Ontinue

Microsoft Security

GUIDE

Maximizing your Microsoft Licensing to Reduce Costs and Increase Security

Executive Summary

Most organizations have bought and deployed Microsoft products. However, all too often they do not realize that their license includes many more products that are not used to their fullest potential or are simply never used at all. This is commonly called shelfware: licenses that are owned but sit on a corporate shelf. This document details the critical security functionality which is included in the E5 license. With this knowledge, organizations can take advantage of the full range of capabilities that come with their Microsoft licenses. In doing so, IT and security leaders can reduce costs by eliminating unnecessary or redundant products.

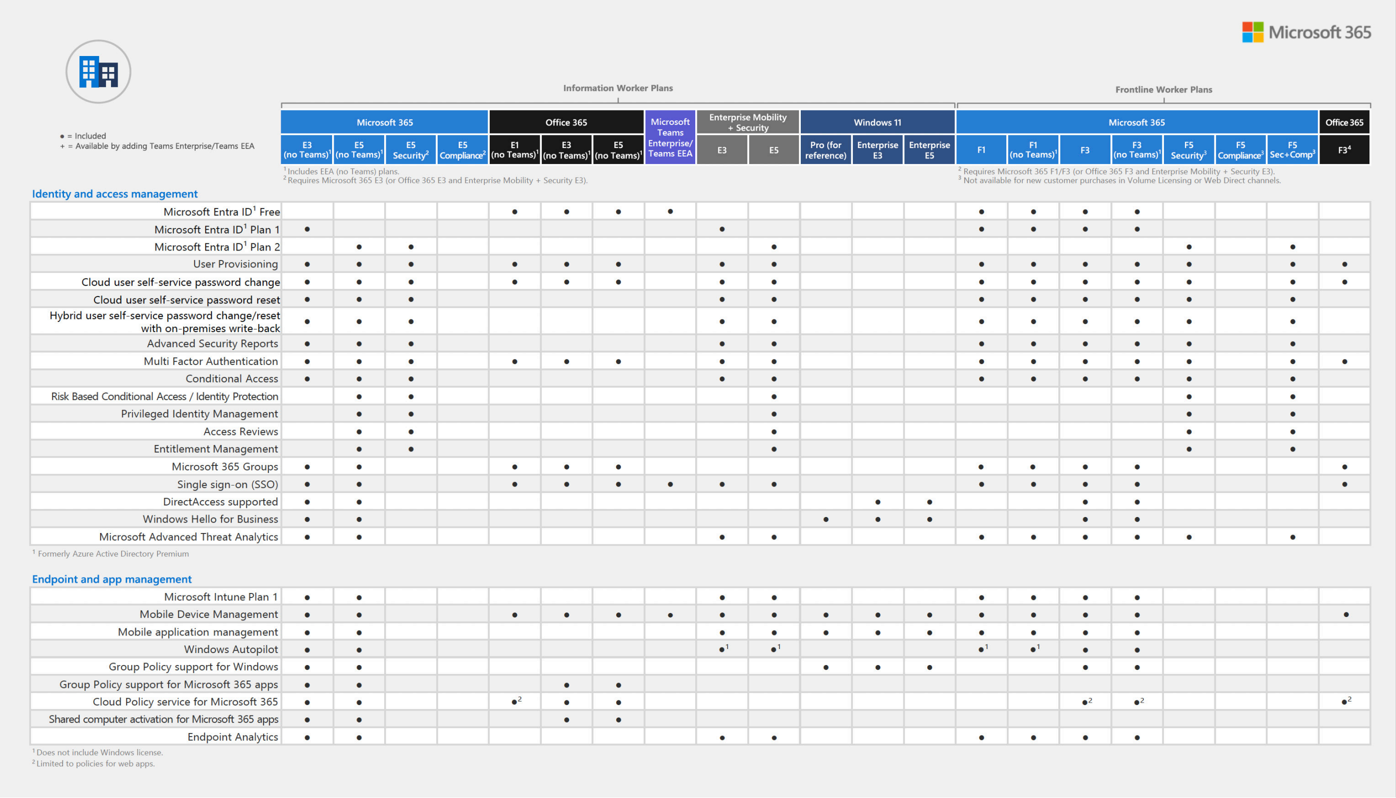
One important note is Microsoft frequently changes product names and associated licenses by adding or removing products or by simply creating new categories. As such, Ontinue frequently updates this guide with the latest publicly available information. This guide was last updated on November 25th, 2024.

To receive specific and detailed advice about your licenses and how you can reduce shelfware to save costs and improve on security, **Ontinue offers a free evaluation of your portfolio** and how to best maximize its use.

Table of Contents

The Basics of Microsoft Licensing

What's included in the licensing packs varies frequently. The following figures detail what identity and security products are included with which specific licenses as of September 1, 2024. This changes frequently so please contact Ontinue for current information.



