

Mastering Microsoft 365 Security Technologies

*Design and implement Microsoft security,
compliance, and identity*

Pramiti Bhatnagar



www.bpbonline.com

First Edition 2025

Copyright © BPB Publications, India

ISBN: 978-93-65892-871

All Rights Reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means or stored in a database or retrieval system, without the prior written permission of the publisher with the exception to the program listings which may be entered, stored and executed in a computer system, but they can not be reproduced by the means of publication, photocopy, recording, or by any electronic and mechanical means.

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true and correct to the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but the publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

To View Complete
BPB Publications Catalogue
Scan the QR Code:



Dedicated to

My little twins Aadi and Shivo

and

My parents

About the Author

Pramiti Bhatnagar is a seasoned professional with over twenty years of deep technical experience in Microsoft technologies, including Microsoft Entra, Microsoft Purview, Microsoft Defender, Microsoft 365 Windows, and Microsoft Endpoint Manager. Pramiti holds an honours degree in applied psychology from the University of Delhi and has numerous technical certifications, such as Certified Information Privacy Manager, Microsoft Certified: Cybersecurity Architect Expert, and Project Management Professional (PMP).

Currently, Pramiti serves as a Principal Product Manager for Microsoft Entra, primarily focusing on Copilot for Security and Entra External Identities. Pramiti has also held various roles at Microsoft, including Global Black Belt, Cloud Solution Architect, and Partner Technology Strategist.

About the Reviewers

- ❖ **Mahesh Kohli** is a product manager at Microsoft, holding CISM certification and Microsoft Certified Trainer credentials, with over 18 years of experience in the IT industry. He is currently focused on enhancing Microsoft Defender solutions, managing roadmaps, overseeing customer expectations, conducting market research, and providing strategic advice to security leadership to help customers strengthen their overall security posture.

Additionally, Mahesh specializes in delivering security-focused training sessions and webinars for both internal and external stakeholders. Before transitioning to a product management role, he served as a Premier Field Engineer, managing security and compliance solutions. In this role, he acted as a trusted advisor, conducting security assessments, health assessments, and workshops, while assisting customers with implementing security controls based on best practices. Outside of his professional role, Mahesh is an avid reader with a passion for classic novels, non-fiction and IT-related books.

- ❖ **Taresh Mehra** is a data protection and cyber security QA Engineer with over 18 years of experience in Edison, New Jersey. He specializes in backup and storage solutions, ransomware mitigation, and data indexing, ensuring data integrity in modern IT environments. His expertise spans AI/ML applications in data security, REST API testing, and cloud technologies.

Taresh has also shaped industry standards through his leadership in the Cloud Security Alliance and extensive contributions as a cyber security publication reviewer. His work advancing the field through IEEE conference papers and technical evaluations at major hackathons earned him the prestigious 2024 SILVER GLOBEE® AWARD for Cyber Security Professional of the Year. As both an IEEE Senior Member and RSA Fellow, he continues to influence the direction of enterprise security, helping define best practices and innovation benchmarks across the industry.

Acknowledgement

I would like to express my sincere gratitude to all those who contributed to the completion of this book.

First and foremost, I want to extend my heartfelt thanks to my family who have offered their unwavering support during the development of this book.

I also want to thank my colleagues, managers and mentors at Microsoft who have provided me with numerous opportunities to learn and grow and become capable of writing a book.

I am immensely grateful to BPB Publications for offering me the opportunity to share my knowledge. Their guidance and expertise in bringing this book to fruition has been incredible. Their support and assistance were invaluable in navigating the complexities of the publishing process.

I would also like to acknowledge the reviewers, technical experts, and editors who provided valuable feedback and contributed to the refinement of this book. Their insights and suggestions have significantly enhanced the quality of the book.

Finally, I want to express my gratitude to the readers who have shown interest in this book. Your support and encouragement have been deeply appreciated.

Thank you to everyone who has played a part in making this book a reality.

Preface

Security is top of mind for most organizations today. With the increasing number of cyber-attacks and shortage of skilled professionals, organizations are struggling to protect themselves from bad actors. At the same time, data is exploding making it even tougher for organizations to keep themselves and their data safe. M365 Security technologies provide end-to-end solutions for protecting and organisation's data, identities and applications.

This book covers end-to-end Microsoft security solutions. Section 1 of this book focuses on Microsoft's identity and access management solution Microsoft Entra. The five chapters in this section introduce Microsoft Entra and then guide the reader through implementation of Microsoft Entra and managing, protecting and governing identities using Microsoft Entra ID Governance, Microsoft Entra Privileged Identity Management. It also introduces the reader to Microsoft Entra Secure Services Edge, Microsoft's Zero Trust network access solution.

Section 2 focuses on protecting the organization against threats. It introduces Microsoft Defender XDR as Microsoft's extended detection and response solution. The chapters in this section shed light on how Microsoft Defender solutions can help protect devices, identities, M365 and non-M365 applications from external threats.

Section 3 shifts the focus on protecting data. This section explains how organizations can protect structured and unstructured data in Microsoft 365 and multi-cloud environments using Microsoft Purview Information Protection, prevent accidental or intentional data exfiltration using Microsoft Purview Data Loss Prevention, identify insider risks and manage regulatory compliance and privacy.

This book is designed to help experienced and novice security professionals become experts in administering and implementing Microsoft security solutions. Through practical examples, comprehensive explanations, hand-on labs, and a structured approach, this book aims to equip readers with a solid understanding of Microsoft security solutions. Whether you are a novice or an experienced learner, this book will serve as a valuable resource as you work towards advancing your cybersecurity career.

Chapter 1: Introduction to Microsoft Entra- This chapter introduces the Microsoft Entra product family. Microsoft Entra is a family of products that help organisations create and manage users and govern user access to applications and services. This chapter introduces the components of the Microsoft Entra and how they can help organisations address

their identity and access management requirements. It touches on the licensing options for each capability. This chapter explains how to create users using Microsoft Entra, the external collaboration capabilities using Microsoft Entra External ID. It also introduces new capabilities like Microsoft Entra Permissions Management, Microsoft Entra Verified ID and Global Secure Access.

