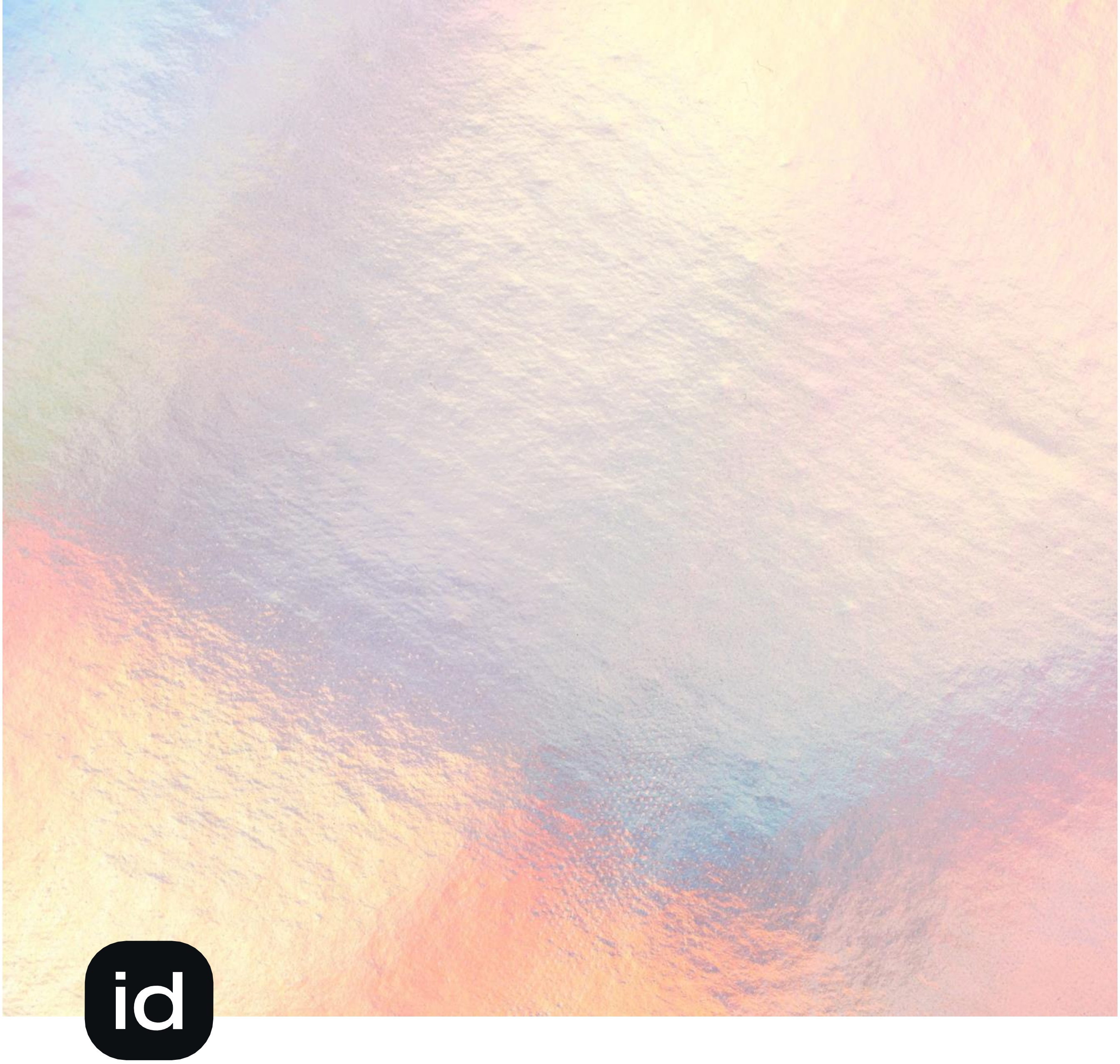
EYEON id

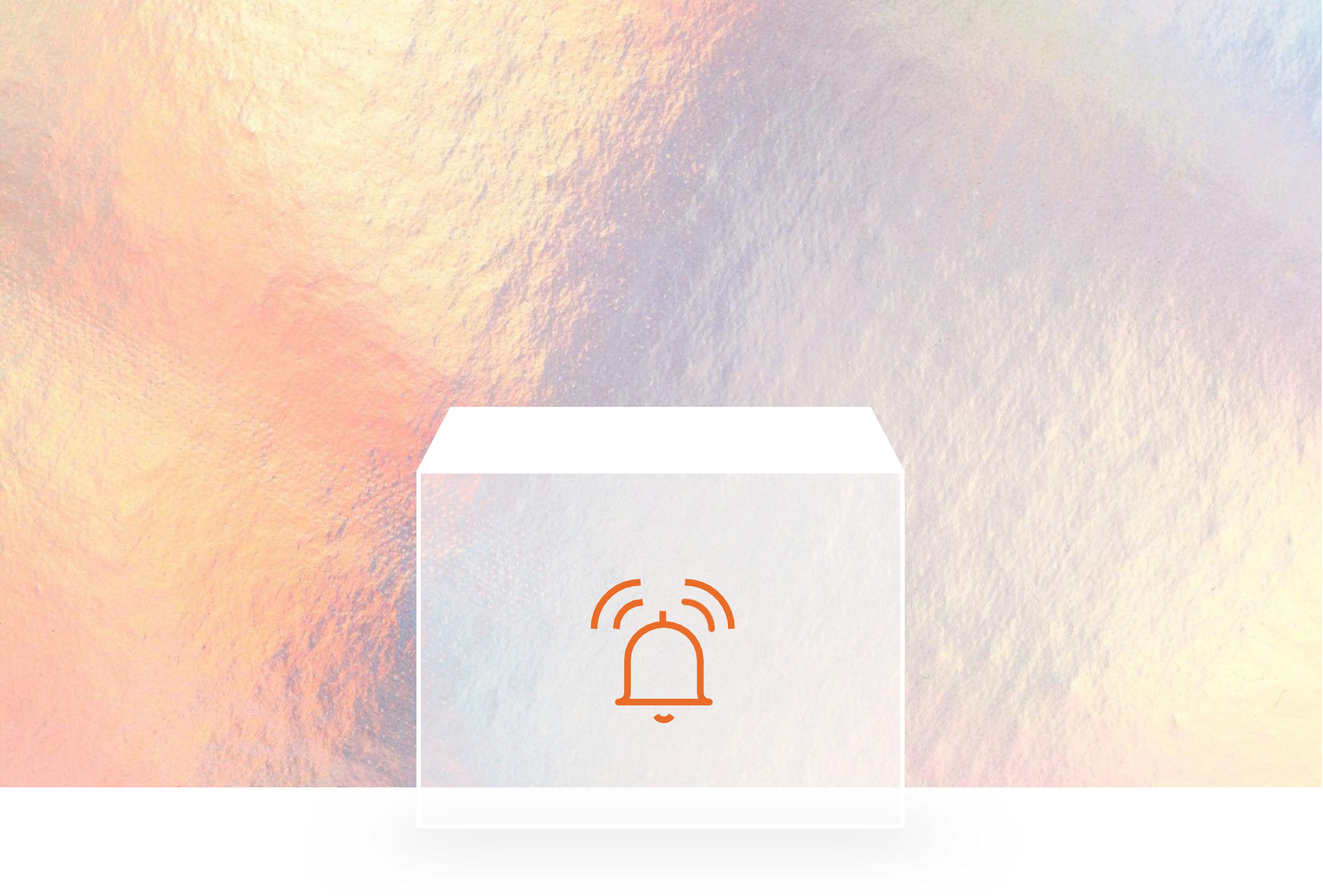
Privacy matters



id

EyeonID

Service description



Proactive monitoring

The core of EyeonID's products 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 analysed automatically and manually, to determine if the information has ended up 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 found data in a much better way.

Customisation possibilities

Brief technical description

Our RESTful API is divided into multiple segments, each catering to specific tasks and responsibility areas. Furthermore, the API is assessed and monitored continuously to make sure that it lives up to the highest security standards.

Full control of the customer journey

The EyeonID API will give you the liberty to freely decide how you want to implement the customer journey and user interactions. The API will also give you more freedom to configure how the data is presented to the end-customer and how it is implemented into your security system, KYC processes and/or risk management.

Monitoring service

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

1) What assets to include in the monitoring service

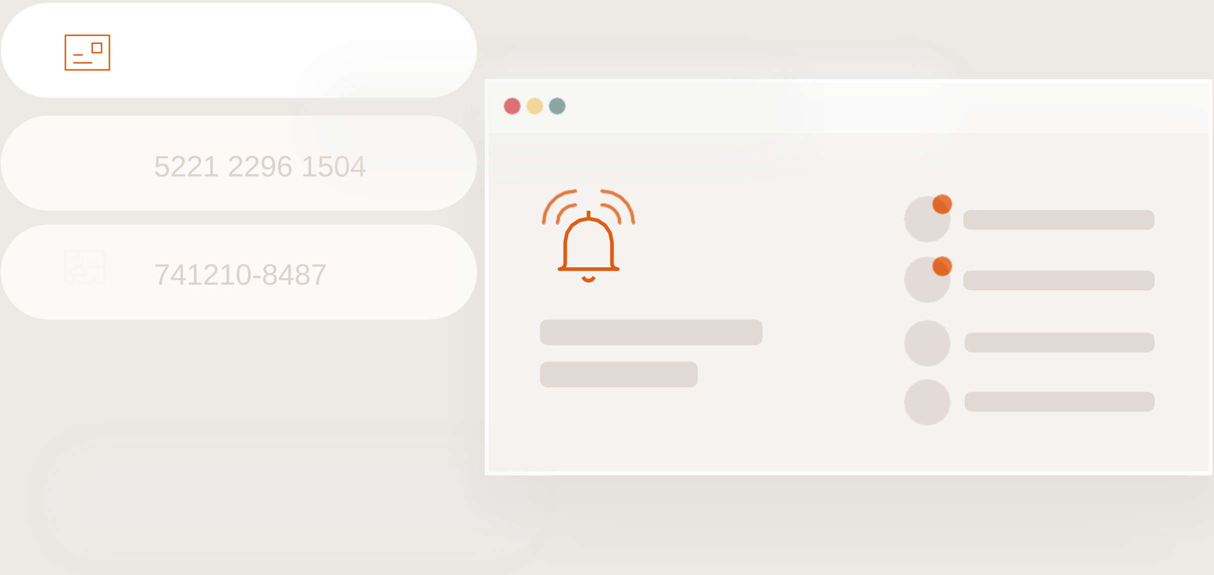
2) Packaging and features

Packaging and features

Note! What endpoints that will be accessible within the partnership will be decided in a separate commercial discussion with EyeonID.

Customer onboarding

As you provide the onboarding of the customer, you can implement the service in the environment you see fit.



Monitoring service

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

Adding an asse

Some unique assets need to be verified when added (e.g., e-mail, and phone number) due to security aspects. When adding an asset for monitoring, the following information is sent together with a reference token.

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

Response

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

```
;”johndoe@example.com”,”
{”_index”:
:542”,””_s
s4534s”,”email”;”johndoe@example.com”,”firstname”:”John”,”lastname”:”Do
e”,”avatar”:”https://fbcdn-profile-a.example.com/profile-ak-
ash3/41688_100000276001053201512303 2_n.jpg”,”id”:542,”created_utc_times
tamp”:”2013-12-09”,”18:51:50”,”modified_utc_timestamp”:”2020-01-22”
```

Credentials

The monitoring of credentials is the core function of the EyeonID API. The API allows full customization when it comes to what type of assets you want to monitor and how many. 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.

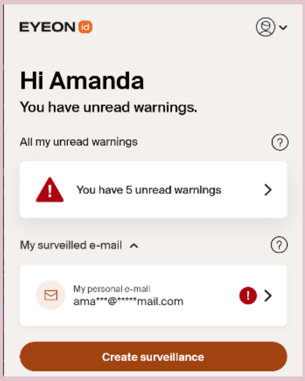
Alarms

When we find a match for the monitored credential and a threat is detected we generate and alert immediately and send it to the users registered email and/or phone number by text message.

The alarms provided can be delivered by email, text message or both. You can either choose to push the alert via your own domain or EyeonID's. The alarms' primary function is to highlight that a match has been found for a given monitored credential and that the user needs to act (e.g., login to the service to learn more).

Alarm Example

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



EYEON id

Hi Amanda

You have unread warnings.

All my unread warnings

You have 5 unread warnings

My surveilled e-mail

My personal e-mail
ama***@*****mail.com

Create surveillance

Alarms – Risk level

The alarms generated by the API can show the following information about the breach:

- General information about the breach.
- When the breach happened.
- When the breach first became public.
- What credentials was found in the breach.
- The estimated risk level of the breach.
- What actions we recommend the user to take.

The alarms come in three different risk-levels (low, medium, high), which reflect the estimated risk of the breach itself. The actions we recommend to the user are specific to the monitored credential found and the estimated risk-level of the breach that the credential was found in.

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 full control to manage the customer lifecycle. This includes:

Creating new customer ID's

An end user is created with a unique external customer ID – which is not identifiable from EyeonID's end.

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 of accounts

When an account no longer is valid, a request for deletion is sent automatically.

In addition to the monitoring and alerting service, the API supports the possibility to add additional features that can be implemented as you see fit.

The additional features strive to increase the end-user's interaction with the service, expand their knowledge horizon and lower potential risk behaviour. These additional features are available as of today:

- Password check
- Risk profile score & surveys
- 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. Our password check also gives the user the opportunity to test their current passwords and get recommendations on how 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 several recommendations on how to improve the password management and mitigate the risk.

General analysis

Additionally, we provide the user with the possibility to check their passwords general security level, as well as provide tips on how to improve them (if needed). E.g., that the password needs to be longer, that it needs to include both lower and uppercase letters etc.

The password check has the following functions:

- Inform the user if the password has been leaked.
- Inform the user about the password's general security level.
- Give the user 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. The activity report includes the following information:

Number of read issues

Informs the customer about how many issues (alerts) they have received and how many of them they have read.

Number of unread issues

Informs the customer about how many issues (alerts) they have received and how many of them that they have not read.

Total number of issues

Informs the customer how many issues (alerts) they have received in total.

Generate the report

You fetch the report through the API by providing a start date and an end date for a selected period.

Risk profile score & surveys

Risk profile score is a compiled assessment of the user´s behaviour, 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.

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 potential risks when using internet services, the risk of becoming a victim will increase over time.

How it works

We can deliver the surveys as you see fit. Either in their entirety to be displayed all at once, or as separate surveys.

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 resulting 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 to give the end user a better understanding of their overall risk exposure and draw their attention to potential risky online behaviour or habits.

Setup

Your technical setup is dependent on your usage of the service and where you aim to implement the service. You can integrate the API in existing 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 aim to have a tight collaboration with our partners in the setup process, which includes us providing a dedicated project manager. During the commercial discussions we also advice on recommended activities for better chances of commercial success, which includes recommendations on marketing activities and content creation.

Security, Compliance and SLA

We treat security and compliance with the uttermost respect.

Here are some of the measures we have taken to fulfil 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 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 engagement from marketing and IT/development from your side.

Eyeonid Group AB (publ)
Sibyllegatan 81
11443 Stockholm

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