Microsoft 365

● = Included
+ = Available by adding Teams Enterprise/Teams EEA

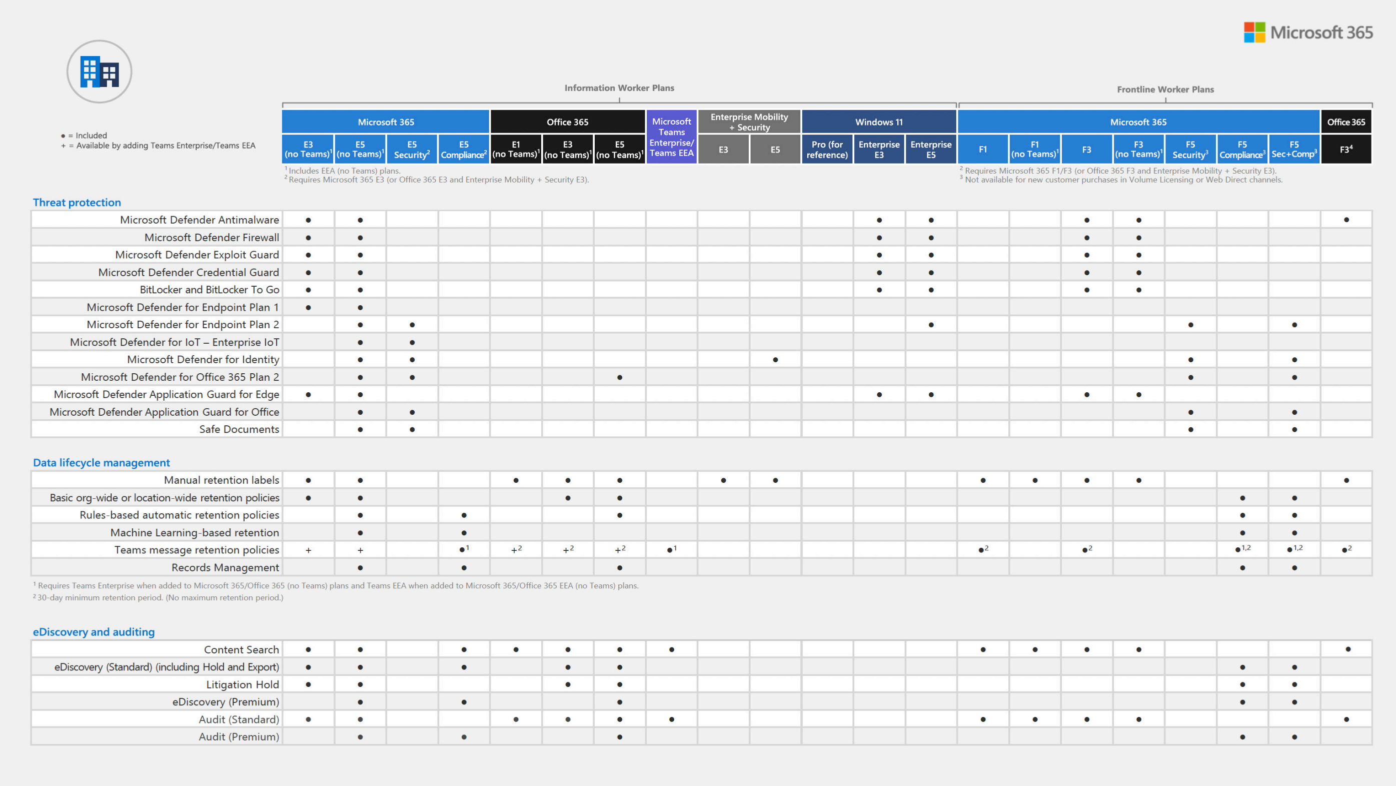
	Information Worker Plans													Frontline Worker Plans							
	Microsoft 365				Office 365			Microsoft Teams Enterprise/ Teams EEA	Enterprise Mobility + Security		Windows 11			Microsoft 365							Office 365
	E3 (no Teams)[1]	E5 (no Teams)[1]	E5 Security[2]	E5 Compliance[2]	E1 (no Teams)[1]	E3 (no Teams)[1]	E5 (no Teams)[1]		E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F1 (no Teams)[1]	F3	F3 (no Teams)[1]	F5 Security[3]	F5 Compliance[3]	F5 Sec+Comp[3]	F3[4]
Identity and access management																					
Microsoft Entra ID[1] Free					●	●	●	●						●	●	●	●				
Microsoft Entra ID[1] Plan 1	●								●					●	●	●	●				
Microsoft Entra ID[1] Plan 2		●	●							●								●		●	
User Provisioning	●	●	●		●	●	●		●	●				●	●	●	●	●		●	●
Cloud user self-service password change	●	●	●		●	●	●		●	●				●	●	●	●	●		●	●
Cloud user self-service password reset	●	●	●						●	●				●	●	●	●	●		●	
Hybrid user self-service password change/reset with on-premises write-back	●	●	●						●	●				●	●	●	●	●		●	
Advanced Security Reports	●	●	●						●	●				●	●	●	●	●		●	
Multi Factor Authentication	●	●	●		●	●	●		●	●				●	●	●	●	●		●	●
Conditional Access	●	●	●						●	●				●	●	●	●	●		●	
Risk Based Conditional Access / Identity Protection		●	●							●								●		●	
Privileged Identity Management		●	●							●								●		●	
Access Reviews		●	●							●								●		●	
Entitlement Management		●	●							●								●		●	
Microsoft 365 Groups	●	●			●	●	●							●	●	●	●				●
Single sign-on (SSO)	●	●			●	●	●	●	●	●				●	●	●	●				●
DirectAccess supported	●	●										●	●			●	●				
Windows Hello for Business	●	●									●	●	●			●	●				
Microsoft Advanced Threat Analytics	●	●							●	●				●	●	●	●	●		●	
Endpoint and app management																					
Microsoft Intune Plan 1	●	●							●	●				●	●	●	●				
Mobile Device Management	●	●			●	●	●	●	●	●	●	●	●	●	●	●	●				●
Mobile application management	●	●							●	●	●	●	●	●	●	●	●				
Windows Autopilot	●	●							●[1]	●[1]				●[1]	●[1]	●	●				
Group Policy support for Windows	●	●									●	●	●			●	●				
Group Policy support for Microsoft 365 apps	●	●				●	●														
Cloud Policy service for Microsoft 365	●	●			●[2]	●	●									●[2]	●[2]				●[2]
Shared computer activation for Microsoft 365 apps	●	●				●	●														
Endpoint Analytics	●	●							●	●				●	●	●	●				