Chapter 2: Implementing Identity- Many organizations worldwide use on-premises Active Directory for managing their identities. When they decide to move to the cloud, they would want to provide their end users with seamless access to both cloud and on-premises applications and resources. This chapter describes how these organizations can sync their on-premises Active Directory identities to Microsoft Entra ID securely so that users can use the same credentials to access both on-premises and cloud resources. It goes on to explain the password synchronization methods like password hash sync and pass-through authentication. It explains the password protection capabilities available in Microsoft Entra ID and how these can be extended to on-premises Active Directory. It also talks about setting up single sign-on for applications and end user self-service in Microsoft Entra ID.

Chapter 3: Identity Management- One of the main tasks of an identity and access management administrator is to make sure that the right system resources are accessible to the right users. This can be a challenging task since there are thousands of user identities in any organisation. This chapter introduces the group management features in Microsoft Entra ID to handle these identities and protect your organisation's resources effectively. It also covers the key concept of role based access control, which aids in understanding the other Microsoft capabilities explained in this book.

Chapter 4: Identity Protection- Identity is the key to access. Hence, a secure cloud deployment relies on a secure identity. Identity attacks have increased dramatically in recent years. Organisations need to enforce rigorous identity protection strategies while also offering a smooth work experience to their end users. This chapter describes the different identity protection features in Microsoft Entra ID like multifactor authentication, passwordless sign-in, unphishable credentials like passkeys. It also explains how Microsoft Entra ID Protection feature like risk-based conditional access policies can help prevent identity-based attacks.

Chapter 5: Identity Governance- Each identity goes through a lifecycle that needs to be managed from when a user joins the organisation to when they leave. The user access must be kept up to date across the joiner-mover-leaver scenario and this must be done efficiently. This chapter shows how to use entitlement management to give the users the right access that they need to do their job. Access reviews can be used to check the user's access to data

and applications regularly, making sure that they do not have more access than necessary to fulfil their job roles. Lastly, it explores how Privilege Identity Management can be used to give just in-time access to the users that have the most sensitive access.

Chapter 6: Microsoft Defender XDR- Organizations these days are exposed to a myriad of threats ranging from viruses, malware, phishing attacks, ransomware and more. They need to have effective threat protection strategies which include a combination of proactive prevention, real-time detection and rapid response. They need to deploy security solutions like firewalls, antivirus software, intrusion detection and protection systems to protect their networks, devices and data from potential harm. Microsoft Defender XDR is a suite of solutions that helps with detection, prevention, investigation and response of threats across endpoints, identities, email and applications. It provides integrated protection against sophisticated cyber-attacks.

Chapter 7: Protecting Identities- Many organizations still have big on-premises Active Directory infrastructures that can be compromised by attackers. Organizations must have tools to identify attacks against these identities and protect them from being stolen or abused. This chapter explores how Microsoft Defender for Identity helps organizations avoid breaches by spotting threats, investigating and responding to incidents. Microsoft Defender for Identity is a cloud-based solution that helps your SecOps teams provide a modern identity and threat detection solution across hybrid environments. It helps stop breaches, identify threats, examine dubious activities and react to attacks.

Chapter 8: Protecting Endpoints- In today's hybrid working environment, users are using a multitude of devices from a multitude of locations. Gone are the days when users used to work only from their offices safe behind the corporate firewall. This exposes user endpoints to threats like never before. The attackers are also becoming very sophisticated. Organizations need modern and intelligent tools to protect their users' devices from bad actors. Microsoft Defender from Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. Coupled with Microsoft Defender Vulnerability Management, it offers proactive protection and visibility into the vulnerabilities in the environment and provides recommendations to strengthen the security posture. Organizations today also use operational technology and Internet of Things devices. It is important for an organization to gain visibility into these devices and the threats surrounding them. Microsoft Defender for IoT provides device discovery and threat protection services for OT and IoT networks across cloud, on-premises and air-gapped infrastructure.

Chapter 9: Protecting M365 Apps- Many organisations are now shifting to cloud-based services. Microsoft is the world's top collaboration SaaS provider. Most organisations

store a lot of data in the M365 cloud, Exchange Online, SharePoint Online, OneDrive for Business and Teams. Attackers try to compromise these applications using different methods like phishing and spoofing. This chapter explains Exchange Online Protection and Microsoft Defender for Office 365 and their roles in defending, detecting, investigating and responding to attacks aimed at your M365 environment.

Chapter 10: Protecting Non-Microsoft Cloud Apps- Today, end users have access to a wide variety of SaaS applications that help them work more efficiently. However, this poses a major challenge for Security Administrators as they might not have visibility of which applications are in use, their security posture and how they are being used. These applications introduce new threat vectors for an organization in terms of cyber-attacks and more avenues for data exfiltration. This chapter explores Microsoft Defender for Cloud Apps and how it can help identify the use of Shadow IT, approve and disapprove applications and ultimately track the usage of those applications to protect your organisation's data and assets.

Chapter 11: Security Management Using Microsoft Sentinel- This chapter introduces the concepts of **Security Incident and Event Monitoring (SIEM)** and **Security Orchestration Automation and Response (SOAR)**. It then goes on to introduce Microsoft Sentinel as Microsoft's cloud-native SIEM and SOAR solution. It explains how Microsoft Sentinel helps SOC analysts manage hundreds of alerts daily, preventing critical security incidents. The chapter covers the setup of Microsoft Sentinel, connecting data sources, handling incidents, creating playbooks, and automating responses. It also highlights the integration with Microsoft solutions and non-Microsoft clouds, the use of Threat Intelligence, and the creation of visual reports.

