Service Definition

Contents

Service Definition

Onfido's identity verification Platform ("Platform") is a cloud-hosted solution that combines various signals to assess whether an applicant is in fact the person they claim to be. The Onfido Platform uses identity documents from across the world as a primary source of identity, and compares them to a digital capture of the applicant in either a photo or a video. The Platform can be quickly integrated into clients' apps or websites, allowing developers to easily add identity verification services.

We verify identity using two product lines that work together in one solution:

1. **Document Verification**
   Verification that a document is genuine, and extraction of data on that document; and

2. **Biometric Verification**
   Verification that the face is genuine (not a mask or picture of a screen) and that it matches the face on the document. Biometric Verification comes in 2 variants: selfie liveness (photo submission) and facial video liveness (video submission / "liveness").

Document Verification
Submission of a government-issued document gives us confidence in the applicant's legal identity. We support a global set of documents (4600+ versions) to ensure we maintain high applicant pass rates. Please check https://onfido.com/supported-documents/ for detailed document coverage per country. The document check performs 2 fundamental tasks:

1. Capture, classification, and extraction of data on the document; and
2. Assessment of whether the document is fraudulent or genuine.

We offer fully automated and fully manual document check configurations, as well as a hybrid combination of the two to map to different client requirements and use cases. Additional extraction options can be applied to the document check.

Biometric Verification
Our biometric verification solution protects against impersonation. It's the most robust way of making sure that the person submitting the documents is the rightful owner of those documents, and that they are actually present. There are two options for biometric (facial) verification:

1. **Facial Verification with Selfie Liveness:**
   We extract the profile photo and data from an ID document using machine learning and then compare them to a selfie taken by the user; and

2. **Facial Verification with Facial Video Liveness:**
   In addition to checking if a user's face matches their ID document, this check ensures the user is a live person. The user records themselves performing multiple challenges. They might need to read aloud randomly generated 3-digit sequences or perform simple head movements. These challenges foil even the most advanced fraud techniques, including pre-recorded videos, 2D masks, and 3D masks.

Data Collection Method

The Onfido Platform collects applicant data through two main methods, depending on client preference:

1. SDK
2. API

SDK

Clients can integrate our SDKs into the front-end of their end user-facing applications, in order to allow applicants to start a journey on a mobile app or Web browser, to use their mobile device to capture identity documents and facial photographs / video, and if necessary to complete the submission in the browser. (Onfido offers 'mobile' SDKs for iOS and Android, as well as a Web SDK). The Onfido technical documentation is available on https://developers.onfido.com.

API

The client provides the applicant's personal data and collected images via calls to REST API endpoints. (APIs are also used to provide identity verification check results back to clients.)

Design of the Hosting Environment

Data is processed and stored on AWS servers in the EU, the United States, and Canada. The three instances of the Onfido Platform, namely "EU", "US" and "Canada", are deployed within different AWS regions (eu-west-1, us-east-1 and ca-central-1 respectively). As part of any implementation, Onfido works with the client to select the appropriate AWS region to meet non-functional requirements. AWS regions provide the ability to deploy the Onfido Platform in geographical proximity to clients and applicants, while meeting any necessary data residency regulations.

Each region consists of multiple Availability Zones with separate physical security, power and cooling, and network connectivity, connected with low-latency links to the other Availability Zones in the region. Within a region, each Availability Zone is an independent data centre, and common points of failure such as generators and cooling equipment are therefore not shared between Availability Zones. Availability Zones are designed and situated such that even extremely uncommon disasters

such as fires, tornadoes or flooding should only affect a single Availability Zone. The Onfido Platform is deployed across multiple Availability Zones per region to provide both Disaster Recovery (DR) and High Availability (HA) automatic failover.

Implementing the Onfido Platform

With guidance from Onfido, clients are responsible for identifying and selecting which regional instance(s) of the Onfido Platform best match their requirements. Onfido's Platform instances are currently hosted in the AWS EU, US and Canada regions, in order to support nonfunctional client requirements such as data and service localisation.

Clients are responsible for using the provided onboarding assistance and guidance materials to perform the integration of the Onfido Platform into client applications.

Clients are also responsible for performing appropriate acceptance testing of the Onfido Platform using the sandbox environment provided. However Onfido will also provide the client with reasonable, limited assistance and guidance with the integration.

Onfido is responsible for creating the client's account(s) within the Onfido's Platform. This includes the enablement and initial login details for the Onfido Dashboard.

Providing Support for Clients

Onfido client support managers and support teams are available to clients to provide ad hoc support or discuss alterations to the services provided.

Clients should request new features or functionality from customer success managers, who will then liaise with the relevant product owner and others as required to investigate the feasibility of the feature. Implementation of the new feature or functionality will depend on the existing development roadmap and strategic priorities.

System Operations

Network Security

Hosting Environment

The network is configured in different layers. AWS security groups are used to restrict traffic between the infrastructure layers using Terraform. On each server, security group ports and protocols are disabled by default, and AWS has native firewalls, the rulesets of which are set to auto-update. The firewalls are only open from whitelisted Onfido IP addresses.

Infrastructure, operating system and application logs are collated using a cloud SIEM solution (Splunk). These logs are utilised by Onfido for capacity and performance monitoring, basic security monitoring, and Onfido Platform application support. AWS GuardDuty threat detection also performs security event monitoring at the infrastructure layer and alerts the Security and DevOps teams for response as appropriate. AWS CloudWatch monitors AWS activity and security settings and produces alerts to the Security Team for deviations from configured CIS Benchmarks. AWS Inspector performs security assessments on a regular basis to help Onfido assess for unintended network accessibility, vulnerabilities and deviations from best practices of our AWS instances, in order for the Security team to remediate them.

Servers are deployed with custom CoreOS hardened images. A penetration test of the hosting environment is performed at least annually. Security updates are automatically applied on AWS, and the DevOps team periodically reviews to ensure that infrastructure patch versions are up-to-date.

Vulnerability and Penetration Testing

Onfido performs annual penetration testing of the Onfido Platform deployed in the hosting environment. All code deployments are scanned for vulnerable dependencies using automated vulnerability scanning tools. Clients also perform occasional vulnerability scans and share the results with Onfido.

Availability

To facilitate capacity management and disaster recovery, virtualisation is used whenever possible. The hosting environment is deployed in AWS Public Cloud.

Hosting Environment

AWS's infrastructure logs, operating system logs, and application logs are aggregated into Splunk and DataDog. Alerts have been configured for both infrastructure and the application. Kubernetes application containers are deployed to a cluster of servers managed by an AWS auto-scaling group, so capacity is added or removed in response to increases and decreases in demand. Where auto-scaling is not possible - such as databases - saturation of CPU, memory and disk usage is monitored to identify the need to upgrade with a target of 60 days lead time. Onfido leverages AWS Route 53 and Shield for DDOS protection. The types of common DDOS attacks mitigated by these tools include Volumetric and Application layer DDOS. The API availability target is 99.5%, 24 hours a day, 7 days a week, 365 days per year.

Business Continuity

Business continuity and disaster recovery plans have been documented and are reviewed and tested at least annually. The plans include an incident communications procedure and emergency response plans for key scenarios such as office evacuations and data centre failures.

Backup and Recovery:

Platform

The EU Onfido Platform application containers are deployed and mirrored across three Availability Zones within the eu-west-1 AWS region in Ireland. The US Onfido Platform application containers are also deployed and mirrored across three Availability Zones within the us-east-1 region in North Virginia, and the Canada Onfido Platform application containers are similarly deployed and mirrored across three Availability Zones within the AWS Canada region (ca-central-1). Each Availability Zone resides in a physically separated data centre with low-latency links. Common points of failures like generators and cooling equipment are not shared across Availability Zones. Automated mechanisms manage failover of services between zones within the region. A snapshot of running applications is taken daily by the Heptio Velero tool, with snapshots replicated across multiple Availability Zones. These production environment snapshots are retained for the past 10 days. Application image versions are stored in an AWS hosted image registry; this is backed- up by S3 and therefore automatically replicated across multiple Availability Zones. To restore the Platform, a snapshot can be referenced, and the relevant application images redeployed.

Recovery

Systems have a defined internal Recovery Time Objective (RTO) and Recovery Point Objective (RPO), which informs the backup and recovery strategy for each system, in line with contractual, regulatory, and operational requirements. Backup monitoring is performed by the DevOps team ensuring that backups are verified for successful completion. Backups are tested periodically as part of business continuity testing and via periodic restore activities upon request or as part of incident recovery. Onfido can restore databases to any point in time with 5 minutes' accuracy within the last 35 days and monthly for the last 12 months.

Data Deletion

Clients are able to manage deletion of data through configured retention periods or on a per-applicant basis through self-service, using either the Onfido Dashboard or Deletion API. Unless a custom schedule is contractually agreed with the client, deletion of such personal data occurs after a standard time window of 30 days from the deletion request; during this time window, the deletion request can be cancelled if required for any reason.

Data deleted in this way is hard deleted and is therefore not recoverable. AWS securely wipes data using techniques detailed in the NIST SP 800-53 framework, and securely decommissions hardware using techniques detailed in the NIST 800-88 framework. Refer to AWS SOC2 report for controls relating to irrecoverability of data once deleted in AWS and secure decommissioning of hardware.