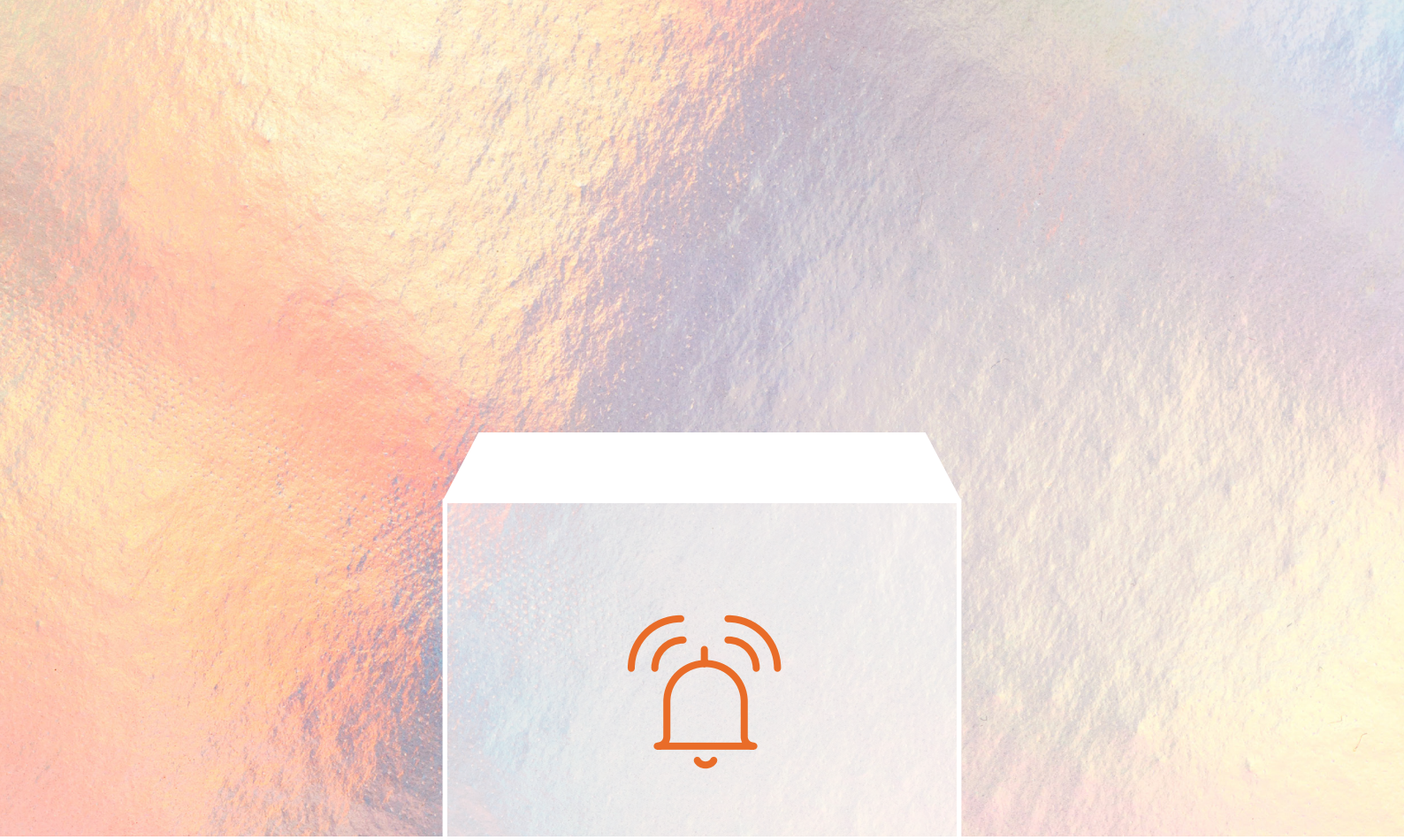
EYEON id

Privacy matters

EyeonID API

Full description – from how the service works to implementation



Proactive monitoring

The core of EyeonID's service is our proactive monitoring service. Our alerting and monitoring service, constantly identifies, collects and evaluates massive amounts of data from all corners of the web, including deep web and darknet. The data is collected and analyzed automatically and manually, to determine if the information is in any potentially dangerous context and to what degree.

By using our proprietary technology, based on 3rd generation NLP (natural language processing) and AI, we add an extra qualitative layer to the automated process and evaluation of the harvested data. In practice this means that our technology can understand and determine the context of the data in a much better way.

Customization possibilities

Brief technical information

Our RESTful API is divided into multiple segments, each catering for its specific role and responsibilities. Our API is secured with OAuth 2.0 and we monitor and assess the API continuously in order to live up the highest security standards.

Full control of the customer journey

If you implement the EyeonID API, you will be able to decide how you would like to provide the customer journey and user interactions. The responses through the API gives you more flexibility to configure, interpret and present to your customers or implement into your customer security systems, KYC processes or risk management.

Monitoring service

When subscribing to the API, you will be able to select:

1) What credentials to include in the monitoring service
2) Number of credentials or adapted to different packaging and subscriptions

Packaging and features

Packaging and features

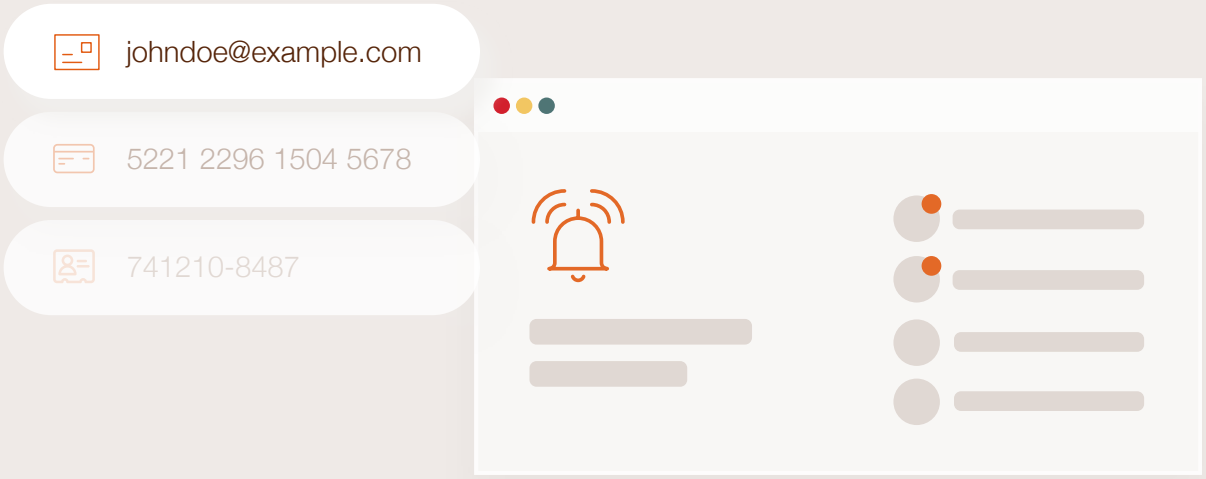
What endpoints that will be accessable within the partnership is decided in the commercial discussion.

Localy adapted

The API responses can be provided in your local language. You use a coutry code for some credentials as well as partnership setup.

Customer (end-user) onboarding

As you provide the onboarding of the customer, you can provide the service in the environment you see fit.
Creating and managing a customer account is handled within the API.



Monitoring service

The monitoring service provides the option to add credentials that should be monitored, such as e-mail, personal identification number or credit card to name a few options. All entered data will instantly be anonymized on EyeonID's side.

Adding a credential

Firstly, customers and unique credentials needs to be verified. When adding a credential for monitoring, the following information is sent in together with a reference token.

1) Type of credential
2) Nickname of the credential (Optional)

Respons

We respond with a masked value of the credential and a response on the verification.

Credentials

The monitoring of credentials is the core function of EyeonID API. The API allows you to fully customize in terms of what types and how many that you and your customers should be able to monitor. For some of the local credentials, you use a Country Code. We offer the following types of credentials:

- Credit card number
- ID – Identification number such as personal code or SSN
- E-mail
- Phone number
- Passport number
- IBAN number

You will be able to display the number of credentials and types connected to the subscription for the end user.

Alarms

When we find a match to the credential and a threat is detected we generate an alert immediately.

The alarms provided can be delivered as either e-mail or by text message. We can either push the alert for you to use your domain as the sender of the e-mail or the text, or provide that service. The alarms primary communication should highlight that a match is found and they should take action.

Alarm Example

- Your name of the service
- Alarm that something has happened
- Call to action to log in into the environment or access the details

Alarms – Risk level

The APIs function for the alarms supports information about the breach, when it happened, what credentials we have found in the breach, what risk we deem the exposed information will have for the user and the appropriate actions to take in light of this information.

- The risk level of the breach.
- Actions for you to take (recommendations).
- Details about the breach.
- Date surrounding the breach.
- Information surrounding the context of how we found the credential.

The alarms are divided into three different levels, reflecting the risk of the breach itself as well as what actions to take related to the specific credential and the risk of the breach.

Low risk	No immediate action is needed but we want to make you aware of the situation.
Medium risk	Action is required as we have found the credential in what we regard as a suspicious and potentially dangerous context.
High risk	Immediate action is needed as we have found the credential in what we regard as a highly suspicious and dangerous context.

Customer Management

The API gives you the full control to manage the customer lifecycle, from creating new customers, subscription management, updating and deletion.

Create customer

An end user is created with a unique external customer ID, not identifiable from EyeonID's end together with information regarding the subscription and e-mail when verification is required.

Subscription

The subscription holds the information on what the customers can access. Subscription activation or deactivation is managed and can be updated with a simple request.

Deletion

When an end user no longer should be valid, a request for deletion is sent.

In addition to the monitoring and alerting service, the API supports additional features for you to provide to the end users or implement as you see fit.

Features are unique additions to the core service that add interaction and customer value by strengthen the knowledge of the customers, keep them informed and strives to lower the users risk exposure.

- Password check
- Risk profile score & surveys
- Knowledge base
- Activity report

Password check

With our Password check the user can check existing passwords against a database of millions of previously stolen and leaked passwords. By doing this the user can avoid choosing already compromised passwords and they can also test their current passwords and get recommendations on what they could do to improve them.

How it works

The password is sent in through the API. The response includes a general analysis and a risk level.

Risk level is set depending on how much exposure it has had: None, Low, Medium, High, Critical.

Together with the risk, we provide a number of suggested recommendations on how to improve the password management and mitigate the risk.

General analysis

Additionally, we provide some actionable tips on what is wrong with the password and why it can be considered a weak password. The reason could be that it lack: a digit, an uppercase letter, a lowercase letter, a symbol or just are too short.

The password check respond with

- Instant feedback on how strong the password is
- Information if the password has been part of a previous leak or not
- Recommendations on how to improve the password

Activity report

A personalized monthly report that you can generate and push to your end users. The report summarizes the main events and actions that have taken place in the last month. Our activity report aims to drive engagement and increase awareness.

Number of read issues

This tells the customer how many issues (alerts) the customer has received that have been read.

Number of unread issues

This tells the customer how many issues (alerts) the customer has received that have not been read.

Total number of issues

This tells the customer how many issues (alerts) the customer has received in total.

Generate the report

You fetch the report through the API by sending in a start date and an end date for a summary of the period.

Knowledge base & FAQ

Our knowledge base and FAQ is another side of our proactive approach to cybercrime. In this section you will find extensive information about ID theft and other online frauds. As knowledge is key in protecting yourself against cybercrime, this is a valuable proactive measure

By providing examples, explanations and descriptions, the users will also have the opportunity to fully understand and learn the context surrounding security buzzwords and computer jargon related to ID theft, as well as to assess the risks of specific online behaviors.

How it works

Possibility to create a page with a knowledge base & FAQ for the customers by retrieving: Articles & featured articles FAQ & featured FAQ, dictionary to explain common words and phrases related to the subject. Pick and choose what you would like to display and mix with the content of what you find is relevant.

Articles, FAQ & Search function

Retrieve article by name and content together with a short summary.
Featured articles can be fetched together with the article.

Risk profile score & surveys

Risk profile score is a compiled assessment of the user´s behavior, knowledge and safety online, and is determined by several factors. It will guide the user towards a better understanding of their risks of being exposed to ID theft.

Today we have created generic surveys with results and recommendations depending on the answers. With the feature, we have the possibility to create additional surveys, something that is be agreed upon in the commercial discussion.

If a user is unaware of all the potential risks when using internet services, the risk of becoming a victim will increase over time.

How it works

You can get the surveys connected to you partnership as you like, all at once for you to display or single surveys separately.

Responses

Within the API, you get back the title of the survey, the questions, possible answers to the questions, advice and actions to take depending on the answer risk score.

When a survey is completed, you can retrieve the average score the customer received to give the customer a risk score. This can be used in order to reflect for the customers their risk exposure of their behavior.

Setup

The setup of the API is dependant on your useage of the service and where you aim to implement the service. You are able to integrate the API in excisting customer environments, create a new app or send requests to the API.

Things you should prepare on your end:

- Branding material
- Customer environment to access the service (Mypages, App)
- Sales process
- Pricing and product information of the packaging
- Customer relationship – Billing, account lifecycle management and customer service in terms of general questions about the service

We always have a tight collaboration with our partners in the setup process and we always also provide a Project Manager from our end. During the commercial discussions, we also scope what actions such as marketing and content creation outside of the technical implementation needs to be created.

Security, Compliance and SLA

We treat the security and compliance with the uttermost respect.

Here are some of the measures we have taken to fulfill this:

- OAuth 2.0
- PCI/DSS compliant
- No personal data is stored
- (Of course) GDPR compliant
- High committed service uptime
- 2nd line support availability
- Support management and processing of support ticket availability
- Integration, implementation and launch support

Internally, we perform penetration testing as well as other types of testing regularly. On a regular occasion we also do testing together with third party security firms to confirm our security.

Code scanning and infra scanning is performed constantly in order to meet the highest standards.

System access and staff management is strict and reviewed regularly.

Implementation process (high-level)

- Scope the set-up and onboarding
- Get full API documentation
- Integration and testing period with support

API implementation

Before the implementation process starts, we always want to secure alignment through meetings to make sure that all involved understand what is expected from both parties to make the launch successful. This generally includes egagement from marketing and IT/development from your side.

Request our full API documentation by reaching out to us.

EYEON id

Eyeonid Group AB (publ)
Blasieholmsgatan 4 4TR
11148 Stockholm

sales@eyeonid.com
www.eyeonid.com
Org. nr. 559005-9415