Chapter 12: Protect and Govern Sensitive Data- Data is the most valuable resource that an organisation has. In today's world data is everywhere and organisations need tools to find the sensitive data, safeguard it from unauthorized access and manage it through its lifecycle. This chapter explores Microsoft Purview Information Protection and how it can be used to find and protect sensitive content; Microsoft Purview Data Loss Protection to prevent sensitive information from being shared with unauthorized parties. It also explains how Microsoft Purview Data Lifecycle Management and Records Management can be used to govern the life cycle of the data from the time it was created till when it is securely disposed of.

Chapter 13: Managing Insider Risks- Data does not move itself, people move data. To understand the user intent behind moving the data, we need to know not only how, but also why the data moved. This chapter explains Microsoft Purview Insider Risk Management and Microsoft Purview Communication Compliance solutions to set up policies that can

track user behaviour over time and prevent insiders from leaking sensitive content. It also covers Adaptive Protection and how to gather forensic evidence for investigations.

Chapter 14: Managing eDiscovery Cases- When something goes wrong, an organization might need to show proof to regulators, legal authorities or their own investigators. This chapter introduces Microsoft Purview eDiscovery as the tool investigate such incidents by creating cases, assigning custodians and conducting searches across the organization to find the data that is most important for the investigation. It can examine and filter the data in-place to save time and money when doing an eDiscovery investigation.

It is also important for organizations to be aware of user and admin activity happening in their environment. Microsoft Purview Audit serves as a comprehensive record of system activities, user actions, and changes to data. This chapter explains it can aid in investigating and resolving incidents of unauthorized access, data breaches, or other security violations.

Chapter 15: Managing Regulatory Compliance- Most organizations are subject to more than one industry or government regulation that they must adhere to. Remaining compliant with these regulations is an arduous task. Organizations invest a lot of time and money to achieve this. Microsoft Purview Compliance Manager is a simple SaaS based solution that helps organizations remain compliant with the regulations by providing easy to use templates and step-by-step guidance to meet the regulation requirements.

Chapter 16: Managing Privacy- Many organizations have a lot of PII stored in unstructured data in different locations. This PII can be mishandled and lead to serious consequences like loss of customer trust and reputation. Microsoft Priva helps a privacy officer to find out where PII is stored, how it moves within the organization and how old it is. It also empowers the user to make smart data handling decisions by providing timely trainings. Microsoft Priva Subject Rights Request is the tool that helps organizations to quickly answer Data Subject Requests. This chapter also introduces Preview capabilities of Consent management, Tracker scanning and Privacy assessments.

Chapter 17: Best Practices- The concluding chapter of this book takes the reader through identity, security and compliance best practices that further enhance the understanding of the concepts. This also enables administrators to take best decisions based on their organization business use cases and requirements.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the *Coloured Images* of the book:

<https://rebrand.ly/am8kms4>

The code bundle for the book is also hosted on GitHub at

<https://github.com/bpbpublications/Mastering-Microsoft-365-Security-Technologies>.

In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at

<https://github.com/bpbpublications>. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At **www.bpbonline.com**, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

<https://discord.bpbonline.com>



Table of Contents

1. Introduction to Microsoft Entra	1
Introduction.....	1
Structure.....	1
Objectives.....	2
Microsoft Entra ID	2
<i>Licensing</i>	2
<i>Creating new Entra ID tenant</i>	3
<i>Prerequisites</i>	3
<i>Steps</i>	3
<i>Adding custom domain name in Entra ID</i>	5
<i>Common verification issues</i>	6
Microsoft Entra ID Governance.....	7
<i>Governing user accounts</i>	7
<i>Governing privileged accounts</i>	8
<i>Licensing</i>	8
Microsoft Entra External ID	9
<i>Pricing</i>	9
Microsoft Entra Permissions Management.....	11
<i>Prerequisites</i>	11
<i>Set-up Permissions Management</i>	11
<i>Onboard your multi-cloud environment</i>	12
<i>Set the controller</i>	12
<i>Configure data collection</i>	12
Microsoft Entra Workload ID	13
<i>Key scenarios</i>	14
Microsoft Entra Verified ID	14
<i>Understanding verifiable credentials</i>	14
<i>Verifiable credentials in action</i>	14
Global Secure Access.....	15
<i>Microsoft Entra Internet Access</i>	15
<i>Microsoft Entra Private Access</i>	16

Conclusion.....	16
Multiple choice questions.....	16
<i>Answer key</i>	17
2. Implementing Identity	19
Introduction.....	19
Structure.....	19
Objectives.....	20
Determine identity model	20
Cloud-only identity	21
<i>Creating and managing user accounts</i>	21
<i>One-by-one</i>	21
<i>Bulk import</i>	23
<i>Windows PowerShell</i>	24
Hybrid identity	25
Microsoft Entra Cloud Sync.....	26
<i>Deployment scenarios</i>	26
<i>Key components</i>	27
<i>Installing Microsoft Entra Cloud Sync</i>	27
<i>Common installation problems</i>	30
Microsoft Entra Connect	30
<i>Installation requirements</i>	31
<i>Connect server requirements</i>	32
<i>SQL server requirements</i>	33
<i>Installation types</i>	33
<i>Installation steps</i>	33
<i>Object filtering</i>	34
<i>Microsoft Entra Connect Health</i>	35
Authentication methods.....	35
<i>Password hash sync</i>	35
<i>Important considerations</i>	37
<i>Selective password hash synchronization</i>	38
<i>Setup password hash synchronization</i>	41
<i>Pass-through authentication</i>	41
<i>Configuration pre-requisites</i>	42

