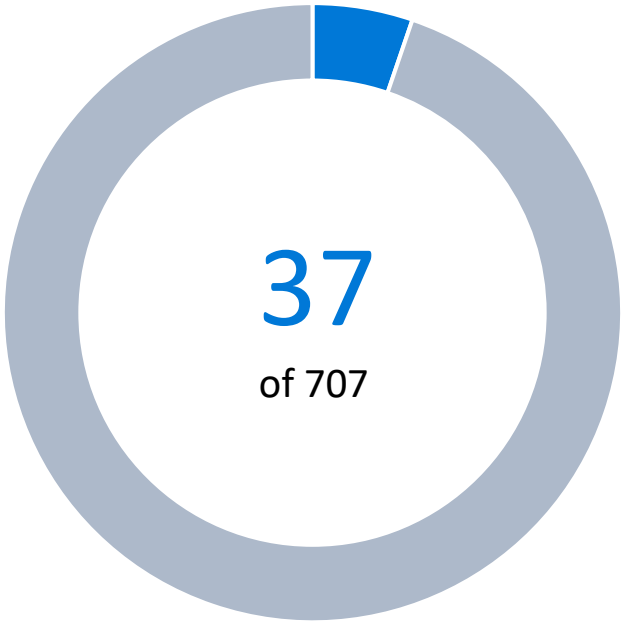
Secure Score Championship 2019

Bjørn Åge, Phillip, Martin, Henning og Ådne

Ever wondered how secure your Office 365 environment really is?

According to Microsoft, the average secure score across all tenants for Office 365 is 37 out of 707.

Average Office 365 environment



Getting compliant in the cloud is a shared responsibility

Customer management of risk

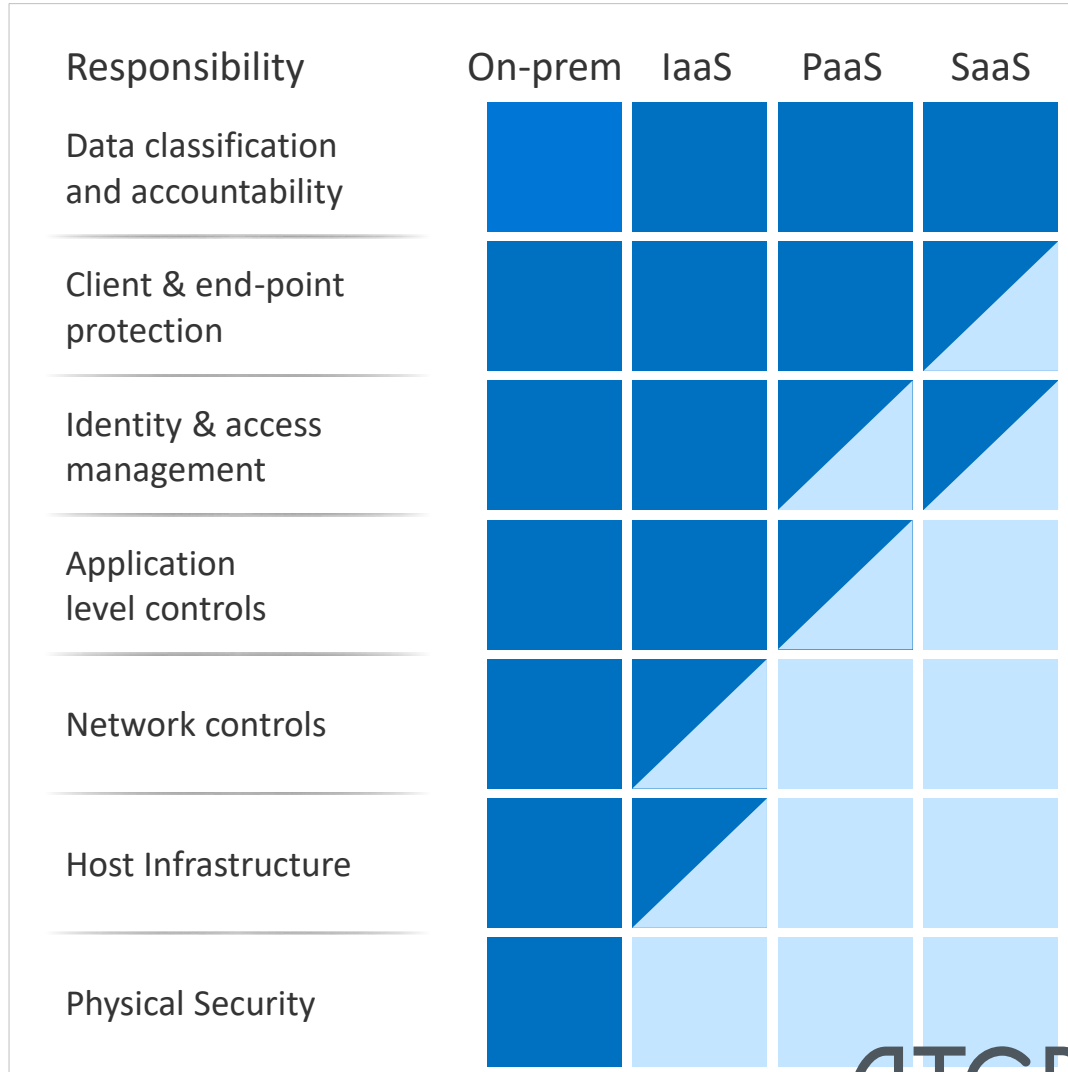
Data Classification and data accountability

