# extensible Visibility Reference Framework

*Google Workspace Enterprise Business Applications Workbook*


## OVERVIEW

The extensible Visibility Reference Framework (eVRF) provides a framework for organizations to identify visibility data that can be used to mitigate threats, understand the extent to which specific products and services provide that visibility data, and identify potential visibility gaps.

The eVRF includes the eVRF Guidebook and eVRF workbooks. Each eVRF workbook defines a visibility surface and enables organizations to produce their own visibility coverage maps for as-planned or as-implemented system configurations.

## VISIBILITY SURFACE

eVRF uses visibility surfaces to represent segments of an organization's enterprise environment. The visibility surface for this workbook focuses on the Cloud Business Applications (see Figure 1) portion of the enterprise, which comprises email, messaging services, and enterprise content management. Beyond the scope of the current visibility surface are items related to the domains of organization on-premises infrastructure and remote user devices, as well as external partner organizations and other external entities with which the agencies communicate.

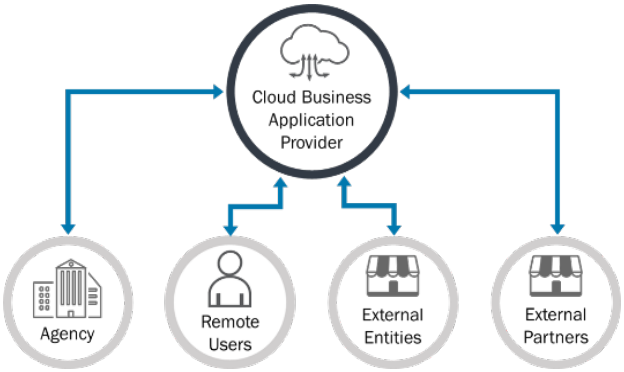


***Figure 1: Cloud Business Applications Scope***

As shown in Figure 2, the observation points identified within the cloud business applications domain include the business application tenancy, labeled as the cloud tenant; and the ingress location(s) for the tenancy, labeled as the cloud reverse proxy. The telemetry is derived from sensors providing visibility into server-side email, messaging services, enterprise content management, and tenant configuration details. Beyond the scope of the current visibility surface definition are items related to the cloud reverse proxy observation point and third party external components and connectivity variations for accessing the business applications.

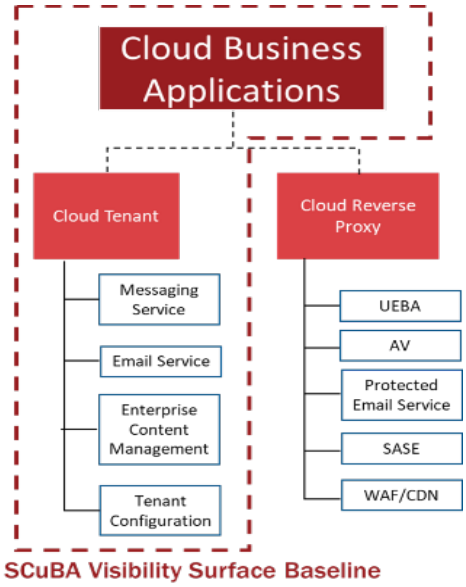


**Figure 2: Cloud Business Applications Visibility Surface Scope**

### Assumptions and Caveats

- All products and services are used and configured optimally.
- Vendors continue to update their product offerings, which may require updated coverage maps to ensure accuracy.

## VENDOR COVERAGE MAPS

Vendor coverage maps characterize how a product addresses a visibility surface by providing relevant cyber-observable data. Vendors may choose to create coverage maps indicating which product tiers and configuration settings can provide visibility into the MITRE ATT@CK® (Adversarial Tactics, Techniques, and Common Knowledge) techniques for a given visibility surface.

The following services or applications are covered in this workbook:

### Google Workspace Product Narrative

Google Workspace is a Software as a Service (SaaS) offering from Google comprising various productivity software applications, the accompanying administration application, and associated application programming interface(s) (APIs). Google Workspace can be accessed via desktop/mobile browsers and native mobile applications.

The majority of Google Workspace's APIs are Representational State Transfer (REST) based and can be accessed via HTTPS. Visibility metrics for Google Workspace can be accessed via several methods:

- Workspace's administration application (user interface).
- Workspace's Reports API (REST).
- Google Cloud Platform's BigQuery (SQL queries, if enabled/integrated).
- Google Cloud Platform's Cloud Logging (user interface of pub/sub, if enabled/integrated).

## Google Workspace Service Inventory

Google Workspace consists of several applications that are considered end-user productivity software: Gmail, Calendar, Drive, Data Studio, Groups, Keep, Chat, Meet, Vault, and Jamboard. Workspace works with Google hardware devices such as Jamboard and Chrome.

Google Workspace has administrative and platform-wide capabilities that are composed of components such as the Google Admin Console and Admin SDK/APIs, which contains the Reports API. Logging data is available via Workspace's administration console or APIs. In addition, Workspace works with Google Cloud Platform's BigQuery and Cloud Logging functionality.

## Google Workspace License Level Details

The majority of Workspace logging is not dictated by license type. Generally, if the license allows users to use a product, those logs are included in Google Workspace. License level dictates the method by which one can access this data. Accessing data via the Reports API and Admin Console is not limited by license, except in cases where features are not available.

An Enterprise license is required to access the data integration with BigQuery. Enterprise or Cloud Identity Premium licenses are required to access some parts of the Cloud Logging integration. Vault is only available to Business Plus and higher (Enterprise) licenses. There are some minor nuances depending on the application type. For example, Gmail is only accessible via BigQuery and, by extension, only available by Enterprise licenses.