<i>Enable Pass-through authentication</i>	43
<i>Test Pass-through authentication</i>	43
<i>Federated authentication</i>	43
<i>Requirements</i>	44
<i>Enable Federation in Microsoft Entra Connect</i>	45
<i>Choosing right method</i>	45
<i>Password protection</i>	47
<i>Global banned password list</i>	47
<i>Custom banned password list</i>	47
<i>Password spray attacks</i>	48
<i>Supporting on-premises</i>	48
<i>Single sign-on</i>	48
<i>End user self-service</i>	49
<i>Self-service password reset</i>	49
<i>Self-service group management</i>	51
<i>Self-service application assignment</i>	52
<i>Conclusion</i>	53
<i>Multiple choice questions</i>	53
<i>Answer key</i>	54
3. Identity Management	55
<i>Introduction</i>	55
<i>Structure</i>	55
<i>Objectives</i>	56
<i>User and group management</i>	56
<i>Inviting guest user</i>	56
<i>Deleting user account</i>	59
<i>Creating new group</i>	59
<i>Role-assignable groups</i>	60
<i>Protecting role-assignable groups</i>	61
<i>PIM and role-assignable groups</i>	61
<i>Adding members to group</i>	62
<i>Nested group</i>	63
<i>Group-based licensing</i>	63
<i>Assigning licenses to user or group</i>	64

Microsoft Entra roles	66
<i>View role definitions</i>	66
<i>View role assignments</i>	68
<i>Viewing assignments for a role</i>	68
<i>Viewing role assignments for an application</i>	69
<i>Viewing role assignments for a user</i>	70
<i>Viewing role assignments for a group</i>	70
<i>Creating custom roles</i>	71
<i>Assigning roles to users and groups</i>	72
<i>Assigning roles to users</i>	72
<i>Assigning roles to groups</i>	73
Administrative units	74
<i>Restricted management administrative units</i>	75
<i>Creating administrative unit</i>	76
<i>Adding members to administrative unit</i>	77
<i>Dynamically add members to administrative unit</i>	78
<i>Assigning administrative roles to administrative unit</i>	79
Protected actions	82
<i>Prerequisites</i>	83
<i>Configuring protected actions</i>	83
Conclusion	85
Multiple choice questions	85
<i>Answer key</i>	86
4. Identity Protection	87
Introduction	87
Structure	87
Objectives	88
Understanding authentication methods	88
<i>Enabling authentication methods</i>	89
Understanding Conditional Access	90
Configuring combined registration	92
Multi-factor authentication	94
<i>Prerequisites</i>	94
<i>Enabling MFA in Microsoft Entra</i>	94
<i>Security defaults</i>	94

MFA registration policy	96
Microsoft Authenticator app	97
OATH software token	100
OATH hardware token	101
Phone options.....	103
Passwordless sign-in	103
Passkey authentication	103
Enable passkeys	104
Registering passkey	105
Sign-in with passkey	105
Temporary Access Pass.....	106
Creating Temporary Access Pass	107
Using TAP.....	109
Microsoft Authenticator app	109
Windows Hello for Business.....	111
Windows Hello for Business deployment	113
Trust types.....	113
Operating system requirements	114
Authentication	114
Device registration	115
Multi-factor authentication	116
Key registration	116
Directory synchronization	116
Device configuration	116
Licensing requirements	116
Microsoft Entra ID Protection.....	117
Understanding risk conditions	117
Risk-based access policies.....	119
Investigate and remediate risks.....	120
Risky users	120
Risky sign-ins.....	121
Risky workload identities	122
Risk detections.....	123
Conclusion.....	123

Multiple choice questions.....	124
<i>Answer key</i>	124
5. Identity Governance.....	125
Introduction.....	125
Structure.....	125
Objectives.....	126
Microsoft Entra ID Governance.....	126
<i>Identity and access lifecycle</i>	126
<i>Privileged access lifecycle</i>	127
Entitlement management	127
Access packages.....	127
Catalog.....	128
Connected organizations.....	128
Add a connected organisation	129
Roles in entitlement management	131
Configure entitlement management	131
Delegate to catalog creator	132
Allow access to Microsoft Entra portal.....	132
Creating catalog	133
Add additional roles	134
Add resources to catalog.....	134
Add resource attributes in the catalog.....	135
Create an access package	136
Request access.....	140
Approve access.....	141
Validate that worked.....	142
Manually assigning an access package	142
Auto assigning users to an access package	143
Licensing requirements.....	145
Access reviews	145
Multi-stage reviews	146
Guest user reviews.....	148
Groups and applications	148
Creating access review.....	149

Review access	152
Access packages.....	153
Creating access review.....	153
Review access	154
Microsoft Entra roles and Azure resource roles	154
Creating an access review.....	155
Review access	156
License requirements.....	156
Privileged Identity Management	156
PIM for Microsoft Entra roles	157
Prepare the role for PIM.....	158
Assigning role	159
Activating role.....	160
Approve assignment.....	161
Extend assignment	161
PIM for Azure resource roles.....	162
Select Azure resources	162
Preparing role for PIM.....	163
Assigning role	163
PIM for groups	164
Bring groups under PIM	165
Preparing group for PIM	166
Assigning role	166
Auditing.....	167
Licensing requirements.....	167
Lifecycle workflows	168
Components	168
Tasks	169
Triggers.....	169
Scope.....	169
Creating lifecycle workflow.....	169
Testing workflow.....	172
Licensing requirements.....	173
Conclusion.....	173

Multiple choice questions.....	173
<i>Answer key</i>	174
6. Microsoft Defender XDR	175
Introduction.....	175
Structure.....	175
Objectives.....	176
Microsoft Defender XDR.....	176
<i>Licensing requirements</i>	177
<i>Roles required</i>	177
<i>Getting started</i>	179
<i>Security Copilot in Defender</i>	180
<i>Incident investigation and response</i>	181
<i>Automated investigation and response</i>	184
<i>Prerequisites</i>	184
<i>Configure devices</i>	185
<i>Understand AIR</i>	186
<i>Automatic attack disruption</i>	188
<i>Prerequisites</i>	189
<i>Exclude users from automated response</i>	190
<i>Understand automatic attack disruption</i>	190
<i>Deception capability</i>	191
<i>Prerequisites</i>	191
<i>Turning on deception capability</i>	192
<i>Advanced hunting</i>	192
<i>Guided mode</i>	193
<i>Advanced mode</i>	193
<i>Security Copilot in advanced hunting</i>	194
<i>Threat analytics</i>	195
<i>Microsoft Defender Experts</i>	195
Microsoft Secure Score	196
Conclusion.....	198
Multiple choice questions.....	199
<i>Answer key</i>	199