Shared management of risk

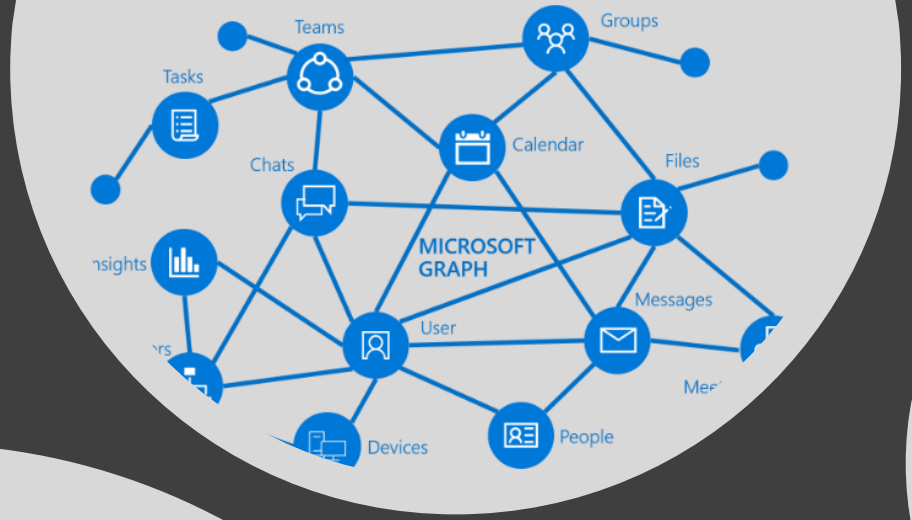
Identity & access management | End point devices