[1] Includes EEA (no Teams) plans.
[2] Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise Mobility + Security E3).

[2] Requires Microsoft 365 F1/F3 (or Office 365 F3 and Enterprise Mobility + Security E3).
[3] Not available for new customer purchases in Volume Licensing or Web Direct channels.

[1] Formerly Azure Active Directory Premium

[1] Does not include Windows license.
[2] Limited to policies for web apps.



Microsoft 365

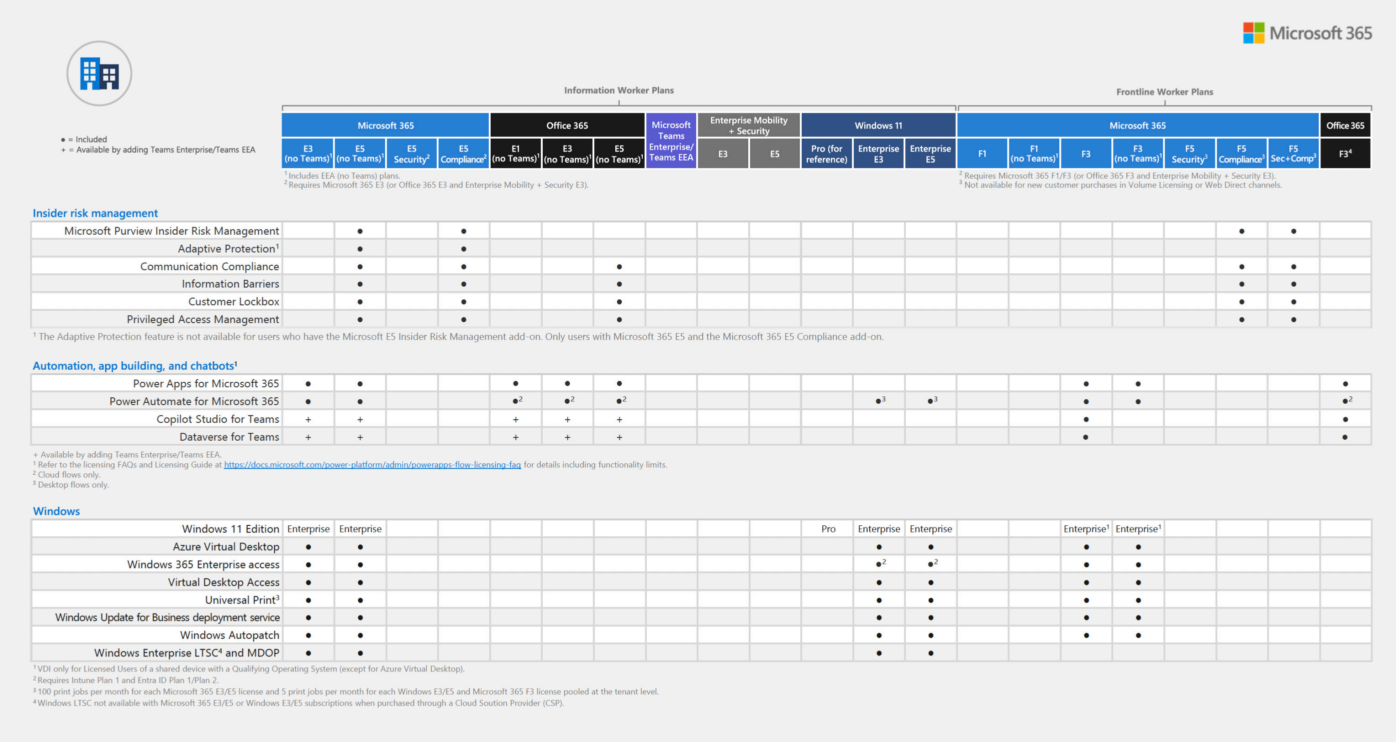
● = Included
+ = Available by adding Teams Enterprise/Teams EEA