7. Protecting Identities	201
Introduction.....	201
Structure.....	201
Objectives.....	202
Microsoft Defender for Identity	202
<i>License requirements.....</i>	<i>204</i>
<i>Roles in MDI</i>	<i>205</i>
System requirements.....	205
Network requirements.....	206
Installing MDI sensor.....	207
Post installation steps.....	209
<i>Collect events</i>	<i>209</i>
<i>Review current configuration</i>	<i>209</i>
<i>Configure auditing on domain controllers.....</i>	<i>209</i>
<i>Advanced Audit Policy</i>	<i>210</i>
<i>Configure NTLM auditing</i>	<i>211</i>
<i>Domain object filtering</i>	<i>211</i>
<i>Configure auditing on AD FS.....</i>	<i>212</i>
<i>Configure auditing on AD CS</i>	<i>212</i>
<i>Configure auditing on configuration container</i>	<i>213</i>
<i>Directory Services Account.....</i>	<i>214</i>
<i>Action accounts</i>	<i>215</i>
MDI domain controllers	217
Investigate and respond	217
<i>Investigate users</i>	<i>217</i>
<i>Investigating lateral movement</i>	<i>219</i>
<i>Working with security alerts</i>	<i>221</i>
Remediation	223
Identity security posture	223
<i>Dashboards and reports</i>	<i>223</i>
<i>ITDR dashboard</i>	<i>223</i>
<i>Viewing health issues.....</i>	<i>224</i>
<i>Microsoft Defender for Identity reports.....</i>	<i>225</i>
Conclusion.....	225

Multiple choice questions.....	226
<i>Answer key</i>	226
8. Protecting Endpoints.....	227
Introduction.....	227
Structure.....	228
Objectives.....	228
Microsoft Defender for Endpoint.....	228
<i>Data storage and privacy</i>	229
<i>Licensing</i>	230
<i>Deploy MDE</i>	231
<i>Prerequisites</i>	231
<i>Define deployment architecture</i>	233
<i>Selecting deployment tool</i>	233
<i>Onboard devices</i>	234
Configure MDE settings	235
<i>General</i>	235
<i>Advanced features</i>	235
<i>Licenses</i>	238
<i>Email notifications</i>	238
<i>Permissions</i>	239
<i>Rules</i>	239
<i>Indicators</i>	239
<i>Web content filtering</i>	239
<i>Automation uploads</i>	240
<i>Automation folder executions</i>	241
Configuration management.....	241
<i>Enforcement scope</i>	241
Device discovery	242
Detect and protect.....	244
<i>Tamper resiliency</i>	244
<i>Tamper protection on Windows</i>	245
<i>Tamper protection on MacOS</i>	246
<i>Attack surface reduction</i>	246
<i>Next generation protection</i>	248

Cloud delivered protection.....	250
Real time protection.....	251
Investigate and respond	252
Remediation action on devices	252
Remediation action on files	254
Microsoft Defender Vulnerability Management	255
Licensing.....	256
Operating system requirements.....	256
Inventories	257
Working with Vulnerability Management	257
Microsoft Defender for IoT	259
Licensing.....	260
Permissions.....	261
Getting started	262
Device inventory.....	262
Alerts	263
Conclusion.....	264
Multiple choice questions.....	264
Answer key	265
9. Protecting M365 Apps.....	267
Introduction.....	267
Structure.....	267
Objectives.....	268
Exchange Online Protection.....	268
Protection policies in EOP.....	269
Anti-malware	270
Anti-spam.....	270
Anti-phishing	273
Zero-hour auto purge.....	274
Microsoft Defender for Office 365.....	274
Safe Attachments in email	275
Safe Attachments in SharePoint, OneDrive and Teams.....	276
Safe Links for emails	277
Safe Links for Teams	278

<i>Safe Links for Office apps</i>	279
Threat protection policies.....	280
<i>Preset security policies</i>	280
<i>Built-in protection</i>	280
<i>Strict and standard</i>	281
<i>Custom policies</i>	281
<i>Policy order</i>	282
Deploy email protection	282
<i>Configuring email authentication</i>	283
<i>Assign permissions to admins</i>	285
<i>Setup priority accounts</i>	285
<i>Enable user reported messages</i>	286
<i>Block and allow entries</i>	288
<i>Train end users</i>	289
Detect threats.....	292
<i>Alert policies</i>	293
<i>Message trace</i>	295
<i>Quarantine</i>	296
<i>Quarantine policies</i>	296
<i>Quarantine notifications</i>	299
<i>Advanced delivery</i>	300
<i>Audit logs</i>	301
<i>Email and collaboration reports</i>	301
Investigate and respond	302
<i>Explorer</i>	302
<i>Campaigns</i>	303
<i>Investigate user reported messages</i>	304
<i>Admin submissions</i>	304
<i>Spoof intelligence insights</i>	304
<i>Impersonation insights</i>	306
<i>Mailbox intelligence</i>	307
<i>Threat tracker</i>	307
Remediate	308
<i>Business email compromise</i>	308

<i>Illicit consent grants</i>	309
<i>Malicious email messages</i>	309
<i>Custom form injections</i>	309
<i>Office rules</i>	310
Conclusion	310
Multiple choice questions	310
<i>Answer key</i>	311
10. Protecting Non-Microsoft Cloud Apps	313
Introduction	313
Structure	313
Objectives	314
Microsoft Defender for Cloud Apps	314
<i>Licensing</i>	316
<i>Roles</i>	316
Network requirements	317
Set up MDCA	318
<i>User groups</i>	318
<i>Scoped deployment</i>	319
Cloud discovery	320
<i>MDE integration</i>	321
<i>Secure Web Gateway integration</i>	322
<i>Configure log collector</i>	323
<i>View discovered apps</i>	323
<i>Identify risky apps</i>	324
<i>Block risky apps</i>	327
Connect apps	329
Working with policies	330
Conditional Access app control	333
<i>Access policy</i>	335
<i>Session policy</i>	336
Microsoft Purview Information Protection	338
<i>Prerequisites</i>	338
<i>Considerations</i>	338
<i>Enable integration</i>	338