Provider management of risk

Physical | Networking



Cloud Customer Cloud Provider

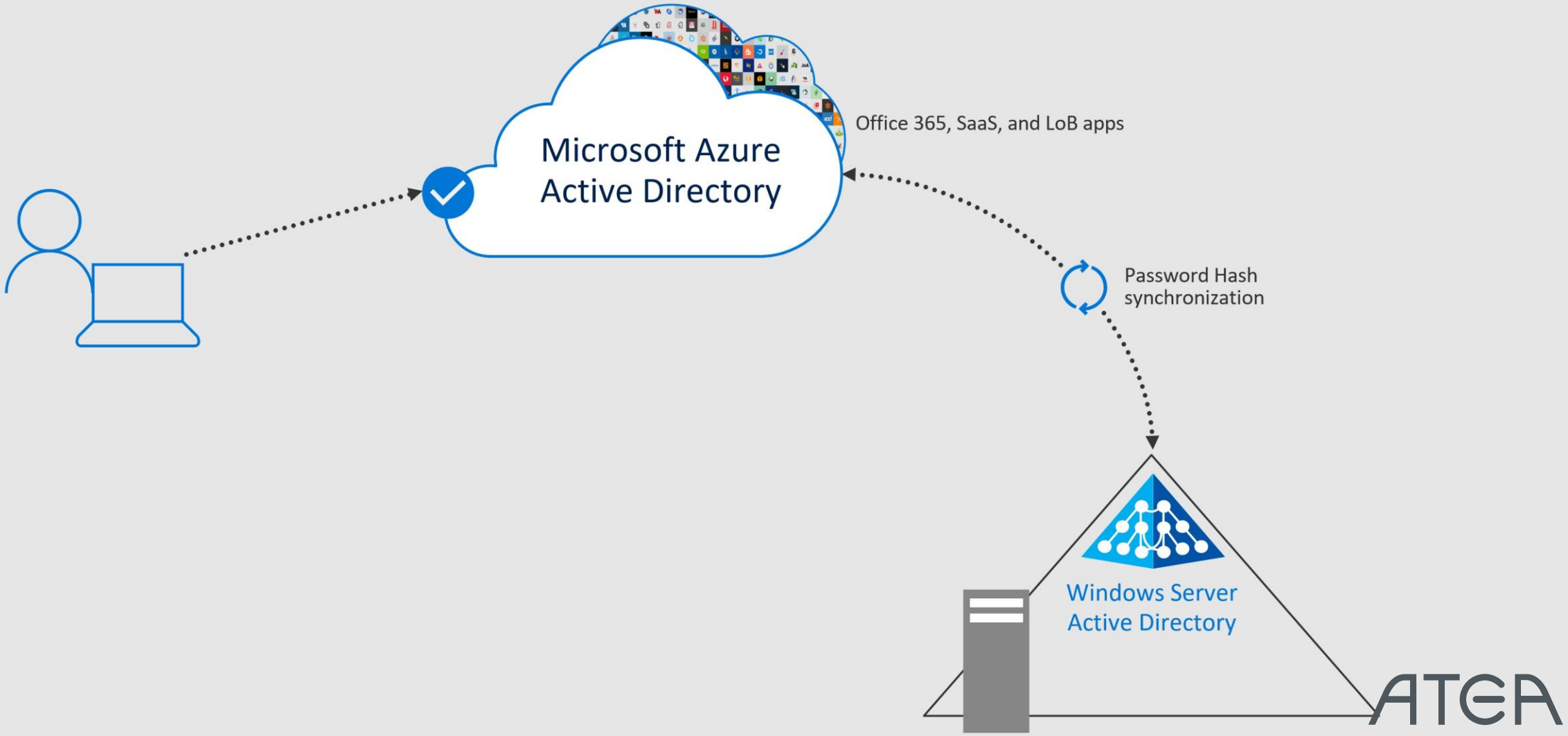


Preperation

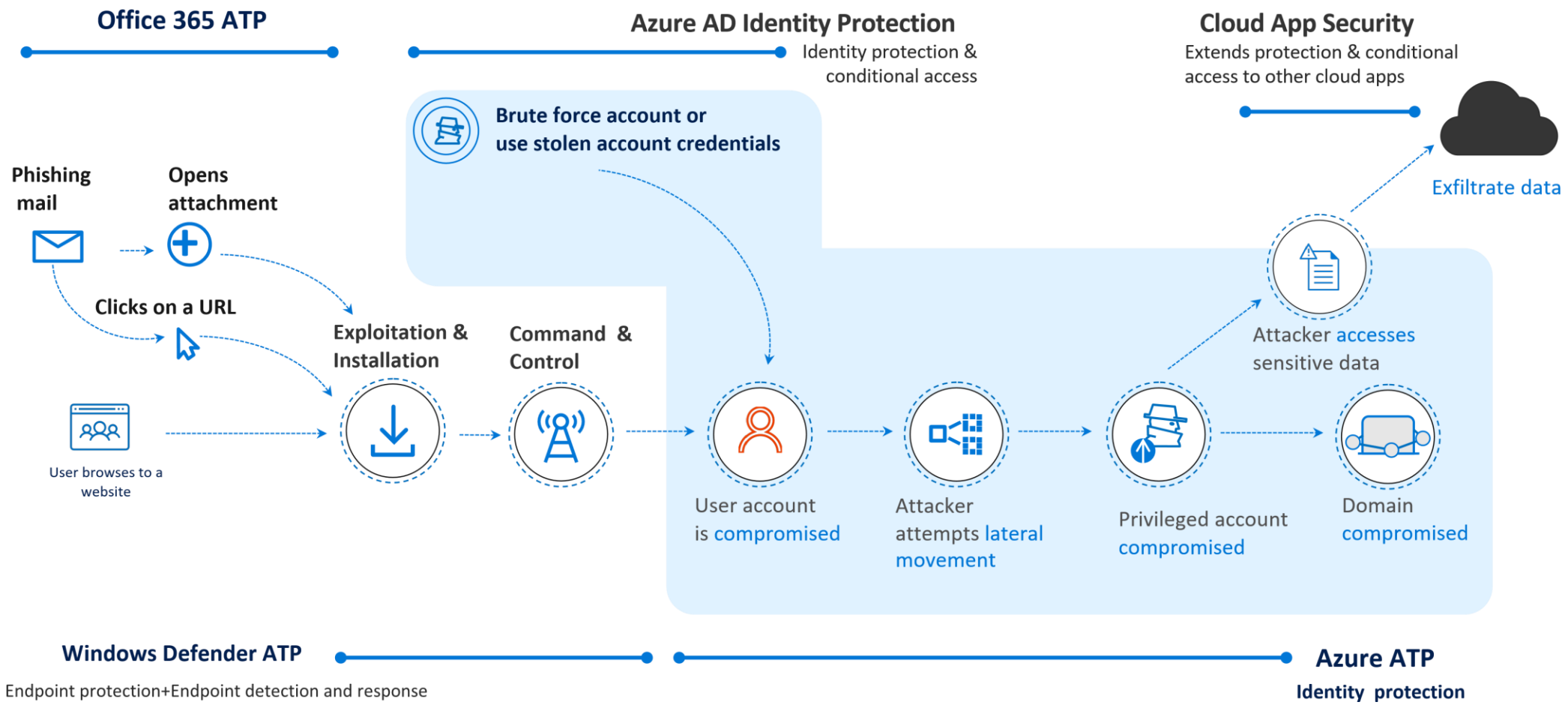
Improvement action	Ansvar	Rank	Score	Script/Manuelt	Kommentar
Require MFA for Azure AD privileged roles	Slutt	1	50/50	Manuelt	Conditional Access
Require MFA for all users	Slutt	2	30/30	Manuelt	Conditional Access
Enable Password Hash Sync if hybrid	Phillip	9	0/10		Sett opp DC
Register all users for multi-factor authentication	Slutt	12	0/10	Manuelt	Conditional Access
Store user documents in OneDrive for Business	Bjørn Åge	14	10/10	Manuelt	Lagre et dokument
Review permissions & block risky OAuth applications connected to your environment	Slutt	15	0/15		
Consume audit data weekly	Slutt	19	0/5	Manuelt	https://protection.office.com/unifiedauditlog
Enable self-service password reset	Philip	20	5/5	Manuelt	https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/PasswordReset
Review mailbox forwarding rules weekly	Slutt	24	0/5	Powershell	https://github.com/OfficeDev/O365-InvestigationTooling/blob/master/DumpDelegatesandForwardingRules.ps1
Review mailbox access by non-owners bi-weekly	Slutt	25	0/5	Manuelt	https://outlook.office365.com/ecp/Reporting/NonOwnerAccessReport.aspx?rfr=admin_o365&exsvurl=1&mkt=en-US&Realm=M365x766677.onmicrosoft.com
Review malware detections report weekly	Slutt	26	0/5	Mauelt	https://protection.office.com/#/insightdashboard
Designate more than one global admin	Slutt	27	5/5	Manuelt	Azure AD
Designate fewer than 5 global admins	Slutt	29	0/1	Manuelt	Azure AD
Do not expire passwords	Martin	33	10/10	Manuelt	O365 > Under Settings > Security & privacy in the Microsoft 365 admin center, Edit the password policy to never let passwords expire. You must be a global admin to edit the password policy.
Do not allow users to grant consent to unmanaged applications	Martin	35	10/10	Manuelt	O365 > To prevent users in your organization from allowing third-party apps to access their Office 365 info, in the Microsoft 365 admin center go to Settings > Services & add-ins. Select Integrated Apps and clear the associated check box.
