Forcepoint Cloud Threat Assessment Report

INTRODUCTION AND FAQ

FORCEPOINT CASB

FORCEPOINT

1 | Cloud Threat Assessment

Forcepoint Cloud Access Security Broker (CASB) provides visibility and control for cloud applications by giving you direct insight into - and control over - your users' cloud activities. Forcepoint CASB enables you to understand the rhythm of your people and the flow of your data.

In focusing on the Human Point, Forcepoint CASB utilizes UBA (advanced user behavioral analytics) to dynamically determine organizational risks by identifying specific users who pose potential threats to your data and information. CASB applies A.I. and machine learning methods to intersect "likelihood and impact" of breaches to provide clear and actionable responses.

Forcepoint is providing complementary threat assessment reports to organizations whom are consumers of one or multiple of the following SaaS applications:

- Microsoft Office 365
- Salesforce
- Box
- G Suite

This assessment is conducted utilizing cloud provider certified APIs and is 100% none intrusive or disruptive. Please refer to the FAQ for complete details on how the assessment is performed. Upon analysis completion, you can expect to receive the following details relating to your cloud posture:

- Cloud service usage pattern – both benign and suspect activities
- Geographic analysis – typically and outlier access based on country of origin
- Privileged users – accounts with potentially excessive privileges
- Dormant users – dormant accounts of over 90 day period
- User risk score – users exhibiting the most risk

As cloud adoption shifts application delivery and maintenance responsibilities, cloud computing also represents increased risks to security, it embodies many risks to businesses of all sizes, including potential internal security, criminal, and regulatory issues. Cloud adoption challenges our understanding and response to these threats. Forcepoint CASB is purpose built to address these challenges, without overwhelming critical resources, and allowing you to focus on what makes you thrive.

2 | FAQ

Q. What will the assessment provide?

A. Forcepoint CASB will provide a detailed report of your cloud application risk posture. This report will include details of users within your organization who present the most behavioral risk, the greatest number of security incidents and your overall risk.

Q. Do I need to deploy anything to receive this information? A. Forcepoint CASB is a cloud service and requires no on-premises or endpoint agents to provide this

information.

Q. Will there be any user impact? A. This report is provided using APIs and is deployed 100% out of band.

Q. What do I need to prepare?

A. In order for Forcepoint CASB to be connected via APIs, we require authorization from you, granting our services to connect via APIs into your environment. We will need your application administrator or an individual who has privileged access to provide this authorization. The authorization will then be granted through a configuration wizard within CASB and the service provider.

Q. Is Forcepoint storing our admin credentials? A. No. Our systems receive an API connection token that contains automatic expiration dates that will vary

from provider to provider. Customers can also explicitly remove access in their administrative console.

Q. What information are you inspecting? A. Forcepoint CASB uses proprietary algorithms to inspect and detect malicious behaviors from information

gathered through the API connection, including various logs and other relevant content.

Q. What information are you storing?

A. Forcepoint CASB only stores meta-data relating to anomalous behaviors and does not store any customer sensitive data.

3 | API Connection Explained

To provide you with our free Cloud Threat Assessment Report, Forcepoint CASB will connect to your selected cloud application and check information including user activity, configuration settings and file sharing. This will be evaluated using the Forcepoint advanced policies and benchmarks to provide you with a full cloud threat assessment of that service.

Forcepoint CASB connection to the cloud service is provided by following this standard and secured flow:

1. The customer (assisted by Forcepoint rep) logs in to the Forcepoint CASB portal

2. Forcepoint CASB opens a cloud application login page

3. The customer logs in to the cloud application (this is a direct login to the cloud application; Forcepoint CASB does not track that connection)

4. Once logged in, the cloud service displays the list of permissions that Forcepoint CASB requests to perform the cloud threat assessment

5. This list should be reviewed and approved by the customer

6. Once the customer approves, the cloud service generates a token that will be used by Forcepoint CASB to connect to the service.

7. Important notes about this token:

a. CASB keeps the token and uses it to access the cloud application. Admin credentials used to create the token are not kept or stored by Forcepoint.

b. The token does not get the permissions of the logged in admin. It gets a subset of the permissions required by Forcepoint CASB which the customer reviewed and approved.

8. Admin privileges required:

a. As mentioned, Forcepoint CASB requires a token with some permissions from the cloud service. Authorizing the cloud application to create such token requires an administrator login.

b. We require an authorized or administrative account for this connection and he or she should be on the set-up call to grant the appropriate access.