<i>Manually apply labels</i>	339
<i>Automatically apply labels</i>	339
Microsoft Sentinel.....	340
Additional integrations	341
Investigate and respond	341
<i>Investigate Cloud Apps</i>	341
<i>Investigate files</i>	342
<i>Investigate users</i>	343
<i>Behaviors</i>	344
<i>Manage OAuth apps</i>	345
App governance.....	346
<i>Licensing</i>	347
<i>Roles</i>	347
<i>Get started</i>	347
<i>Investigate apps</i>	348
<i>App policies</i>	348
<i>Investigate alerts</i>	349
Conclusion.....	349
Multiple choice questions.....	350
<i>Answer key</i>	350
11. Security Management Using Microsoft Sentinel	351
Introduction.....	351
Structure.....	351
Objectives.....	352
Understanding SIEM and SOAR.....	352
Microsoft Sentinel.....	353
Understanding solutions and content.....	356
Repositories	357
Plan for Microsoft Sentinel.....	358
<i>Prerequisites</i>	358
<i>Roles and permissions</i>	358
<i>Microsoft Sentinel roles</i>	358
<i>Azure roles</i>	359
<i>Log Analytics roles</i>	360
Costs.....	360

Deploy Microsoft Sentinel.....	361
<i>Out-of-the-box data connectors</i>	361
<i>Custom connectors</i>	363
<i>Set up analytics rules</i>	364
<i>Scheduled analytics rules</i>	364
<i>Near-real-time analytics rules</i>	366
<i>Anomaly detection rules</i>	366
<i>Set up automation rules</i>	367
<i>Set up playbooks</i>	369
<i>Set up watchlists</i>	370
Visualize data	373
<i>Workbooks</i>	374
<i>Power BI</i>	375
Hunt threats.....	375
<i>Livestreams</i>	379
<i>Notebooks</i>	380
Create and investigate incidents	380
Conclusion.....	381
Multiple choice questions.....	382
<i>Answer key</i>	382
12. Protect and Govern Sensitive Data	383
Introduction.....	383
Structure.....	383
Objectives.....	384
Microsoft Purview	384
<i>Role-based access control</i>	385
<i>Adaptive scopes</i>	386
Data security and governance	387
<i>Sensitive information types</i>	388
<i>Built in SITs</i>	389
<i>Named entity SITs</i>	389
<i>Custom SITs</i>	389
<i>Document fingerprinting</i>	390
<i>Exact data match SIT</i>	390
<i>Trainable classifiers</i>	390

Know your data	391
Microsoft 365 cloud	391
On-premises	392
Pre-requisites	393
Configuring scanner settings	394
Installing scanner	395
Running scanner	396
Protect your data	396
Sensitivity labels	397
Label settings	398
Basic details	398
Scope	399
Protection settings	399
Access control settings	399
Content marking	401
Microsoft Teams meetings and chats	401
Auto-labelling for files and emails	401
Groups and sites	402
Schematized data assets	402
Label order	403
Publish labels	403
Auto labelling content	405
Prevent data loss	408
DLP for Exchange	409
DLP for SharePoint and OneDrive	410
Teams DLP	411
Endpoint DLP	412
Endpoint DLP settings	413
Just-in-time protection	415
DLP for non-Microsoft applications	415
DLP for on-premises repositories	416
Creating DLP policy	416
DLP alerts	416
Govern your data	417
Retention policy	418

Retention labels.....	420
File plan	421
Marking items as records	421
Label policies	423
Licensing.....	425
Principles of retention.....	426
Managing data disposition	426
Gain visibility.....	428
Conclusion.....	429
Multiple choice questions.....	430
Answer key	430
13. Managing Insider Risks	431
Introduction.....	431
Structure.....	431
Objectives.....	432
Microsoft Purview Insider Risk Management	432
Getting started	432
Get permissions	433
Enable auditing	433
Enable analytics	433
Configure connectors.....	434
Configure Insider Risk Management settings.....	434
Data sharing.....	434
Policy indicators.....	435
Detection groups	436
Global exclusions.....	436
Inline alert customization	436
Intelligent detections	437
Microsoft Teams	437
Notifications	438
Policy timeframes	438
Power Automate flows	438
Priority physical assets.....	439
Priority user groups	439
Privacy	439

Additional configuration.....	439
Creating insider risk management policy.....	439
Investigate activities and manage alerts.....	441
User activity reports.....	441
Alert dashboard	443
Audit log.....	446
Forensic evidence	446
Licensing and billing.....	447
Configure your environment.....	447
Configure supported devices	448
Configure settings	448
Create a policy	448
Define and approve users	449
Viewing captured clips	450
Adaptive protection.....	450
Permissions	452
Configuring Adaptive Protection.....	453
Microsoft Purview Communication Compliance	454
Getting started	455
Get permissions	455
Enable auditing	456
Configure Communication Compliance settings.....	456
Privacy	456
Notice templates	456
Sentiment analysis	456
Cross-policy resolution.....	456
Teams	457
Convert Viva Engage to Native Mode	457
Configure connectors.....	457
Create a communication compliance policy	457
Review policy matches	459
Manage alerts	460
Reports.....	460
Microsoft Purview Information Barriers.....	461
Getting started	462

