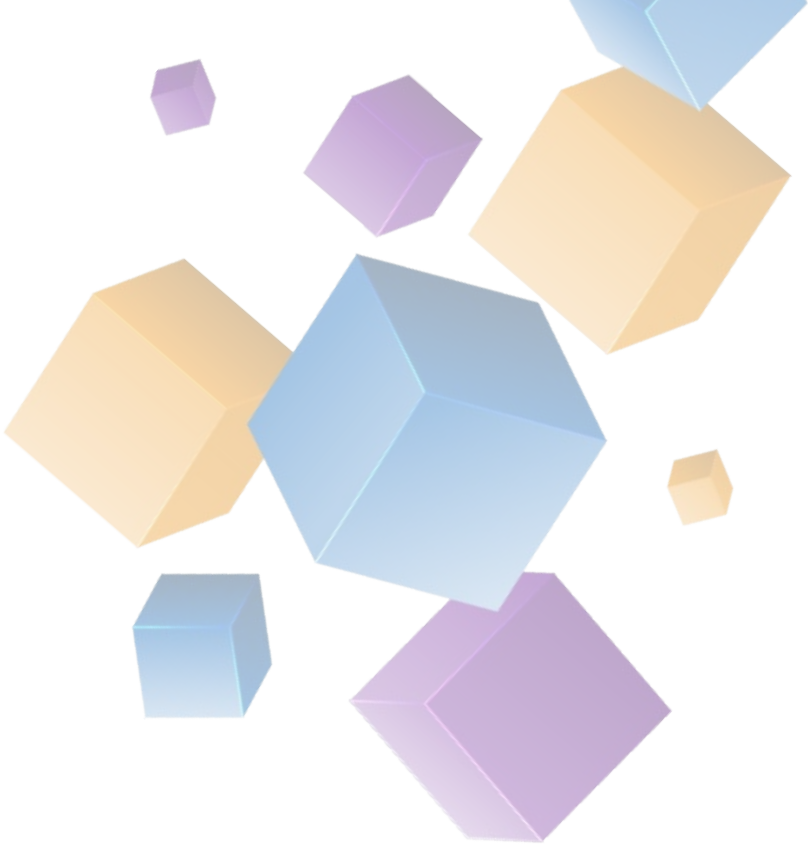


WHY TESSERACT REQUIRES THE MICROSOFT 365 E5 OR G5 LICENSE

What are the Requirements

All future and current Tesseract customers are making strides towards the same goal: getting and staying compliant with Cybersecurity Maturity Model Certification (CMMC) and maintaining cost-effective cybersecurity programs. Tesseract leverages a variety of Microsoft applications and services to help build these programs, and Ardalyst has designed Tesseract around using the Microsoft E5/G5 license due to its advanced features around compliance and security. One of the big questions we get from new customers is why we say that the E5/G5 license is mandatory for successful execution of a Tesseract Program. Let's break this down.

How Does it Compare to Business Premium or the E3/G3 License?

The most popular alternative license we are often asked about is leveraging the Microsoft Business Premium license or just using the E3/G3 license. There is certainly some appeal, with the Business Premium and the E3 licenses having a host of advanced features at a portion of the initial cost of the E5/G5. While pricing is a big motivator when it comes to license selection, the missing advanced features that are built-in to the E5/G5 license are the keys to making or missing your compliance and cybersecurity goal.

Below is a table that shows the most impactful missing features of the Business Premium and E3/G3 license when compared to the M365 E5/G5. You can find a more comprehensive comparison of these features over at M365 Maps Feature Matrix.

Feature	Business Premium	E3/G3	E5/G5	Explanation	CMMC Assessment Objectives
eDiscovery Premium	✗	✗	✓	Offers a comprehensive workflow for preserving, collecting, analyzing, reviewing, and exporting content for internal and external investigations across Microsoft 365 and Office 365, aiding organizations in meeting CMMC requirements by managing and protecting data, and responding to legal matters or internal investigations.	AU.L2-3.3.1 AU.L2-3.3.5
Rules-Based Classification	✗	✗	✓	Offers capabilities for auto-labeling content based on regular expressions present in a document. This helps capture potentially sensitive data that wasn't manually labeled otherwise.	MP.L2-3.8.4 MP.L2-3.8.5
Defender for Identity	✗	✗	✓	Provides insights on Identity configuration to better identify, detect, and investigate advanced threats directed at your organization to prevent unauthorized access to organizational resources. Tesseract requires this to be integrated with Sentinel for alert generation and response.	AC.L1-3.1.1 IA.L1-3.5.2
Defender for Cloud Apps	✗	✗	✓	Provides comprehensive protection and control for your cloud applications, aiding in identifying and mitigating potential cyber threats. Tesseract requires this to be	AC.L2-3.1.12

