Whatfix Security Overview

This white paper provides an overview of key security topics that relate to the Whatfix Platform. The following topics are covered

Drive Digital Adoption

TABLE OF CONTENTS

Functional Overview

Whatfix runs as an overlay on top of the web applications and does not store, process, or record any sensitive data from the application or personal information from the end-users.

For Whatfix to function it only requires element level information which enables Whatfix to identify the element on the page and position the balloon tip on top of the element and a snapshot of the screen for multi-format (slideshow, pdf, video) content.

Web:

Whatfix can be integrated into your application in the following two ways :

- Code Embed: A single line of Javascript that sits in the header of your application. The Javascript calls your Whatfix content after your application has loaded for end-users. (recommended for in-house/homegrown applications)
- Browser Extension: A small plugin that is pushed automatically through IT policy and functions in the same way to call your Whatfix content after your application has loaded for end users. (recommended for third-party applications).

Desktop:

Whatfix Desktop provides three distinct Microsoft Installer (MSI) packages that IT Administrators and end users can use to install the Player application for Windows.
These three MSI packages are fundamentally different - where one is supposed to be used by the end users to install the Player themselves, IT admins can use another to mass deploy the Player, and the third can be used for virtual desktop deployment, etc.

- **User-level installation** (recommended for end-users)
- **System-level distributor** (recommended for IT Admins)
- **System level installation**

Mobile:

Whatfix enables you to integrate the Whatfix Mobile SDK (Software Development Kit) to create in-app experiences for your end users if you have the source code of your mobile app. Once you sign up to Whatfix, you can add your mobile app and easily integrate the Whatfix Mobile SDK for your respective app frameworks. Whatfix Mobile supports the following frameworks,

- **Android**
- **iOS**
- **React Native (Android/iOS)**
- **Xamarin (Android/iOS)**
- **Cordova (Android/iOS)**
- **Ionic**

The Wrapper approach is used to display content on a mobile application when you don't have access to the source code of your native mobile app. This means that you cannot modify the app and integrate Whatfix. With the Wrapper approach, Whatfix enables you to integrate Whatfix with your EAS applications and present it as a mobile app for your end users.

Key Roles in the Platform

Content Creators or Editors have access to create new flows or other guided features to enable higher adoption of Client applications. Their access has to be configured in the Whatfix application console by Whatfix Account Management Team.

End-users of the client application(s) are the consumers of the flows and the users created using Whatfix DAP.
End users are not required to authenticate to the Whatfix Application. The content is served from Cloudflare CDN, based on the predefined actions or events on the Client's application. The end users only need to have access to the Client's application where Whatfix DAP has been deployed.

Whatfix supports the following mechanisms for enabling access for editors to access their Whatfix account

- Via Client's SSO, Whatfix DAP. Supports SAML 2.0.
- In case SSO is not opted for, Password policies can be configured as per the Client's policies.