Get permissions	463
Enable auditing	463
Enable IB for SharePoint and OneDrive.....	464
Configure IB modes.....	464
Open	464
Owner moderated	464
Implicit	465
Explicit	465
Mixed.....	465
Segment users.....	466
Apply the policies	466
Configure user discoverability	467
Conclusion.....	468
Multiple choice questions.....	468
Answer key	469
14. Managing eDiscovery Cases.....	471
Introduction.....	471
Structure.....	472
Objectives.....	472
Microsoft Purview eDiscovery	472
Licensing.....	473
Permissions.....	474
eDiscovery workflow.....	475
eDiscovery components	476
Cases.....	476
Data sources	476
Hold and hold policies	476
Searches	477
Search samples.....	477
Processes.....	477
Review sets	477
Configure eDiscovery settings.....	478
Creating and managing cases in eDiscovery.....	478
Create hold policies.....	482
Search for content.....	484

<i>Adding results to a review set</i>	488
<i>Export content</i>	489
Microsoft Purview Audit.....	490
<i>Licensing requirements</i>	490
<i>Roles required</i>	490
<i>Getting started with auditing</i>	490
Conclusion.....	493
Multiple choice questions.....	494
Answer key.....	494
15. Managing Regulatory Compliance	495
Introduction.....	495
Structure.....	496
Objectives.....	496
Microsoft Purview Compliance Manager.....	496
<i>License requirements</i>	497
<i>Permission requirements</i>	498
<i>Compliance score</i>	498
<i>Multi-cloud support</i>	499
<i>Understanding regulations</i>	501
Building and managing assessments.....	503
<i>Controls</i>	506
<i>Improvement actions</i>	507
<i>Alert policies</i>	512
Conclusion.....	514
Multiple choice questions.....	514
<i>Answer key</i>	515
16. Managing Privacy	517
Introduction.....	517
Structure.....	517
Objectives.....	518
Microsoft Priva.....	518
<i>Privacy Risk Management</i>	519
<i>Getting started with Privacy Risk Management</i>	519
<i>Creating and managing policies</i>	521

Investigating and remediating alerts.....	527
<i>Subject Rights Requests.....</i>	528
<i>SRR for data in M365.....</i>	530
Creating and managing delete request	536
<i>Delete workflow</i>	537
<i>Priva and Microsoft Purview Data Lifecycle Management.....</i>	538
<i>Action execution log</i>	538
<i>SRR for data beyond M365.....</i>	539
<i>Data agents</i>	540
<i>Tracker scanning.....</i>	540
<i>Consent management</i>	542
<i>Creating consent model.....</i>	543
<i>Publishing consent model</i>	544
<i>Privacy assessments.....</i>	545
<i>Assessment workflow</i>	546
<i>Privacy rules</i>	546
Conclusion.....	546
Multiple choice questions.....	547
Answer key.....	547
17. Best Practices.....	549
Introduction.....	549
Structure.....	549
Objectives.....	550
Identity best practices	550
<i>Microsoft Entra roles</i>	550
<i>Apply the principle of least privilege.....</i>	550
<i>Use PIM to grant just-in-time access</i>	551
<i>Turn on MFA for all admin accounts.....</i>	551
<i>Configure access reviews</i>	551
<i>Limit the number of Global Administrators</i>	551
<i>Limit the number of privileged role assignments.....</i>	551
<i>Use groups for role assignments</i>	552
<i>Activate multiple roles as once.....</i>	552
<i>Use cloud-native accounts.....</i>	552

<i>Risk policies</i>	552
<i>User risk policy</i>	552
<i>Sign-in risk policy</i>	552
<i>Conditional Access policies</i>	553
Security best practices	553
<i>Microsoft Defender for Identity</i>	553
<i>Microsoft Defender for Office 365</i>	554
<i>Responding to business email compromise</i>	555
<i>Microsoft Defender for Cloud Apps</i>	555
<i>Microsoft Sentinel</i>	557
<i>Roles and permissions recommendations</i>	558
Compliance best practices	558
<i>Insider risk management</i>	558
<i>Managing resource constraints</i>	559
<i>Communication Compliance</i>	559
Conclusion.....	560
Multiple choice questions.....	561
<i>Answer key</i>	561
Index	563-576

CHAPTER 1

Introduction to Microsoft Entra

Introduction

This chapter introduces you to Microsoft Entra. Microsoft Entra is a family of products that help organisations create, manage, and govern user access to enterprise applications and services. In this chapter, we will learn the components of the Microsoft Entra and how they can help organisations address their identity and access management requirements. We will also explore the licensing options for each capability. This chapter will demonstrate how to create users using Microsoft Entra, the external collaboration capabilities using Microsoft Entra External ID. It will also introduce new capabilities like Microsoft Entra Permissions Management, Microsoft Entra Verified ID and Global Secure Access.

Structure

The chapter covers the following topics:

- Microsoft Entra ID
- Microsoft Entra ID Governance
- Microsoft Entra External ID
- Microsoft Entra Permissions Management
- Microsoft Entra Workload ID

- Microsoft Entra Verified ID
- Global Secure Access

Objectives

By the end of this chapters, readers will be able to explain the different components of the Microsoft Entra product family. You will be able to understand the different licensing options available to organisations when they buy Microsoft Entra ID and the identity governance capabilities in Microsoft Entra ID. This chapter also explains how Microsoft Entra enables secure collaboration with external vendors, partners and customers using Microsoft Entra External ID. Finally, you will understand the new capabilities Microsoft Entra Permissions Management, Microsoft Entra Workload ID, Microsoft Entra Verified ID and Global Secure Access.

The future chapters in this book build on the concepts covered in this chapter.

Microsoft Entra ID

Microsoft Entra ID, previously known as Azure Active Directory, is Microsoft's cloud-based service for identity and access management. This allows users in the organisation to access internal and external resources like Microsoft 365, Azure and many other third-party cloud applications.

Microsoft Entra ID serves many purposes for users in an organisation depending on their role:

- **IT admins:** They can use Microsoft Entra ID to create and manage user accounts and control access to applications and other resources.
- **Application developers:** They can use Microsoft Entra ID to authenticate users and provide **single sign-on (SSO)** for their applications. This allows users to access applications with their Entra ID login information.
- **Microsoft 365, Office 365, Azure or Dynamics CRM online users:** Microsoft Entra ID enables users to authenticate and gain access to resources required to do their job.