	Information Worker Plans													Frontline Worker Plans							
	Microsoft 365				Office 365			Microsoft Teams Enterprise/ Teams EEA	Enterprise Mobility + Security		Windows 11			Microsoft 365							Office 365
	E3 (no Teams)[1]	E5 (no Teams)[1]	E5 Security[2]	E5 Compliance[2]	E1 (no Teams)[1]	E3 (no Teams)[1]	E5 (no Teams)[1]		E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F1 (no Teams)[1]	F3	F3 (no Teams)[1]	F5 Security[3]	F5 Compliance[3]	F5 Sec+Comp[3]	F3[4]
Threat protection																					
Microsoft Defender Antimalware	●	●										●	●			●	●				●
Microsoft Defender Firewall	●	●										●	●			●	●				
Microsoft Defender Exploit Guard	●	●										●	●			●	●				
Microsoft Defender Credential Guard	●	●										●	●			●	●				
BitLocker and BitLocker To Go	●	●										●	●			●	●				
Microsoft Defender for Endpoint Plan 1	●	●																			
Microsoft Defender for Endpoint Plan 2		●	●										●					●		●	
Microsoft Defender for IoT – Enterprise IoT		●	●																		
Microsoft Defender for Identity		●	●							●								●		●	
Microsoft Defender for Office 365 Plan 2		●	●				●											●		●	
Microsoft Defender Application Guard for Edge	●	●										●	●			●	●				
Microsoft Defender Application Guard for Office		●	●															●		●	
Safe Documents		●	●															●		●	
Data lifecycle management																					
Manual retention labels	●	●			●	●	●		●	●				●	●	●	●				●
Basic org-wide or location-wide retention policies	●	●				●	●												●	●	
Rules-based automatic retention policies		●		●			●												●	●	
Machine Learning-based retention		●		●															●	●	
Teams message retention policies	+	+		●[1]	+[2]	+[2]	+[2]	●[1]						●[2]		●[2]			●[1,2]	●[1,2]	●[2]
Records Management		●		●			●												●	●	
eDiscovery and auditing																					
Content Search	●	●		●	●	●	●	●						●	●	●	●				●
eDiscovery (Standard) (including Hold and Export)	●	●		●		●	●												●	●	
Litigation Hold	●	●				●	●												●	●	
eDiscovery (Premium)		●		●			●												●	●	
Audit (Standard)	●	●			●	●	●	●						●	●	●	●				●
Audit (Premium)		●		●			●												●	●	

[1] Includes EEA (no Teams) plans.
[2] Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise Mobility + Security E3).

[2] Requires Microsoft 365 F1/F3 (or Office 365 F3 and Enterprise Mobility + Security E3).
[3] Not available for new customer purchases in Volume Licensing or Web Direct channels.

[1] Requires Teams Enterprise when added to Microsoft 365/Office 365 (no Teams) plans and Teams EEA when added to Microsoft 365/Office 365 EEA (no Teams) plans.
[2] 30-day minimum retention period. (No maximum retention period.)



Microsoft 365

● = Included
+ = Available by adding Teams Enterprise/Teams EEA

	Information Worker Plans													Frontline Worker Plans							
	Microsoft 365				Office 365			Microsoft Teams Enterprise/ Teams EEA	Enterprise Mobility + Security		Windows 11			Microsoft 365							Office 365
	E3 (no Teams)[1]	E5 (no Teams)[1]	E5 Security[2]	E5 Compliance[2]	E1 (no Teams)[1]	E3 (no Teams)[1]	E5 (no Teams)[1]		E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F1 (no Teams)[1]	F3	F3 (no Teams)[1]	F5 Security[3]	F5 Compliance[3]	F5 Sec+Comp[3]	F3[4]
Insider risk management																					
Microsoft Purview Insider Risk Management		●		●															●	●	
Adaptive Protection[1]		●		●																	
Communication Compliance		●		●			●												●	●	
Information Barriers		●		●			●												●	●	
Customer Lockbox		●		●			●												●	●	
Privileged Access Management		●		●			●												●	●	
Automation, app building, and chatbots[1]																					
Power Apps for Microsoft 365	●	●			●	●	●									●	●				●
Power Automate for Microsoft 365	●	●			●[2]	●[2]	●[2]					●[3]	●[3]			●	●				●[2]
Copilot Studio for Teams	+	+			+	+	+									●					●
Dataverse for Teams	+	+			+	+	+									●					●
Windows																					
Windows 11 Edition	Enterprise	Enterprise									Pro	Enterprise	Enterprise			Enterprise[1]	Enterprise[1]				
Azure Virtual Desktop	●	●										●	●			●	●				
Windows 365 Enterprise access	●	●										●[2]	●[2]			●	●				
Virtual Desktop Access	●	●										●	●			●	●				
Universal Print[3]	●	●										●	●			●	●				
Windows Update for Business deployment service	●	●										●	●			●	●				
Windows Autopatch	●	●										●	●			●	●				
Windows Enterprise LTSC[4] and MDOP	●	●										●	●								

[1] Includes EEA (no Teams) plans.
[2] Requires Microsoft 365 E3 (or Office 365 E3 and Enterprise Mobility + Security E3).

[2] Requires Microsoft 365 F1/F3 (or Office 365 F3 and Enterprise Mobility + Security E3).
[3] Not available for new customer purchases in Volume Licensing or Web Direct channels.

[1] The Adaptive Protection feature is not available for users who have the Microsoft E5 Insider Risk Management add-on. Only users with Microsoft 365 E5 and the Microsoft 365 E5 Compliance add-on.

