extensible Visibility Reference Framework

Microsoft 365 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

The 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 portion of the enterprise. Beyond the scope of the current visibility surface are items related to the domains of the organization's on-premises infrastructure and remote user devices, as well as external partner organizations and other external entities with which the agencies communicate.

As shown in Figure 1, 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.

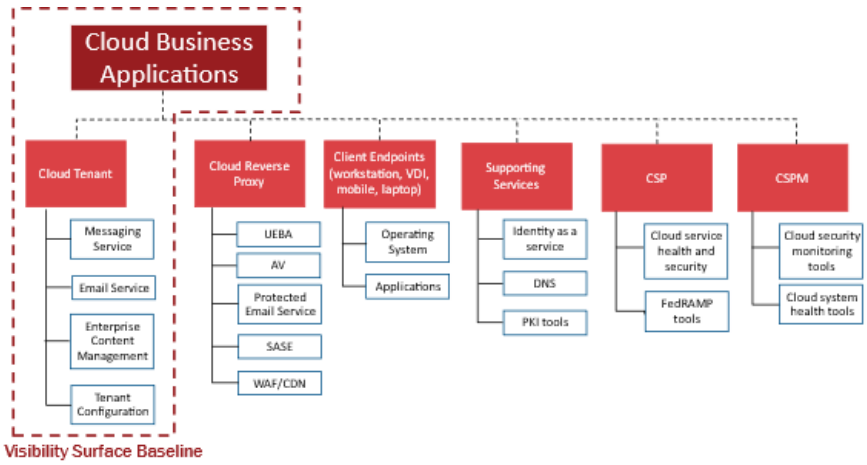

Figure 1: Cloud Business Applications Visibility Surface Scope

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 Microsoft services or applications are covered in this workbook:

Vendor Product Narrative: Microsoft 365

The Microsoft 365 (M365) Coverage Map provides specific visibility information of M365 Software as a Service (SaaS) Services in response to CISA characterized visibility data. This visibility is established through service specific audit logs, which exist in the Microsoft Purview auditing (formerly Unified Audit Log (UAL)). Microsoft Purview auditing is the log repository for all M365 Services, and the audited activities are referenced throughout the M365 Coverage Map.

Resources:

- Microsoft Purview auditing solutions - Microsoft Purview (compliance) | Microsoft Learn
- Office 365 US Government - Service Descriptions | Microsoft Learn

Vendor Service Inventory: Microsoft 365

The specific services below are assessed within the M365 Coverage Map:

- Email—Exchange Online
- Content Management—SharePoint Online and OneDrive for Business
- Messaging—Microsoft Teams (Chat)

Additional categories in blue are included in the workbook that showcase Microsoft services (e.g., PowerBI, PowerApps, Security and Compliance, etc.) that are not currently captured by the existing visibility surface scope.

M365 Services Resources:

- Microsoft 365 and Office 365 service descriptions - Service Descriptions | Microsoft Learn

VENDOR LICENSE LEVEL DETAILS: MICROSOFT 365

The M365 Coverage Map is aligned with two specific Licensing tiers: Microsoft 365 Government G3 and Microsoft 365 Government G5. Microsoft Purview Audit Standard (formerly known as Basic Audit) is included with M365 G3, and Microsoft Purview Premium Audit (formerly known as Advanced Audit) is included with an M365 G5 license. The M365 Coverage Map captures the differences in visibility between the licensing tiers. Figure 2 presents the differences between the Basic Audit and the Advanced Audit.

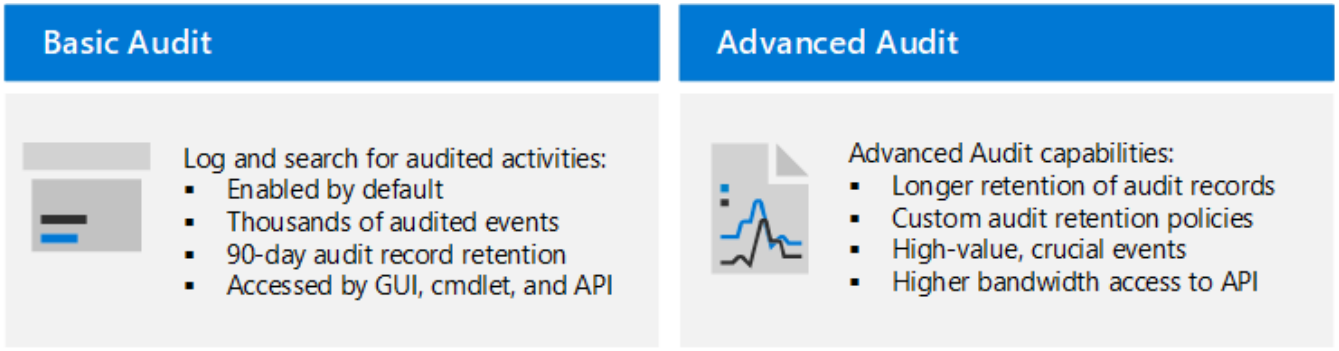

Figure 2: Basic Audit vs. Advanced Audit

Licensing Resources:

- Microsoft 365 Government
- Microsoft Purview auditing solutions - Microsoft Purview (compliance) | Microsoft Learn