				integrated with Sentinel for alert generation and response.	
Risk-Based Conditional Access	✗	✗	✓	Allows organizations to protect users by configuring policies that respond to risky behaviors, automatically blocking sign-in attempts or requiring additional security measures depending on the risk-level of the activity.	AC.L2-3.1.12 AC.L2-3.1.8 AC.L1-3.1.20
Privileged Identity Management	✗	✗	✓	Allows organizations to create a "Just-in-Time" access management solution where users request activation of their privileged roles. This creates an audit trail of when privileged roles were activated and by who, allowing for more secure and auditable use of privileged identity accounts.	AC.L2-3.1.5 AU.L2-3.3.9
Attack Surface Reduction	✗	✓	✓	Offers organizations the ability to deactivate any unnecessary processes running on a managed endpoint to reduce the endpoints attack surface area, protecting the asset from potentially malicious activity.	AC.L2-3.1.14 CM.L2-3.4.7
MIP Integration	✗	✗	✓	Allows for Defender for Endpoint to scan endpoints for sensitive or labeled content on a device, increasing the protected surface area of CUI labeled documentation.	MP.L2-3.8.4 MP.L2-3.8.5
Windows Autopatch	✗	✓	✓	Automates patching of Windows, M365 apps for Enterprise, Microsoft Edge, and Teams to eliminate the need for manual continuous patching, reducing the threat and exposure of potential vulnerabilities.	MA.L2-3.7.1
Trainable Classifiers	✗	✗	✓	Allows for training data labels on a variety of examples of CUI documentation to enhance the capability to autodetect, label, and protect CUI data even if the labeling or content isn't always consistent.	AC.L2-3.1.14 CM.L2-3.4.7
Microsoft Sentinel Ingestion Benefit	✗	✗	✓	Sentinel allows for correlating log and alert data across multiple security platforms and viewing that data in a single pane of glass. With an E5 license, customers are granted a free 5MB of data ingestion per E5 user, per day!	AU.L2-3.3.1

Exclusive Features of the E5/G5 License that make Tesseract Program's Successful

The E5 license is not just another license; it's a comprehensive suite of tools and features that we leverage to make Tesseract an effective compliance program. Without these exclusive features, Tesseract wouldn't be the robust and reliable solution it is today. Here are the features unique to the E5 license that set it apart:

- Data Lifecycle Management: This feature, exclusive to the E5 license, provides data retention rules and labels, along with inactive and archive mailbox capabilities. These tools are crucial for managing the lifecycle of data, ensuring its availability when needed, and are not available in lesser licenses.
- Purview for Records Management: This feature includes record labeling and retention, File Plan, and litigation hold functionalities. These tools are essential for managing records and ensuring their preservation for future reference or legal purposes and are unique to the E5 license.
- eDiscovery Premium: This feature offers investigation, quarantine, and spill/inadvertent data disclosure remediations. These capabilities are critical for managing potential data breaches and mitigating their impact and are not found in other licenses.
- Advanced Message Encryption: Purview's advanced message encryption, exclusive to the E5 license, provides more flexible controls over external recipients of encrypted email, enhancing the security of communication.
- Defender for Office 365 Plan 2: This feature offers attack simulation training, real-time reports, safe attachments, and safe links for email protection. It eliminates the need for third-party email filtering or protection services, providing a comprehensive security solution only available with the E5 license.
- Privileged Access Management: Microsoft Purview's Privileged Access Management helps protect your organization from breaches and helps meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings. This feature, only available with the E5 license, implements just-in-time access rules for tasks that need elevated permissions.
- Data Loss Prevention: This feature allows you to define policies that help prevent people from sharing sensitive information in a Microsoft Teams channel or chat session. This crucial feature for preventing data leaks and ensuring the confidentiality of information is exclusive to the E5 license.
- Defender for Cloud Apps: This feature helps you discover and protect your SaaS applications and the data that is produced, stored, and processed. This comprehensive protection feature is unique to the E5 license.
- Defender for Identity: Fully integrated with Microsoft Defender XDR, this feature leverages signals from both on-premises Active Directory and cloud identities to help you better identify, detect, and investigate advanced threats directed at your organization. This advanced threat detection feature is exclusive to the E5 license.
- Advanced Hunting: This is a query-based threat hunting tool that lets you explore up to 30 days of raw data. You can proactively inspect events in your network to locate threat indicators and entities. The flexible access to data enables unconstrained hunting for both known and potential threats. This powerful threat hunting tool is only available with the E5 license.