Apply IRM protections to documents	Bjørn Åge	41	0/5	Manuelt	Lage et dokument
Remove TLS 1.0/1.1 and 3DES dependencies	Philip	43	5/5	Manuelt	Last ned rapport. https://servicetrust.microsoft.com/AdminPage/TlsDeprecationReport/Download Done
Configure expiration time for external sharing links	Martin	44	0/2	Manuelt	https://m365x742202-admin.sharepoint.com/_layouts/15/online/ExternalSharing.aspx
Set up versioning on SharePoint online document libraries	Bjørn Åge	45	2/2	Sjekk	
Use limited administrative roles	Slutt	50	1/1	Sjekk	
Delete/block accounts not used in last 30 days	Slutt	51	0/1	Powershell	https://github.com/OfficeDev/O365-InvestigationTooling/blob/master/InactiveUsersLast90Days.ps1
Do not allow mailbox delegation	Philip	52	1/1		
Allow anonymous guest sharing links for sites and docs	Martin	53	0/1	Manuelt	https://m365x742202-admin.sharepoint.com/_layouts/15/online/ExternalSharing.aspx
Apply Data Loss Prevention policies	Henning/Bjørn Åge	54	0/20	Manuelt	https://protection.office.com/datalossprevention?id=9247a17b-7b4f-4780-a703-81555f53eb88
Enable Microsoft Intune Mobile Device Management	Ådne	55	20/20	Manuelt	Lisens
Discover risky and non-compliant shadow IT applications	Martin/Ådne	56	0/20	Manuelt	Cloudapps
Set automated notifications for new OAuth applications connected to your corporate environment	Martin	57	0/20		
Turn on sign-in risk policy	Ådne	58	0/30	Manuelt	Lisens PIM
Turn on user risk policy	Ådne	59	30/30	Manuelt	Lisens PIM
Enable policy to block legacy authentication	Ådne	65	0/20	Manuelt	Conditional Access
Turn on Cloud App Security Console	Martin/Ådne	70	20/20	Manuelt	https://protection.office.com/advancedsecuritymanagement
Set automated notifications for new and trending cloud applications in your organization	Martin	72	0/15		
Set up Office 365 ATP Safe Attachment policies	Bjørn Åge	75	15/15	Manuelt	https://protection.office.com/#/safeattachment
Set up Office 365 ATP Safe Links to verify URLs	Bjørn Åge	77	15/15	Manuelt	https://portal.office.com/AdminPortal/Home?switchtomoderndefault=true#/catalog