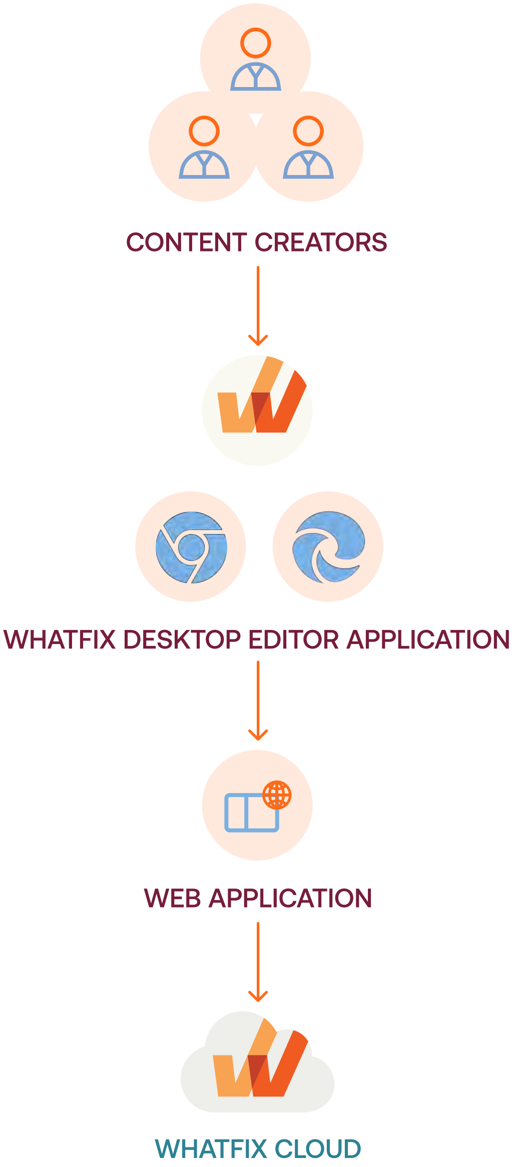
WEB

Whatfix Content Development (Studio)

1. Secure Access via HTTPS
2. Editor extension hosted on Chrome, and Microsoft Edge Web Stores.
3. SSO capability (SAML 2.0)
4. Access Control through privileges
5. Password policy configurations as per enterprise
6. Editor profile data is encrypted

Content Deployment Process Flow

1. Content authoring is done using browser extensions.
2. Available on Google Chrome, and Microsoft Edge (Chromium based)
3. Content is published on Whatfix cloud



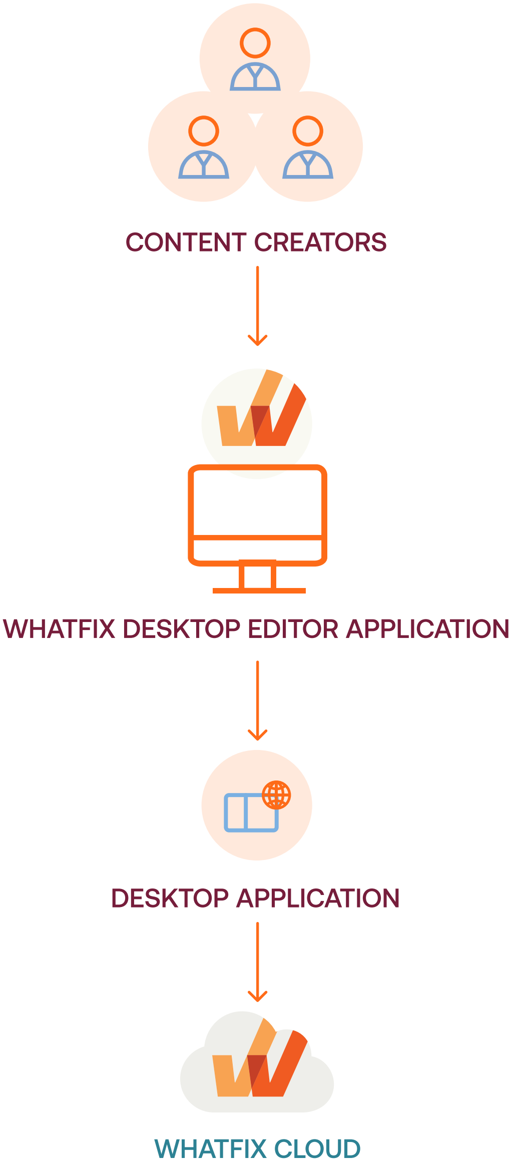
DESKTOP

Whatfix Content Development (Editor)

1. Secure Access via HTTPS
2. Whatfix Desktop Editor
3. Access Control through privileges
4. Password policy configurations as per enterprise
5. Editor profile data is encrypted