These exclusive features in the E5 license provide a comprehensive and robust security and compliance solution, making it a critical requirement for Tesseract. The E5 license is not just a cost, but an investment in the security and compliance of your organization. While we understand that other licensing models in the M365 ecosystem can feel more cost-effective in the short term, the features that are missing with the absence of the E-5/G-5 license leaves your compliance program with feature gaps that will end up incurring operational cost in failed assessments and remediation times.

Why Not Just have one E5/G5 License and the Rest of them E3?

When choosing licensing and features, a common question that comes up is "What if I just get one E5 license to get some of the security features, then give everyone else a lower license like the E3?" The reasoning behind this logic comes in play when you look at how Microsoft activates features for your environment when you assign a license.

Most features, like the Office 365 productivity tools, Teams, SharePoint, and some other productivity tools are all gated behind a license. Have an F3 license and want to use the desktop version of Word? You'll need to upgrade to an E3 or E5 license. Have an E3 license but need PowerBI Pro? You'll need to either buy an extra PowerBI Pro license or upgrade to the E5. These examples are to point out that, for most features, Microsoft controls access on a per user/per license basis. When you go to access a Microsoft application, the first thing it's going to do is audit your account for the license SKU you have and what features are activated for that SKU. If you don't have the relevant entitlement to use the application, you'll be denied.

Where this gets tricky is when you get to what Microsoft refers to as "Tenant-level" features, or features that are turned on when the relevant license is activated but it cannot gate access to the feature at the user/license level. Look at Microsoft Defender for Office 365 for example. Microsoft Defender for Office 365 Plan 2 (MDO P2, going forward) is included in the E5/G5 license. As a tenant-level service, the only thing MDO P2 needs to be activated is a singularly assigned E5/G5 license. Once assigned, MDO P2 will be activated and all users in the tenant will receive protection while using all email and collaboration tools since there is no way at this time to filter out users based on their license assignment for this service.

While this makes it tempting to implement a single E5/G5 license for the tenant-level features, Microsoft clearly states in their documentation that any user who needs to leverage a specific service should have the appropriate license. Even if that service is activated at the tenant-level. To ensure organizations are complying with their Program Terms, Microsoft conducts routine license compliance verification audits each year by programmatically selecting customers each year and reviewing their license usage and assignment. If any customer is found to be in violation of Microsoft's Program Terms, such as having a single E5 for the tenant-level features that E3 users are leveraging, you can incur a monetary penalty and be forced to purchase any missing licensing. It's important to note that these audits are mandatory, and you contractually agree to the possibility of an audit as soon as you purchase a license from Microsoft.

Ways to Manage Costs for Your Tesseract Program

At the heart of Tesseract are two specific core values that allow us to work with customers from many industries and of all different sizes: ***Tesseract is flexible and cost-effective.*** What that means for our customers is that we can build your Tesseract program to suit your organization's unique requirements while working to keep costs within your budget. While Tesseract leverages the comprehensive suite of features and tools provided by the E5/G5 license, we also understand that it comes with a higher price tag when compared with other license models. That's why Tesseract supports a variety of **User Groups** that mix different licenses and capabilities to suit your needs.

- **Full Users** include an identity, a fully managed endpoint, and a mobile endpoint for maximum computing power and a typical user experience. These users are best suited for the E5/G5 license to get the most out of those managed endpoints and the required security features.
- **Cloud Users** are the same as Full Users, but with a virtual endpoint like a W365 PC or Azure Virtual Desktop, for maximum computing power in travel and WFH situations, without requiring a physical endpoint. These users are also best suited for the E5/G5 license for the same reasons as Full Users.
- **Web-Only Users** only access the enclave through Microsoft Web Applications and a mobile device, saving cost and reducing risk for users that don't need full endpoints or desktop versions of Microsoft Office. These users are best suited for the F3/F5 Security and Compliance combination license, which gives all the access and security a web user needs without the extra features required to manage physical endpoints. The F3/F5 license combination is the E5/G5 equivalent for users who only need those web-based features.

- **E-Mail Only Users** are limited to the Outlook Web experience, perfect for users that work primarily on GFE, on shop floors, or in other environments where they need limited access. These users are also best suited for the F3/F5 license. We manually disable the features that an E-mail only user doesn't need but maintain the security and compliance protections necessary to have a compliant CMMC program.

