The pace of digital transformation is accelerating with the shift to working from home, which leads to increased reliance on cloud applications. However, before a new app can be rolled out to employees, risk assessments and business impact analyses need to be conducted as part of the Governance, Risk, and Compliance process.

Yet, information security professionals with the domain expertise in the various cloud apps that a business may need to use are in short supply. This often means enterprises are forced to choose between saying “No” to apps that can bring agility and resilience, or saying “Yes” to risks that exceed what the business can sustain.

Forcepoint created the Business Impact Analysis (BIA) feature for Forcepoint Cloud Access Security Broker (CASB) to help customers mitigate risks introduced by cloud apps in a more consistent and easy-to-use way. Forcepoint CASB engineers analyzed and scored every user action in the most-used cloud apps based on the potential security impact to a business. By having a method to interpret the risks posed by any user action in various cloud apps in a consistent, quantitative way; customers can say “Yes” to on-boarding new cloud apps while quickly and easily mitigating the associated risks.

**Mitigate all high-risk activities in an app with a single rule**

The BIA feature introduces the Impact Score predicate in the CASB rule editor. This allows for the easy creation of rules which can apply consistent mitigation for user activities with similar impact scores.

Customers can now create a CASB rule that takes any “Critical” level activities as a predicate and, for example, prompt the user for Multi Factor Authentication, thereby enforcing consistent security policies against risky user activities without needing to have domain expertise in specific apps. This helps to accelerate the time to value of cloud adoption for Forcepoint CASB customers by giving security professionals predefined methods to mitigate risk for the most popular business applications out-of-the-box.

### Impact Score

- The business impact score is a numeric value in a range of 0-100, which reflects the potential impact of a single user activity on specific data in a cloud application, in terms of Confidentiality, Integrity, Availability (CIA).

  The value range is divided into the following tiers:
  - **Critical:** 81-100
  - **High:** 55-80
  - **Medium:** 31-54
  - **Low:** 0-30
The BIA scoring model consists of a basic detection rule with a numeric score (0–100), and these scores are broken down into four different levels: Critical, High, Medium, and Low. The Impact Score is included in the activity audit log, and for customers using a SIEM tool, this can be ingested by the SIEM to allow for automating enforcement changes in response to changes in Impact Score trends.

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>RANGE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>81–100</td>
<td>Sensitive activities. For example, sensitive administrative actions, modifying or disabling main security controls, bulk data export, mass deletion, bulk sharing.</td>
</tr>
</tbody>
</table>
| High   | 55–80 | High-impact activities that usually require high-level permissions, but do not need to be reviewed by a security department each time they occur. For example, modifying a Price Book in Salesforce, resetting a user password.  
Individually, these activities do not need to generate a security alert or a push notification. It is recommended to use additional conditions with these activities to generate an alert. |
| Medium | 31–54 | Activities that require common permissions. For example, sharing a file, exporting a report, viewing a lead.  
Individually, these activities do not need to generate a security alert or a push notification. It is recommended to use additional conditions with these activities to generate an alert. |
| Low    | 0–30  | Activities that do not require special roles or permissions. For example, modifying personal profile settings, uploading or downloading content to personal user folder. |

**Features include:**

- 750 unique activities mapped just for SalesForce!
- 50 of which are “Critical” impact activities.
- This means you can mitigate risk from 50 critical activities with a single rule.