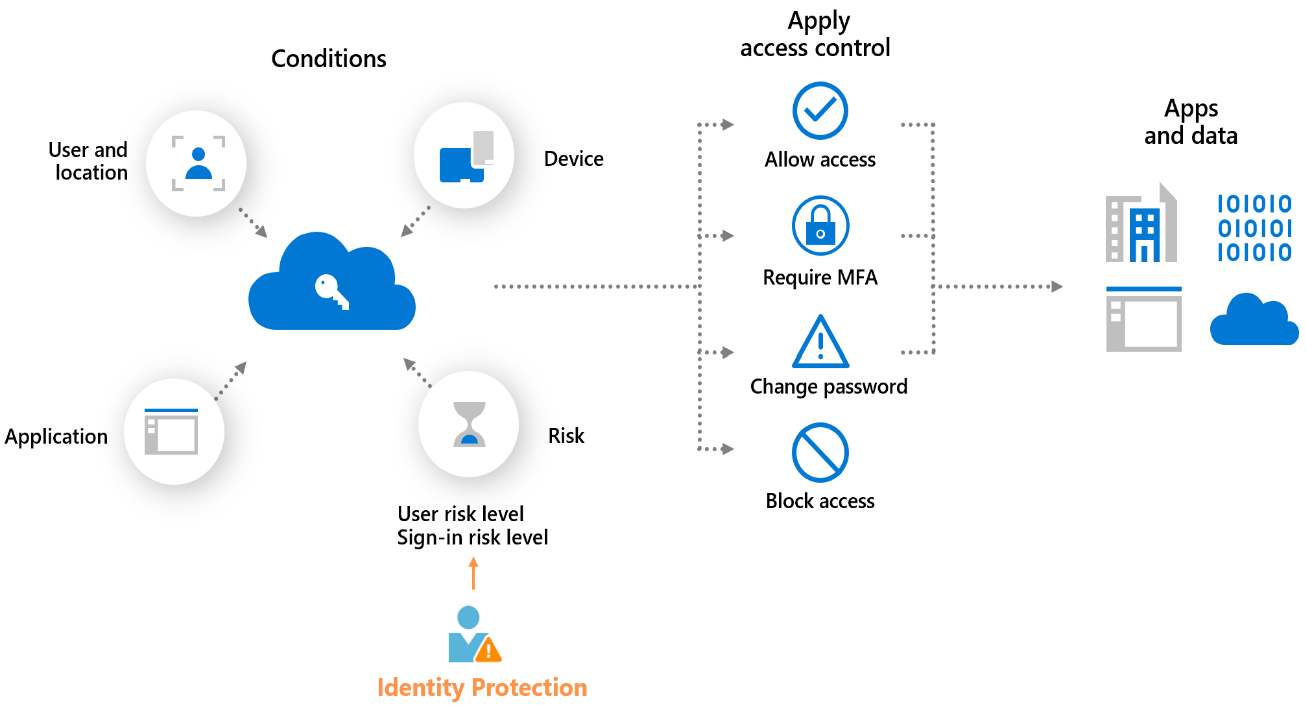
+ Available by adding Teams Enterprise/Teams EEA.
[1] Refer to the licensing FAQs and Licensing Guide at https://docs.microsoft.com/power-platform/admin/powerapps-flow-licensing-faq for details including functionality limits.
[2] Cloud flows only.
[3] Desktop flows only.

[1] VDI only for Licensed Users of a shared device with a Qualifying Operating System (except for Azure Virtual Desktop).
[2] Requires Intune Plan 1 and Entra ID Plan 1/Plan 2.
[3] 100 print jobs per month for each Microsoft 365 E3/E5 license and 5 print jobs per month for each Windows E3/E5 and Microsoft 365 F3 license pooled at the tenant level.
[4] Windows LTSC not available with Microsoft 365 E3/E5 or Windows E3/E5 subscriptions when purchased through a Cloud Soution Provider (CSP).

Identity Protection

Identity protection should matter most to all organizations. No matter how much money has been spent on firewall, anti-virus, and other security protection, if a hacker compromises an identity, they have full access to corporate resources. This is because the security infrastructure sees the hacker as the identity of the of the compromised user and authorizes the hacker with the exact same access. Today 80% of all hacking attempts are identity based.

Most organizations are already using Microsoft Entra ID (formerly called Azure AD) as their identity access management (IAM). User and password management has always been a headache for IT. To solve this problem, organizations implement Multi Factor Authentication (MFA) and conditional access which force users to use a second tool to authenticate – typically their mobile phone and look at additional variables such as device configuration and location. The problem with the E3 Entra ID is that although it now supports MFA and Conditional Access, it has no way to detect a compromised user. This shortcoming has historically forced IT to buy additional products such as Okta and Ping to augment the deficiencies of E3 Entra ID. With E5's enhanced capabilities, organizations can remove these products to save money.