Each organization has a unique mix of users and business cases that drive how they build out their environment. A Tesseract program is designed to work alongside your business, not interfere with it, and that same concept applies to how we organize our user communities. This also allows us to build you the most cost-effective program possible by ensuring the right users have the right features and access, without breaking the bank.

What if I Still Want to Use a Different License?

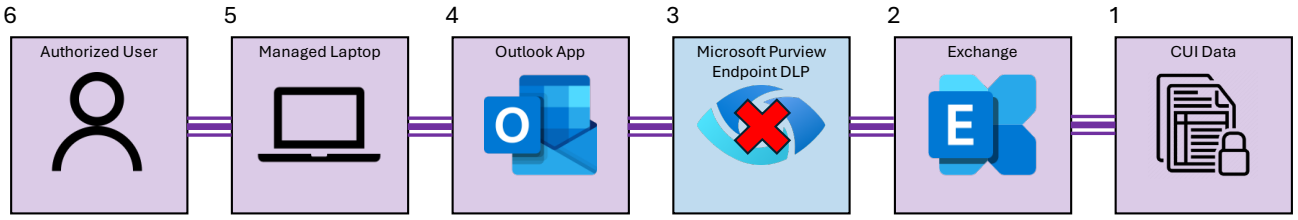
As we stated in the previous section, two of the core values of Tesseract are providing flexible and cost-effective programs for our customers. Cost-effectiveness means something different to every organization depending on the budget that has been allocated to building or improving your cybersecurity posture. Throw in the comprehensiveness of Microsoft's library of licenses and organizations have many options for designing how their users should interact with the Azure and Microsoft 365 services. While Ardalyst recommends that users seeking CMMC compliance, especially level 2 compliance, purchase licensing the falls in line with one of our user types, we understand that organizations could have their own reasons for choosing a different licensing structure. Maybe you want to leverage the less expensive Business Standard or Business Premium offerings. Ardalyst can help build a Tesseract program around these licenses that can provide you with an effective cybersecurity program, but it's important to understand how using these different license types can impact your journey to compliance.

1. **Risk to Compliance Goals –** The biggest risk to achieving CMMC L2 compliance is applying the right licenses for the right features to protect your Users, Data and Assets. The pitfalls to choosing licenses like Business Premium or Business Standard are, gaps in compliance framework configurations, gaps in tool features in Microsoft Defender XDR suite and, speed to implement compliant baseline configurations.
2. **Gaps in Security Architecture** – As mentioned in the sections discussing features, the E5/G5 license comes packed to the brim in features that enable environments to leverage the full suite of security tools Microsoft has to offer without needing an extra license. As you start to select lower cost licenses, you start to lose access to more security features and benefits. For example, Microsoft's Business Premium license doesn't support Defender for Cloud Apps. While it does provide a more basic protection in Office 365 Cloud App Security, Defender for Cloud Apps is a critical part of managing and securing access to all cloud applications your organization relies on, while reducing the footprint of shadow IT which can introduce a wide range of threat vectors to your environment. This is just one example, among many, where choosing a cheaper option can increase your appetite for risk.
3. **Cost of Remediation –** Tesseract customers all receive a Remediation Guarantee as a part of their program. This gives customers peace of mind knowing that, in the unlikely event they don't pass an assessment, Ardalyst will update and improve their program free of charge to prepare them to pass any future re-assessments. This guarantee relies on customers purchasing license types that align with our Tesseract User types. Programs that use non-standard licenses, while still eligible for the guarantee, might be required to upgrade their licensing should Ardalyst determine that the gap between the current program posture and CMMC compliance requires features only available in a higher-level license.

Let's analyze one of the many controls required to be met by organizations seeking CMMC Level 2 compliance against a specific license and scenario. Let's say we have two different organizations.

Organization one has users who have physical laptops and Microsoft Business Premium licenses. Organization two has users who have physical laptops and E5/G5 licenses. Each organization needs to be able to meet the requirements of SC.L2-3.13.6[a], which states that "the confidentiality of CUI at rest is protected." Let's take a look at the diagrams below to understand how a Business Premium license might put an organization at risk for complying with this control.

