissions for the automation.

User Permissions

Catalytic has 4 levels of user permissions:

- **Team Member**: Most users are team members. These users can interact with automations that have been built and view data that has not been explicitly set to be confidential.
- **Builder**: Can do everything a team member can do, plus can create and edit automations.
- **Admin**: Can do everything a builder can do, plus can create additional admin users, manage integrations, and set permissions.
- **Guest**: Can be assigned tasks and complete them, but cannot access other areas of Catalytic or see tasks that are not assigned to them directly. Cannot view any data that is not classified as Public.

Logging

All Catalytic interactions are recorded and logged. This includes login history, navigation, and field updates. Contact help@catalytic.com regarding any suspicious activity that you observed or any concerns that you may have and our team will assist with reviewing logs for your Catalytic account.