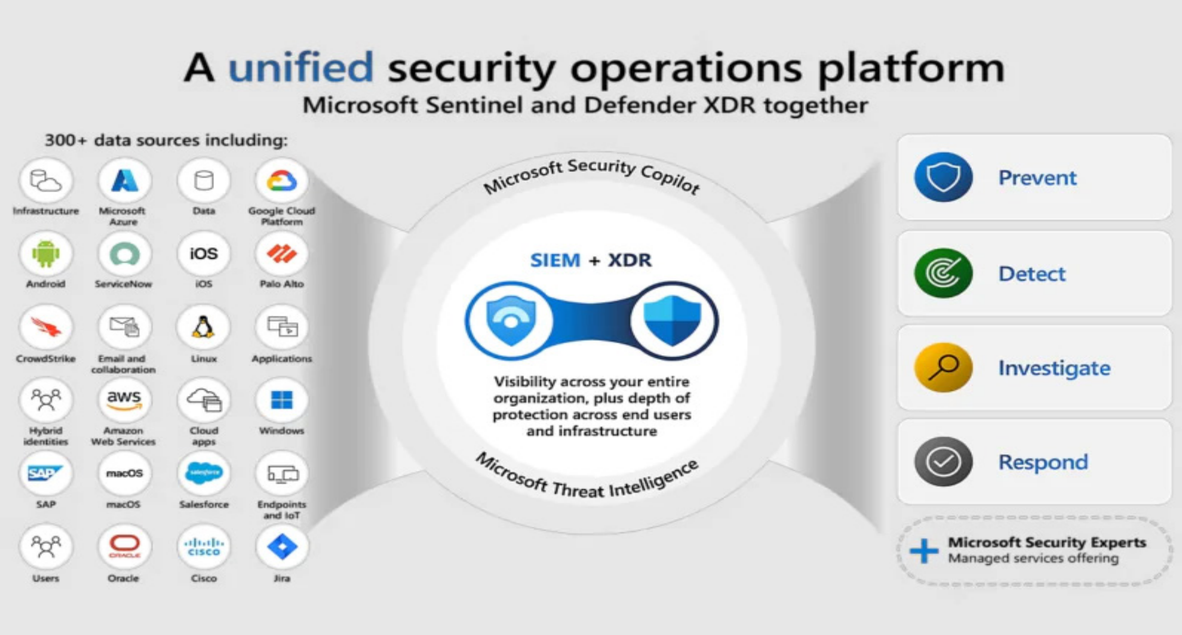


With E5, Entra ID includes Identity Protection which enables organizations to detect, investigate, and remediate identity-based risks. These identity-based risks can then be used for Risk Based Conditional Access. This enables the administrator to create access policies by configuring sign-in and user risk conditions and by choosing an access control method. During each sign-in, ID Protection sends the detected risk levels to Conditional Access, and the risk-based policies apply if the policy conditions are satisfied. In addition, with Privileged Identity Management organizations can manage, control, and monitor access to important resources in the organization.

Endpoint and Network Protection

Identity should matter most to an organization but a close second should be its endpoint and network protection. The problem with this protection is that it requires significant time and resources for an organization to deploy, maintain, and monitor it correctly. Gartner found that less than 10% of their large enterprise clients were capable of doing so, resulting in higher risk and more frequent security breaches. Many organizations only use desktop anti-virus. Running only desktop anti-virus on a user's device will detect common malware but it has no way to detect advanced threats such as ransomware or stop the spread of it across a network when an infection occurs.

The E3 license only includes basic desktop anti-virus. It does not include Endpoint Detection and Response (EDR). EDR allows for the correlation of all events across all the organization's endpoint devices including PC, MAC, and mobile. With all events reported to a single location, IT can now find and remediate against many more threats and respond to them on a corporate basis versus each device having to detect and respond to an event. To do this correctly, organizations need to have IT staff monitor the EDR system 24 hours a day and 7 days a week as most hacking occurs outside traditional business hours. Since most mid-size and large enterprises don't have these resources, organizations turn to Ontinue to deliver Managed Detection and Response (MDR) which then eliminates the need for any additional IT staff while providing government grade security protection.


A unified security operations platform
Microsoft Sentinel and Defender XDR together
300+ data sources including:
Infrastructure
Microsoft Azure
Data
Google Cloud Platform
Android
ServiceNow
iOS
Palo Alto
CrowdStrike
Email and collaboration
Linux
Applications
Hybrid identities
Amazon Web Services
Cloud apps
Windows
SAP
macOS
Salesforce
Endpoints and IoT
Users
Oracle
Cisco
Jira
Microsoft Security Copilot
SIEM + XDR
Visibility across your entire organization, plus depth of protection across end users and infrastructure
Microsoft Threat Intelligence
Prevent
Detect
Investigate
Respond
Microsoft Security Experts
Managed services offering

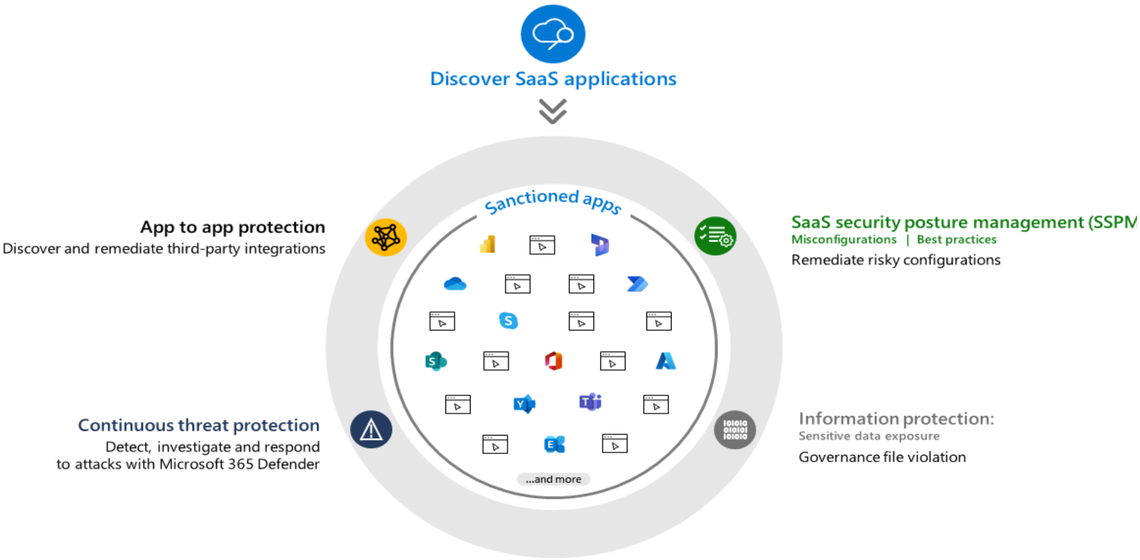
To add additional level of protection, it is now possible to combine the data received in an EDR system combined with all the data from network devices. This is known as Extended Detection and Response (XDR). With XDR, Ontinue can find and remediate against a greater number of threats more quickly across the entire organization. With a managed XDR solution, organizations can be confident that a much greater number of threats such as ransomware are detected and remediated against before becoming a much larger scale problem.

Data Loss Prevention (DLP) and Anti-SPAM protection

Ask any Chief Information Officer (CIO) if they care about security and most will say yes but it isn't their top priority. Ask the same CIO if they care about data loss, and all will say it is extremely important. As such they have deployed DLP and anti-SPAM tools such as Proofpoint, Digital Guardian, Mimecast, or Zscaler. With E5 these products are no longer required and can be removed to save money.
Microsoft Defender for Office enables the manual, default, automated, and mandatory sensitivity labelling in Office 365, Exchange, SharePoint, and OneDrive. It can also provide DLP for emails and files.
The anti-SPAM feature helps reduce junk email by using proprietary spam filtering (also known as content filtering) technologies to identify and separate junk email from legitimate email. The spam filtering learns from known spam and phishing threats and user feedback from Microsoft's consumer platform, Outlook.com.

Cloud Application Protection

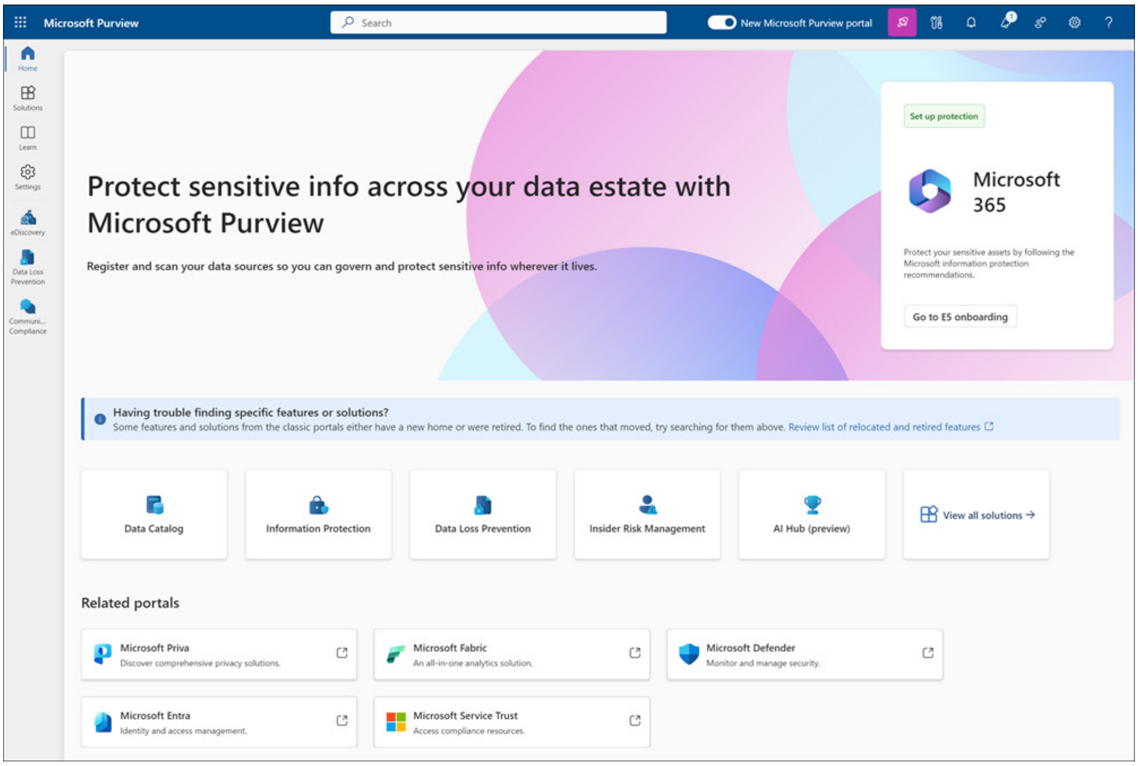
Driven in part by the global pandemic, organizations have accelerated their embrace of the cloud and increased their use of third-party cloud-based applications. The core problem for organizations with these applications is that IT no longer controls how data is stored, accessed or managed in the application and has far less control over user behaviors. For example, an employee might download all data to a local PC just before quitting. To combat this, technology known as a Cloud Access Security Broker (CASB) has become a common tool to control cloud applications.


Discover SaaS applications
Sanctioned apps
...and more
App to app protection
Discover and remediate third-party integrations
SaaS security posture management (SSPM
Misconfigurations | Best practices
Remediate risky configurations
Continuous threat protection
Detect, investigate and respond to attacks with Microsoft 365 Defender
Information protection:
Sensitive data exposure
Governance file violation

A CASB gives IT visibility into what and how applications are being used. It can discover, control, and configure apps to ensure employees are using trusted and compliant applications. It can protect data leakage by classifying and protecting sensitive information at rest, in use, and in motion. It also can control how the applications are accessed and under what conditions such as device, location, and time. CASBs can also regulate how apps interact with each other. Microsoft's CASB is called Defender for Cloud Apps and is included as part of the E5 license. With it you can remove your existing CASB such as Netskope, Zscaler, or Skyhigh CASB to reduce costs.

Compliance and Auditing

Ask a Chief Security Officer (CISO) which matters more security or compliance and all too frequently the answer is compliance due to the legal ramifications of being a non-compliant organization. Commonly deployed tools such as OneTrust, Resolver, and Vanta can now be replaced with an E5 license which includes Purview (a combination of Azure Purview and Microsoft 365 compliance solutions).



Protect sensitive info across your data estate with Microsoft Purview

Register and scan your data sources so you can govern and protect sensitive info wherever it lives.

Protect your sensitive assets by following the Microsoft information protection recommendations.

Having trouble finding specific features or solutions?
Some features and solutions from the classic portals either have a new home or were retired. To find the ones that moved, try searching for them above. Review list of relocated and retired features

Related portals

Microsoft Priva
Discover comprehensive privacy solutions.

Microsoft Fabric
An all-in-one analytics solution.

Microsoft Defender
Monitor and manage security.

Microsoft Entra
Identity and access management.

Microsoft Service Trust
Access compliance resources.

Purview helps organizations govern, protect, and manage data, wherever it lives. It provides integrated coverage and helps address fragmentation of data visibility across organizations. It helps safeguard and manage sensitive data across its lifecycle wherever it lives, providing governance of data and the ability to manage critical risks and regulatory requirements

Configuration, Deployment, and Management

It might sound surprising but the number one issue Ontinue sees with new clients is misconfigured security products. These misconfigurations range from basic policy errors to security rules in place that no current employee can fully explain. Oftentimes, misconfigurations result from otherwise sophisticated security teams not fully grasping the myriad ways in which disparate best-of-breed solutions need to integrate with one another.. Every security configuration and policy should be continuously audited and verified as current and correct to maximize both usability and security.

Deployment of a system as complex as Microsoft's Entra ID, Defender for Cloud Apps or Sentinel incorrectly can in the worst cases result in security breaches as well as potential outages of service. Deployment and configuration should be performed with the assistance of a certified professional who has experience with the products being deployed.

Contact Ontinue if you are interested in a **free security strategy review**.

.

Summary

Microsoft naming and licensing is confusing and changes regularly. This causes confusion as to what features and functionality are available resulting in the purchase of unnecessary software. To alleviate this problem, a few basic questions need to be answered to determine if an organization is getting the most from their products and Microsoft license:

1. What product licenses are owned?
2. What is deployed today?
3. Which of the 3rd party products that are currently deployed can be migrated to Microsoft?
4. How often are the products updated?
5. How many people are on staff supporting these products?
6. What hours are the products monitored and maintained? 24/7/365?
7. When was the last time an audit was performed of the infrastructure and security?

Knowing the answers to the above questions is often impossible. Ontinue can conduct a free audit of your licenses and infrastructure. **Please reach out to us** to schedule a consultation.

Gartner
Peer Insights™

Ontinue MXDR Helps You Get More out of Microsoft

The Ontinue ION Managed Extended Detection and Response (MXDR) service understands your Microsoft environment to give you more. We help you get greater efficiencies, continuous protection, and faster response times. All with an AI-Powered MXDR that provides superior protection.

We've intelligently aligned our platform and services with the industry-recognized leader in integrated security solutions—Microsoft. Our powerful Ontinue ION Platform was custom built for Microsoft's security and collaboration tools, including Defender, Sentinel, Azure, and Teams.

What Our Customer Have to Say

Read More Reviews >

> " The service is based on Sentinel and well designed into M365. They help you to enable and configure all required logs (if not done yet)."
>
> ★★★★★
>
> Head of IT Infrastructure - Energy and Utlities

> " Helped us undertstand and use the Microsoft enviornment that we had and never used its maximum capabilities"
>
> ★★★★★
>
> IT Security & Risk Management - IT Services

> " Resources will be allocated to Teams Bridge from Ontinue within 10-15mins. Recommendations from Advisors are top notch, and we were able to leverage our Microsoft E5 licenses better."
>
> ★★★★★
>
> IT Security & Risk Management - IT Services

> " We are a Microsoft shop and it utilizies these tools which works well for us. We also like the Teams integration."
>
> ★★★★★
>
> CIO - Consumer Goods

Ontinue

About Ontinue: Nonstop SecOps

Ontinue, a leading provider of AI-powered managed extended detection and response (MXDR) service, combines powerful proprietary AI with the industry's first collaboration with Microsoft Teams to continuously build a deep understanding of our customers' environments, informing how we prevent, detect, and respond to threats.