TESSERACT™

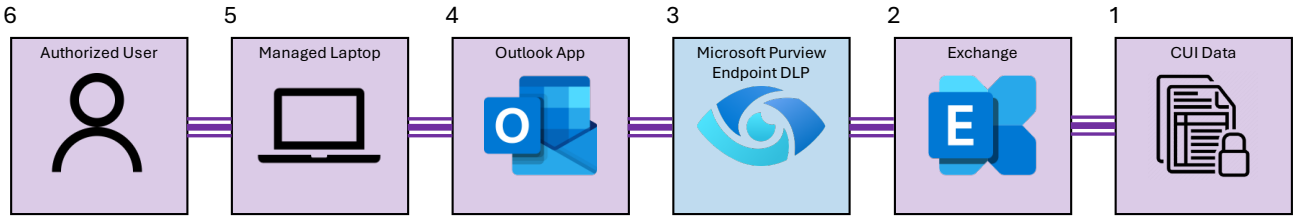


Organization 1 – CUI Authorized User on a Managed Laptop accessing CUI on the local device, using a Business Premium license

The data flow in this scenario is as follows:

1. CUI is sent to a user's mailbox via an encrypted email, either directly from the DoD or from another partner.
2. The sensitive email arrives at the user's Mailbox and is ready to be synchronized with the user's Outlook application on their desktop.
3. While Business Premium does include features for data labeling and data loss prevention, it doesn't allow for the integration of DLP for Endpoints, so Purview is unable to track the file once it is on the endpoint.
4. Outlook syncs with Exchange Online and makes the encrypted email available to the user.
5. The user opens and reads the encrypted email and downloads the document to their laptop for further use.
6. The Authorized User manipulates the file and changes some of its contents in preparation to send it back to their customer but, without Endpoint DLP, Microsoft Purview isn't aware that the edited content might still be sensitive and therefore takes no action.

In a best-case scenario, the end user encrypts the email with the sensitive file prior to sending it back to the correct recipient. Without endpoint DLP, however, Microsoft Purview can't ensure that an unintentional action with sensitive information is prevented. For contrast, let's look at the scenario for Organization two.



Organization 2 – CUI Authorized User on a Managed Laptop accessing CUI on the local device, using an E5/G5 license

The data flow in this scenario is as follows:

1. CUI is sent to a user's mailbox via an encrypted email, either directly from the DoD or from another partner.
2. The sensitive email arrives at the user's Mailbox and is ready to be synchronized with the user's Outlook application on their desktop.
3. The E5/G5 license that is assigned to the user comes with the full suite of Microsoft Purview capabilities, to include endpoint DLP, so Purview knows that this sensitive file should be tracked throughout its entire lifecycle, even when on the physical managed laptop.
4. Outlook syncs with Exchange Online and makes the encrypted email available to the user.
5. The user opens and reads the encrypted email and downloads the document to their laptop for further use.
6. The Authorized User manipulates the file and changes some of its contents in preparation to send it back to their customer and, because the E5/G5 license includes Endpoint DLP, Microsoft Purview is aware that the edited content might still be sensitive and can take appropriate action to protect that document.

This scenario considers that even well-trained users are still capable for user error and helps prevent unauthorized exposure of CUI data from happening in the first place. By considering the investment in a higher cost license, organization two got ahead of the risk and was able to put the correct safeguards in place to protect sensitive information.

If the decision-making criterion by any organization is primarily influenced by the cost of implementation, and if regulatory compliance isn't a requirement, then choosing to purchase a less expensive license might be a perfectly reasonable solution. Ardalyst is committed to helping all customers achieve a cybersecurity posture that doesn't impede organizational operations and is cost-effective for companies of all sizes. Should your team want to implement a solution based around a license that isn't aligned with the standard Tesseract offering, simply let us know! We can build you a Tesseract program that improves your security posture while also documenting any risks that may be introduced by a lack of feature availability.

It All Comes Down to Compliance

The Tesseract Program's primary goal is to assist clients in attaining CMMC compliance, enabling them to fulfill governmental criteria and secure contracts. It is tailored to align with your organization's need for a sensible compliance program without hindering the user experience. This is the reason Tesseract, built on the E5 licensing model, represents the most straightforward route to compliance for customers. Should you choose to utilize a non-standard license for your Tesseract program, Ardalyst is still committed to building the best possible cybersecurity and compliance program possible and will advise you on what possible pitfalls and risks you may be exposed to without utilizing one of the standard Tesseract license offerings.

Sign-Up for a Free Tesseract Trial

To help our customers make informed decisions about choosing a provider to help with their Cybersecurity program, we offer a free trial of Tesseract. During one of our trials, prospective customers will work with our Solutions Architects to scope their entire Enclave, determine the flow of CUI throughout their organization, and learn how Tesseract can meet their specific organizational needs through Tesseract Blocks™ selection.

Interested? Head over to https://tesseract.ardalyst.com/ and click "Start your free Trial" to get in touch with our team!

Document Control

Revision History

2023 SEPT 13	Date of original publication