Create a custom activity policy to discover suspicious usage patterns	Martin	80	0/10		
Discover trends in shadow IT application usage	Martin	82	0/5		
Create a Microsoft Intune Compliance Policy for iOS	Ådne	84	0/10	Powershell	Graph API
Create a Microsoft Intune Compliance Policy for Android	Ådne	85	0/10	Powershell	Graph API
Create a Microsoft Intune Compliance Policy for Android for Work	Ådne	86	0/10	Powershell	Graph API
Create a Microsoft Intune Compliance Policy for Windows	Ådne	87	43748	Powershell	Graph API
Create a Microsoft Intune Compliance Policy for macOS	Ådne	88	0/10	Powershell	Graph API
Create a Microsoft Intune App Protection Policy for iOS	Ådne/Henning	89	0/10	Powershell	Graph API
Create a Microsoft Intune App Protection Policy for Android	Ådne/Henning	90	0/10	Powershell	Graph API
Create a Microsoft Intune Windows Information Protection Policy	Ådne/Henning	91	0/10	Powershell	Graph API
Create a Microsoft Intune Configuration Profile for iOS	Ådne	92	0/10	Powershell	Graph API
Create a Microsoft Intune Configuration Profile for Android	Ådne	93	0/10	Powershell	Graph API
Create a Microsoft Intune Configuration Profile for Android for Work	Ådne	94	0/10	Powershell	Graph API
Create a Microsoft Intune Configuration Profile for Windows	Ådne	95	10/10	Powershell	Graph API
Create a Microsoft Intune Configuration Profile for macOS	Ådne	96	0/10	Powershell	Graph API
Mark devices with no Microsoft Intune Compliance Policy assigned as not compliant	Ådne/Henning	97	10/10	Manuelt	Conditional Access
Enable enhanced jailbreak detection in Microsoft Intune	Ådne/Henning	98	0/10	Powershell	Graph API Compliance policy setting
Enable Windows Defender ATP integration into Microsoft Intune	Ådne/Henning	101	0/10	Manuelt	
Use Cloud App Security to detect insider threat, compromised account and brute force attempts	Martin	107	0/15		
Turn on customer lockbox feature	Ådne/Henning	127	0/5	Manuelt	https://portal.office.com/AdminPortal/Home?switchtomoderndefault=true#/settings/security