Content Deployment Process Flow

1. Content Authoring is done using the Desktop Editor
2. Content is published on the Whatfix cloud

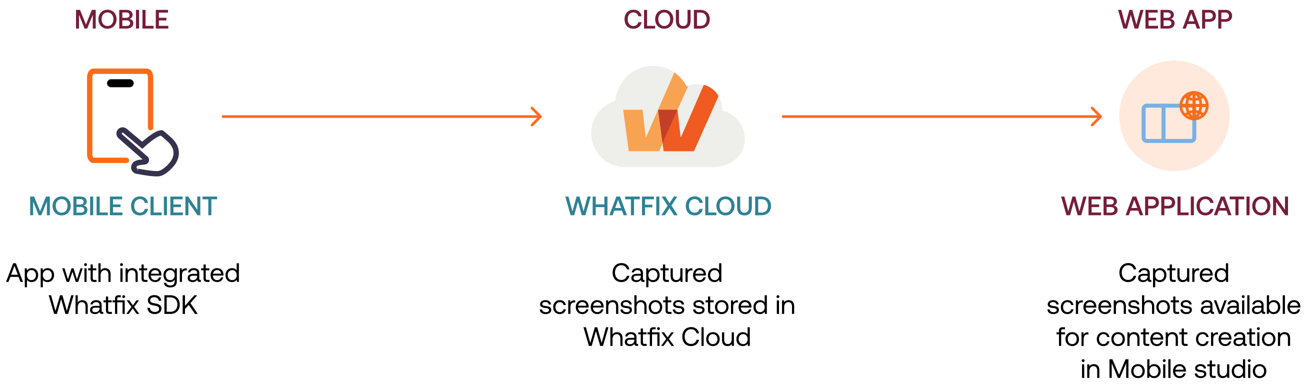


MOBILE

Whatfix Content Development (Mobile)

1. Secure access via HTTPS
2. SSO Capability (Coming soon)
3. Access control through privileges
4. Enterprise password policy

Capture



MOBILE

MOBILE CLIENT

App with integrated Whatfix SDK

CLOUD

WHATFIX CLOUD

Captured screenshots stored in Whatfix Cloud

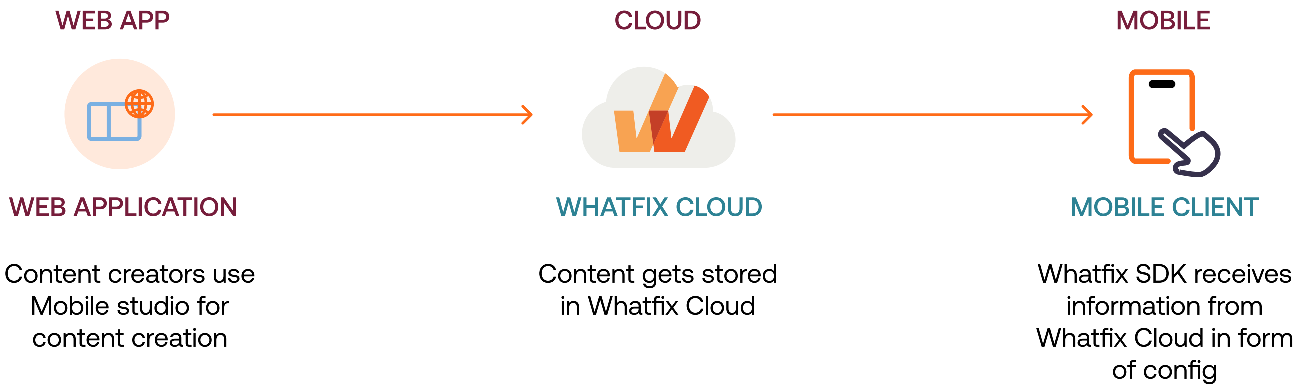
WEB APP

WEB APPLICATION

Captured screenshots available for content creation in Mobile studio

Content Creation and Deployment

1. Content creation is done using mobile device and desktop browsers
2. Mobile device is used to capture the screens
3. Mobile studio is used to create content on top of those screens
4. Mobile studio recommends Google Chrome or Chromium based browsers