Licensing

Microsoft Online business services such as Microsoft 365 or Microsoft Azure rely on Microsoft Entra ID to enable sign-in for users and help secure their identities. If your organisation uses any of these services, you already have the free version of Microsoft Entra ID.

To access other advanced user management and identity governance features, you can purchase Entra ID P1 or Entra ID P2.

Following is a short description of these license types:

- **Microsoft Entra ID free:** It is included in Microsoft cloud subscriptions such as Microsoft 365 and Azure. It offers basic user and group administration, on-premises directory sync, SSO and basic reporting features.
- **Microsoft Entra ID P1:** This plan offers all the features of the free plan, plus it allows hybrid users to access applications both on-premises and in the cloud. It also gives advanced administration options like dynamic groups, self-service group management and self-service password reset for on-premises users. It can be purchased as a separate product. It is included in Microsoft 365 E3 and Microsoft 365 Business Premium.
- **Microsoft Entra ID P2:** P2 offers all the capabilities of free and P1 and adds identity protection features such as risk-based Conditional Access and Privileged Identity Management that give access to administrators only when needed. It can be purchased on its own or comes with Microsoft 365 E5.

Creating new Entra ID tenant

All administrative tasks related to Microsoft Entra ID are done using the Microsoft Entra admin centre. You will begin by creating a new tenant for your organisation.

Prerequisites

To get started with Microsoft Entra ID you need to create an Entra ID tenant. For this, you need the following:

- An Azure subscription.
- An account with the Tenant Creator role assigned.

Note: If you do not have an Azure subscription create a free account by going to <https://azure.microsoft.com/en-us/free/>.

Steps

Following are the steps to create a new Microsoft Entra ID tenant:

1. Login to the Azure portal at **<https://portal.azure.com>** with an account that has the Tenant Creator role assigned.
2. Select **Microsoft Entra ID**.
3. Navigate to **Overview | Manage tenants** and then click **Create**.
4. On the **Basics** page, select **Microsoft Entra ID** and click **Next: Configuration** as shown in the following figure:

Home > Contoso | Overview > Manage tenants >

Create a tenant

Microsoft Entra ID

* Basics * Configuration Review + create

Microsoft Entra ID and Azure AD B2C enable users to access applications published by your organization, and share same administration experiences. [Learn more](#)

Tenant type

Select a tenant type *

☒ Microsoft Entra ID

☐ Azure AD B2C

[Help me choose...](#)

Figure 1.1: Creating a new tenant

- On the **Configuration** page enter the **Organisation name**, **Initial domain name** and **Location** and click **Next: Review + create**.

Refer to the following figure:

Home > Contoso | Overview > Manage tenants >

Create a tenant

Microsoft Entra ID

* Basics * Configuration Review + create

Directory details

Configure your new directory

Organization name * ⓘ

Initial domain name * ⓘ

Location ⓘ

☒ Geographic location - United States

The location selected above will determine the geographic location where Microsoft Entra ID will store your Cor data, see Microsoft Entra ID Data residency.

Figure 1.2: Enter organisation details

The new tenant will be created with the domain **domainname.onmicrosoft.com**.

When you create a new Microsoft Entra tenant, you become the Global Administrator of the tenant. You are also listed as the technical contact for the tenant.

Adding custom domain name in Entra ID

Microsoft Entra tenants are created with an initial domain like **yourorganisationname.onmicrosoft.com**. The user IDs are hence in the format **user1@yourorganisationname.onmicrosoft.com**. This cannot be changed or deleted but an additional domain name can be added to the tenant. This creates an additional domain name that is, familiar to the users, such as **user1@yourorganisationname.com**.

Following are the steps to add a custom domain name:

1. Login to **https://entra.microsoft.com** with an ID that has the Domain Name Administrator role assigned.
2. Browse to **Identity | Settings | Domain names | Add custom domain**.
3. Click on **Add custom domain**. Enter your organisation's domain and click **Add domain**.

Refer to the following figure:

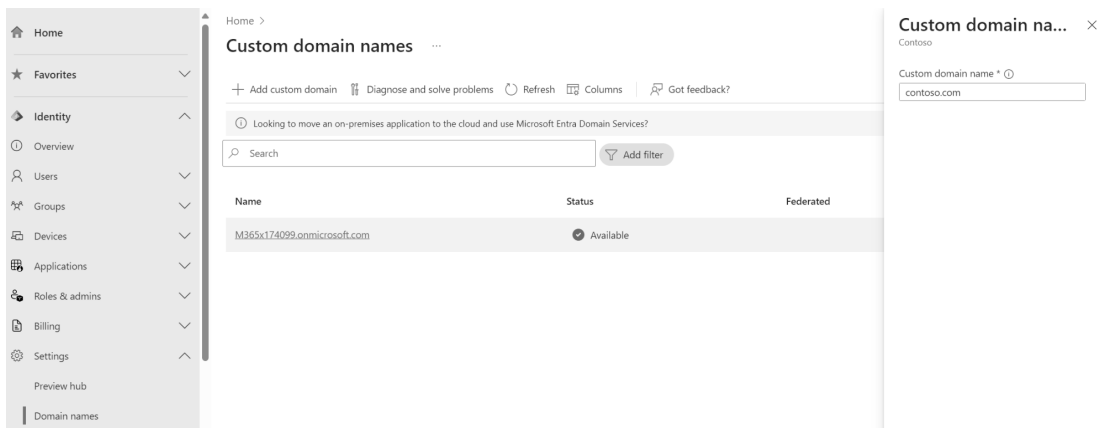


Figure 1.3: Adding a custom domain name

Note: The custom domain name must include **.com**, **.net** or any other top-level extension for this to work. The organization should already have a top-level domain registered with a domain registrar.

4. The unverified domain is added, showing the DNS information as in the screen below. This will be required to validate your ownership of the domain. Save this information.

Refer to the following figure: