FAQs for SaaS PoC

What SaaS application connectors are supported by Borneo?

Borneo support 10 SaaS connectors: Slack, Jira, Confluence, Github, Gmail, GDrive, Salesforce, Zendesk, Zoom, Splunk(beta). Lets us know if you require any new connectors and we can prioritize them on our roadmap.

How many data classifiers (INFOTYPES) are supported by Borneo for SaaS?

Borneo supports 100+ ML-powered pre-configured data classifiers across a wide variety of categories like Healthcare, Finance, Government IDs, Crypto Tokens, and Developer Tokens.

Find the list of supported Infotypes below:

LOCAL_MAC_ADDRESS	Developers Secret
MAC_ADDRESS	Developers Secret
UUID	Developers Secret
AWS_ACCESS_KEY_ID	Developers Secret
AWS_SECRET_ACCESS_KEY	Developers Secret
FACEBOOK_ACCESS_TOKEN	Developers Secret
FACEBOOK_APP_TOKEN	Developers Secret
FACEBOOK_OAUTH	Developers Secret
GENERIC_API_KEY	Developers Secret
GITHUB_TOKEN	Developers Secret
GOOGLE_API_KEY	Developers Secret
HEROKU_API_KEY	Developers Secret
INSTAGRAM_API_KEY	Developers Secret
JWT	Developers Secret
MAILCHIMP_API_KEY	Developers Secret
MAILGUN_API_KEY	Developers Secret
PASSWORD	Developers Secret
SLACK_TOKEN	Developers Secret
SLACK_WEB_HOOK	Developers Secret
SQUARE_ACCESS_TOKEN	Developers Secret
SQUARE_OAUTH_SECRET	Developers Secret
STRIPE_API_KEY	Developers Secret
STRIPE_RESTRICTED_API_KEY	Developers Secret
SWIFT_CODE	Developers Secret
TWILIO_API_KEY	Developers Secret
TWILIO_AUTH_TOKEN	Developers Secret
TWILIO_API_SECRET	Developers Secret
TWILIO_SID	Developers Secret
TWITTER_ACCESS_TOKEN	Developers Secret
SALESFORCE_ID	Developers Secret
CREDIT_CARD_NUMBER	Finance

CVV	Finance
IBAN_CODE	Finance
DATE_OF_EXPIRY	Finance
AMERICAN_BANKERS_CUSIP_ID	Finance
US_BANK_ROUTING_MICR	Finance
MONEY (Change to Currency)	Finance
COUNTRY	General
DATE	General
IP_ADDRESS	General
LAT_AND_LONG	General
LATITUDE	General
LONGITUDE	General
US_STATE_CITY	General
DOMAIN_NAME	General
PASSPORT_NUMBER	Govt. ID
DRIVER_LICENSE_NUMBER	Govt. ID
US_PASSPORT_NUMBER	Govt. ID
US_ADOPTION_TAXPAYER_IDENTIFICATION_NUMBER	Govt. ID
US_EMPLOYER_IDENTIFICATION_NUMBER	Govt. ID
US_INDIVIDUAL_TAXPAYER_IDENTIFICATION_NUMBER	Govt. ID
US_PREPARER_TAXPAYER_IDENTIFICATION_NUMBER	Govt. ID
US_SOCIAL_SECURITY_NUMBER	Govt. ID
US_VEHICLE_IDENTIFICATION_NUMBER	Govt. ID
FDA_CODE	Healthcare
US_HEALTHCARE_NPI	Healthcare
US_DEA_NUMBER	Healthcare
PHONE_NUMBER	Personal Information
STREET_ADDRESS	Personal Information
DATE_OF_BIRTH	Personal Information
AGE	Personal Information
AGE_RANGE	Personal Information
GENDER	Personal Information
INCOME	Personal Information
INCOME_RANGE	Personal Information
EMPLOYMENT_STATUS	Personal Information
RACE	Personal Information
RELIGION	Personal Information

EDUCATION_QUALIFICATION	Personal Information
POSTAL_CODE	Personal Information
Age	Personal Information
US_PHONE_NUMBER	Personal Information
US_ZIP_CODE	Personal Information
SOCIAL_NETWORK_ID	Personal Information

Do you support any integrations for Incident alerts or SIEM's ?

All of the findings/remediation actions can be sent to your SIEM/ticketing system of choice like Jira, Email, Splunk, SNS, EMail, API, etc.

What all controls are in place to prevent API abuse, since Borneo uses API based authentication.

- To monitor and manage API calls coming from automated scripts (bots), we have monitoring in place on the Slack end and we also use limit/budget tags on AWS to ensure we don't overrun the system.
- To drop primitive authentication, we only use Slack-approved OAuth.
- To implement measures to prevent API access by sophisticated human-like bots, we do not support any open / publicly accessible APIs. The internal-only API for config is set up behind the customer VPN and is authenticated.
- To support robust encryption, we only use Slack-approved/provided endpoints.
- Token-based rate-limiting equipped with features to limit API access based on the number of IPs, sessions, and tokens based on Slack's approved rate limits - details https://api.slack.com/docs/rate-limits#rate-limits__overview.

What type of access is required by Borneo's employees to deploy the application/connector in our environment? What are the privileges associated with this access? For how long is such access required?

This is optional i.e. We do not require this role if the customer is doing the deployment themselves. In case the customer wants us to do the deployment, we use a scoped IAM dev-ops role which is limited to run the deployment scripts, it will not have any access to user data. The role is only required for ~30 mins for the deployment. We share the cloud formation templates/role for review.

Does Borneo only support public channels in Slack? Is there support for scanning private channels/direct messages, connected channels, without adding the app to each one?

For our Enterprise version, there is no need to add the app to every channel (public, private or direct), you just need to authorize the app into your slack workspace.

Our PoC version currently only supports scanning Public channels. You will need to add the app in the admin channel for the PoC to receive the notifications, however, you can skip this in our production version if you chose to send the notification directly to your SIEM (Jira, Splunk, etc).

Pl refer to the table below for our Slack coverage:-

	Public	Private	Direct
PoC Version	Y	N	N
Enterprise	Y	Y	Y
Business Plus	Y	Y(1)	Y(1)
Business Standard	Y	N(2)	N(2)

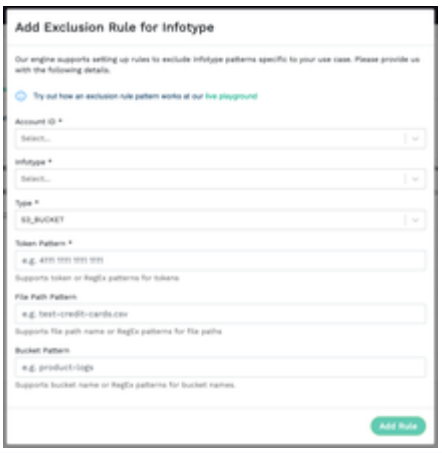
(1) Uses data export feature from Slack. Does not support realtime scanning.
(2) Not possible due to API restriction's imposed by Slack for standard plans.

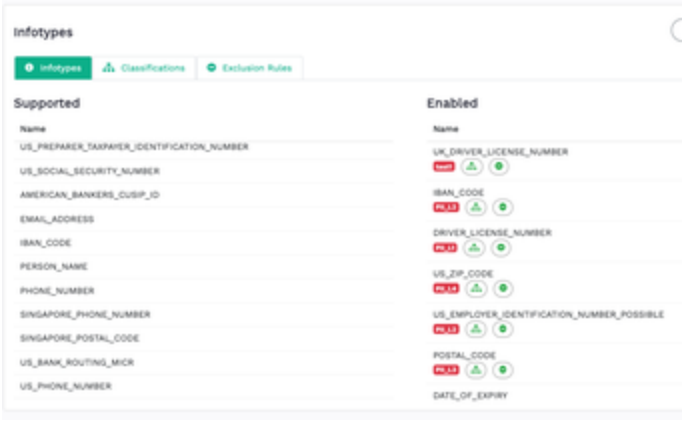
Does Borneo support attachment unwrapping? If an xlsx/docx or txt document is uploaded will its content be scanned?

Yes, Borneo supports attachment unwrapping for both PoC and Production versions. Our extraction service supports an exhaustive list of file types. Please note our PoC version has a file size limit of 10MB.
Contents in Xlsx/Docx or txt documents will be scanned. However, there is a limitation of our PoC version, where the first row is treated as header info, this has been addressed in our Production version.

Is there a main dashboard where one can do some tuning work?

Our PoC dashboard is limited. Our Production version supports infotype classification based on your internal policies, as well as exclusion rules which can be customized to reduce noise for your environment to deal with your specific example. Do let us know if you want us to fine-tune your PoC instance to disable Name/Data etc to reduce the noise while you are testing. (check out screenshots attached below).





Does Borneo provides any remediation workflows?

Yes, Borneo supports multiple remediation workflows such as :

1. Automated timed deletion/cleanup - This will delete the content after a certain configurable period of time, which is most preferred as it reduces the risk surfaces with the least amount of noise or overhead for both users and security teams
2. Admin alerts with optional admin triggered deletion.
3. Creating an issue ticket in Jira or any ticketing system and have the ticket automatically assigned to a user or a group.
4. Forwarding alert events into Splunk or any other SIEM system.

Do we support custom infotypes?

Yes, we support custom infotypes. You just need to request it and our team will custom build and ship it to you within few weeks. We just require enough data points around to get it built for high accuracy.