WEB APP

WEB APPLICATION

Content creators use Mobile studio for content creation

CLOUD

WHATFIX CLOUD

Content gets stored in Whatfix Cloud

MOBILE

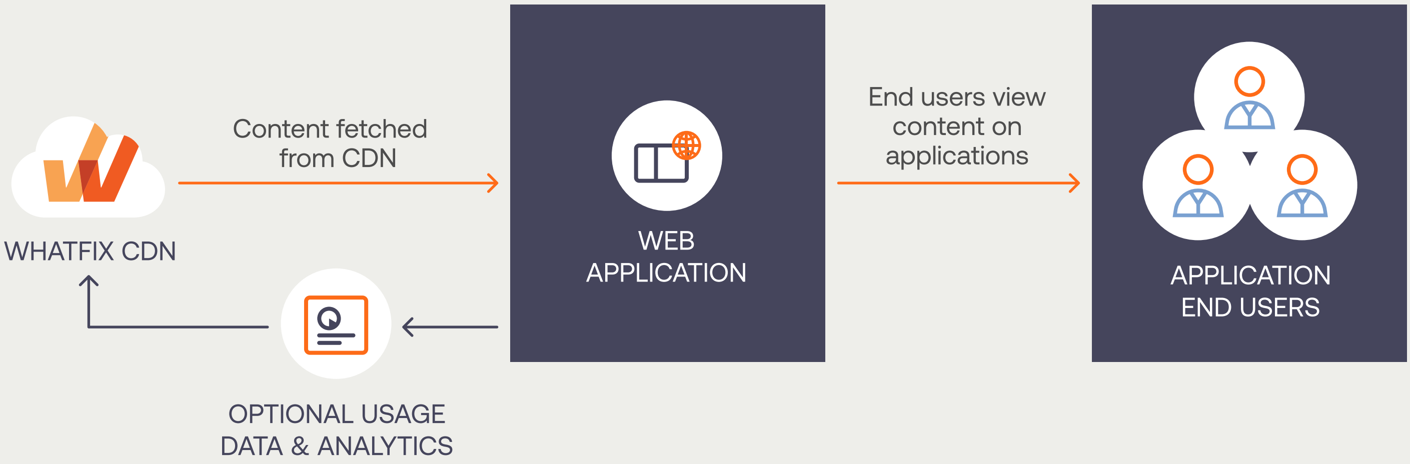
MOBILE CLIENT

Whatfix SDK receives information from Whatfix Cloud in form of config

DEPLOYMENT MODELS

Whatfix Cloud deployment

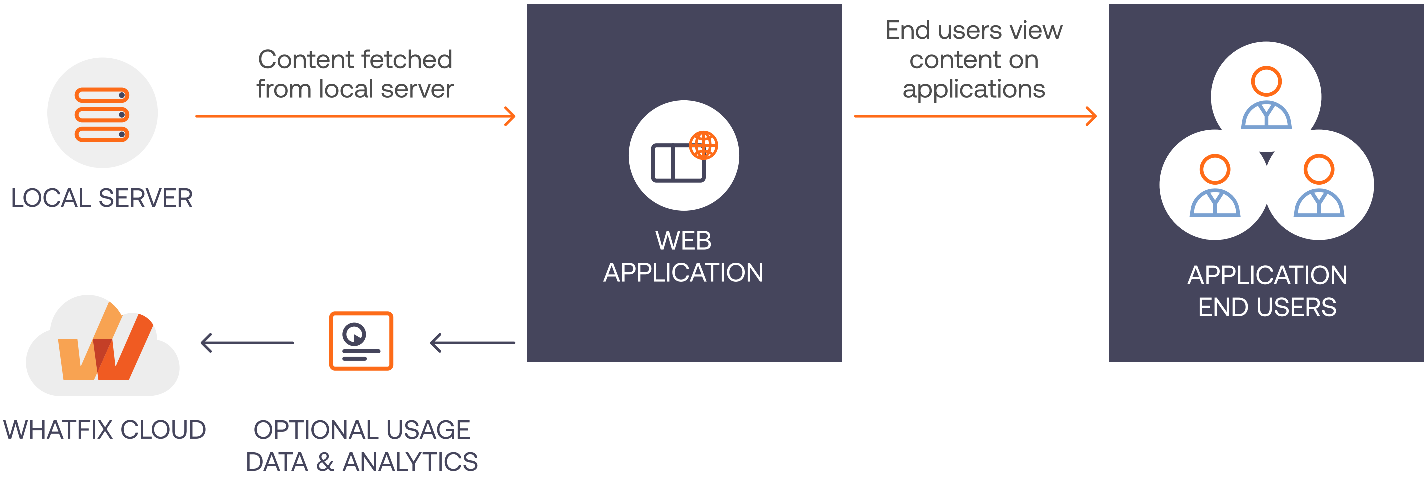
1. Built on ISO27001 & SOC2 compliant data centers
2. Annual third party vulnerability tests of both infrastructure & application
3. DR plans are tested half yearly
4. Secure development practices (OWASP principles, environment separation etc)
5. Periodic backups in keeping with RTO and RPO objectives



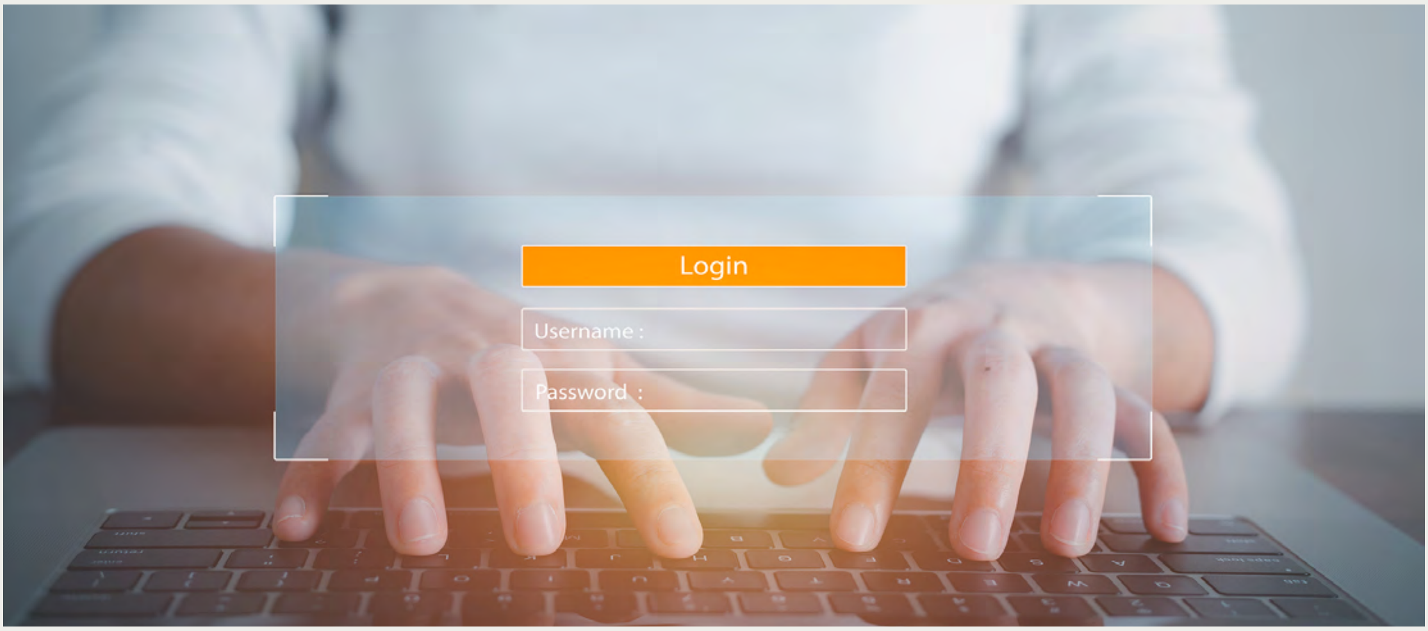
Whatfix Self Hosted Model

Host Whatfix content on your web server/CDN*. No server side software required. No communication with Whatfix cloud. Optional Analytics tracking

1. Contains only static files, any web server/CDN can serve the content
2. Only front-end integration, No server side libraries are required
3. Only GET requests are made to servers hosting Whatfix content
4. No calls are made to any server except your server
5. No third party libraries are used/required to run Whatfix on your application

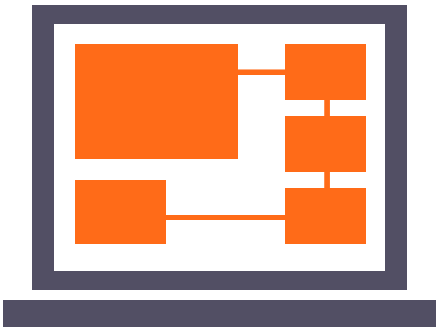

Content fetched from local server
LOCAL SERVER
WEB APPLICATION
End users view content on applications
APPLICATION END USERS
WHATFIX CLOUD
OPTIONAL USAGE DATA & ANALYTICS

PRODUCT SECURITY FEATURES



Whatfix platform allows clients to customise their security controls ranging from Password policies etc. More details on Product security features can be found here

Whatfix Application Flow Architecture



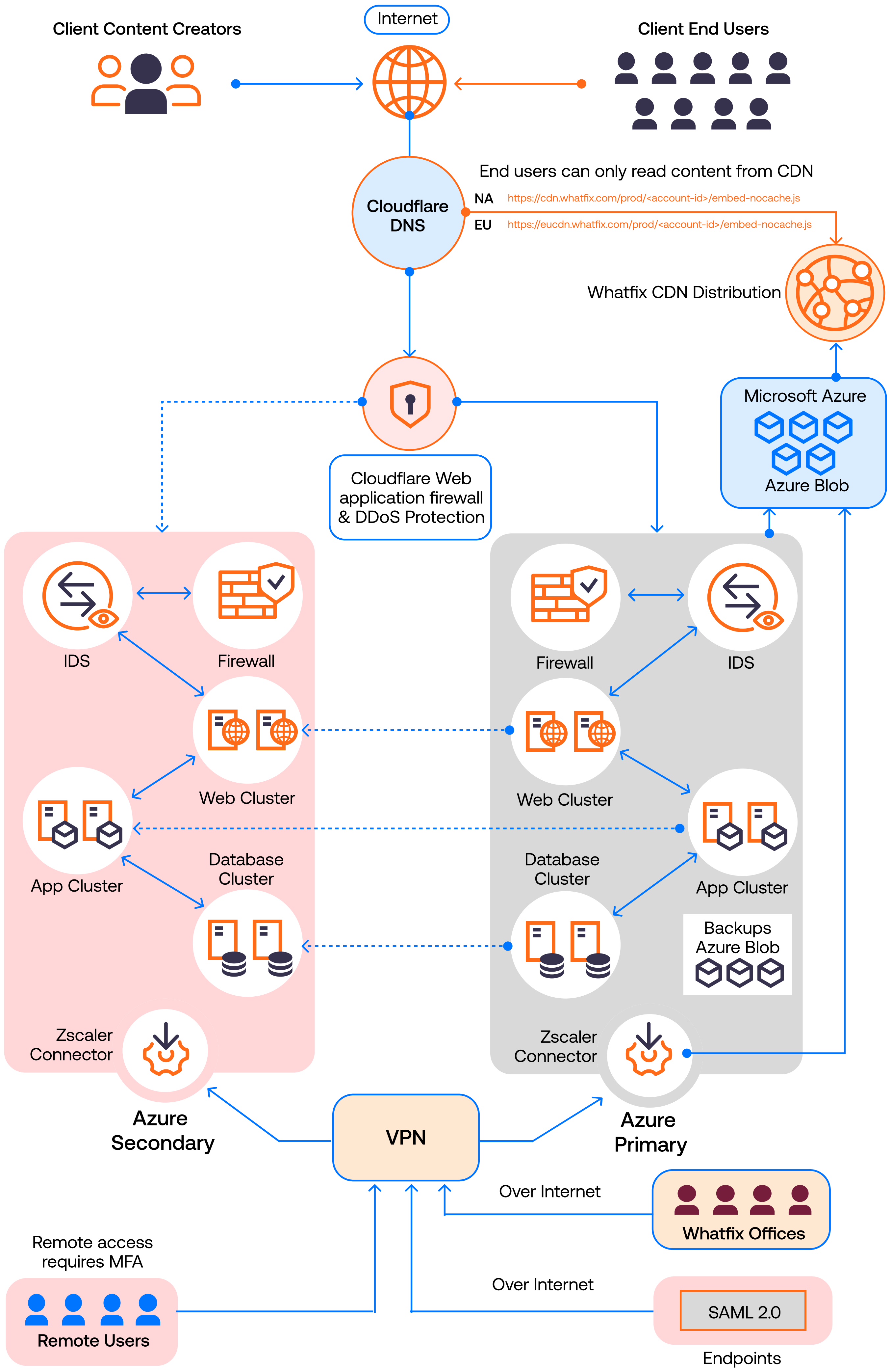
End-user content is served from the nearest Cloudflare Content Delivery Network.

1. Once a Account Manager creates/Modifies a flow using the Whatfix platform, the contents of the account have to be explicitly pushed for deployment by the Account Manager.

2. Once pushed, the Core Application Infrastructure makes an SSH connection to the predefined folder in the Azure blob where the Content needs to be deployed and pushes the content.

3. The Clients can choose to first push the content to their UAT environment of the application for testing before pushing them to the Production Instance of the application.

- Production Infrastructure in Azure (Key Based access) for pushing the Content from the application.
- All other access requires Multi-Factor authentication (Key and OTP)



End users can only read content from CDN

NA https://cdn.whatfix.com/prod/<account-id>/embed-nocache.js

EU https://eucdn.whatfix.com/prod/<account-id>/embed-nocache.js

Data Center

US: Azure

EU: Azure

Workspace Security

1. Access to Work areas are restricted through badge readers.
2. Access is restricted to Whatfix employees and its contractors only.
3. Visitors to Offices have to be always escorted.
4. Surveillance cameras are placed at various strategic point.

Logical Infrastructure Security and Operational Controls

1. Whatfix DAP employs Defense in Depth strategy at both infrastructural as well as Application level.
2. WAFs, Firewalls, Intrusion Detection and Prevention Systems are deployed to strengthen the perimeter security.
3. Every host has EDR implemented.
4. Whatfix production and Development infrastructure are both logically and physically segregated.
5. All changes to production and UAT (including release pushes) are only carried out by DevOps team post explicit approvals from the Quality and Security teams.
6. Access to Production Management plane.
   - is centrally managed and is restricted to the Infrastructure Management Team only.
   - requires Multi-factor Authentication and secure tunneling.
   - All connection to PROD and DEV Environment is through Bastion Host/ Jump Box.
   - Periodic User reviews and certifications to validate only approved personnel have access.
7. Malware protection solutions to detect and respond to latest threats.

LOGGING AND MONITORING

1. Whatfix log management systems ensure that all critical events generated from Systems, Firewalls, IDPS, WAF are all logged and monitored round the clock.
2. SOC runbooks are updated periodically to ensure that remedial actions and escalations are carried out at the earliest and in parallel.
3. Incident response plans and processes are tested periodically to validate their effectiveness and adequacy.

APPLICATION SECURITY

1. Every release goes through elaborate security reviews and tests against OWASP standards and other industry best practices:
    - Automated Code Review,
    - Manual Peer Review,
    - Image certification/Validation
    - White-box Security Testing by the Blue team
    - Post-Release/Deployment Infra and Application assessment.
2. Every developer undergoes a mandatory Security in Coding Training annually

DISASTER RECOVERY

1. The Whatfix product is built on highly resilient infrastructure and architecture.
2. Our infrastructure is built on the principle of high availability and resiliency through Service clustering and redundancies to avoid single points of failure.
3. Whatfix Business continuity program ensures that our Plans are tested at least once annually and upon a significant change in infrastructure.

ENCRYPTION

1. FIPS 140-2 compliant TLS 1.2 encryption (with strong ciphers) for data in transit.
2. AES 256 bit encryption with 2048 bit key-strength for data at Rest
3. Azure key vault for Key management with access to the keys restricted to authorized few individuals.
4. Keys are rotated periodically and upon exit of individuals who had knowledge of the keys

VULNERABILITY DISCLOSURE PROGRAM (VDP) AND 3RD PARTY PENETRATION TESTS

1. Whatfix runs a Vulnerability Disclosure Program (VDP) which is open to anyone to participate.
    - Researchers and testers are provided with relevant access to the Whatfix platform to test the security of both application and infrastructure.
    - These exercises are carried out across the year and all issues identified are reviewed, prioritized, and addressed accordingly.
2. At least once Annually a reputed third party is engaged for carrying out the Infrastructure and Application Penetration test.

PERSONNEL SECURITY

1. Security starts with the people we employ/engage. Our onboarding process for employees and contractors includes the following
    - Mandatory training on Whatfix's Security and compliance practices and policies and acknowledgment
    - Non Disclosure, Confidentiality Agreements, and Acceptable Use Policy
    - Background check on all employees and Contractors
2. Our contracts with all third-party service providers include the requirement of background checks as well as mandatory training and acknowledgment on Information security policies and practices.

Third Party Security Management

1. Whatfix's policies mandate that before engaging any third parties, mandatory due diligence be carried out. This due diligence may include and not limited to

   - Compliance Risk assessments
   - Security Risk Assessments
   - Vulnerability and Penetration tests

2. All third parties must sign Confidentiality agreements and other appropriate Security and Compliance clauses based on the criticality of their services to Whatfix.

3. Periodic audits/ assessments are carried out to validate their compliance to their obligations outlined in their Contracts with Whatfix

CERTIFICATIONS AND ATTESTATIONS

Whatfix complies with all applicable regulations and legislations of Geographies and business verticals it operates and provides services to. Over the past few years, Whatfix has achieved and maintained security certifications for its products and services with industry organizations, frameworks, and standards bodies—creating assurances and safeguards that support customer requirements. Our certifications include:

HIPAA COMPLIANT

CLOUD COMPUTING COMPLIANCE CONTROLS CATALOGUE C5

AICPA SOC — SOC 2 TYPE II CERTIFIED

TISAX RESULT AVAILABLE

bsi ISO/IEC 27001 Privacy Information Management CERTIFIED

bsi ISO/IEC 27001 Personal Data in the Cloud CERTIFIED

bsi CSA STAR Cloud Security CERTIFIED

bsi ISO/IEC 27001 Information Security Management CERTIFIED

GDPR READY

CCPA READY

CYBER ESSENTIALS

This document is for informational purposes only. No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of Whatfix., except as otherwise permitted by law. Prior to publication, reasonable effort was made to validate this information.

For any questions: Contact: Infosec@Whatfix.com