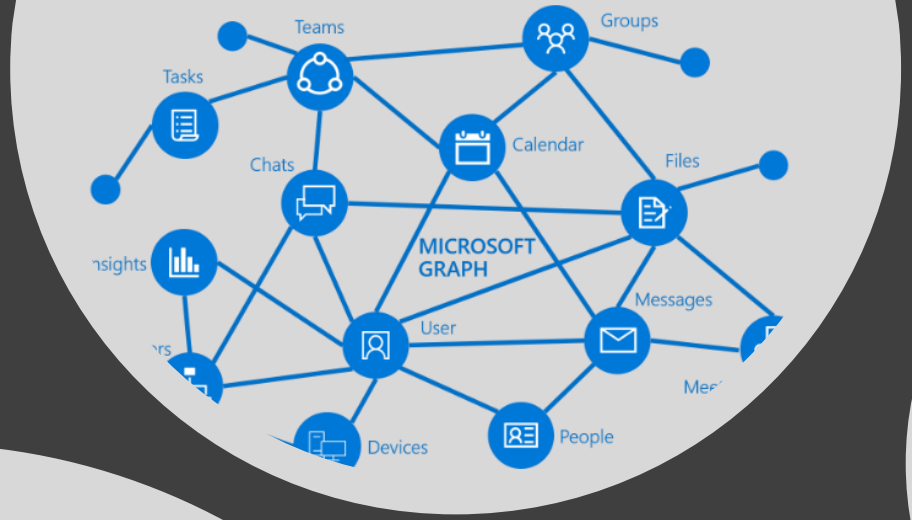
Azure AD Connect authentication options

Password Hash synchronization



Maximize protection



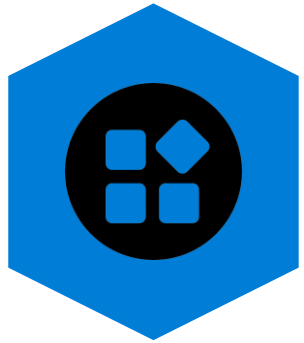

Teams
Groups
Tasks
Calendar
Chats
Files
MICROSOFT
GRAPH
Messages
User
Devices
People

Results

Secure Score Championship 2019

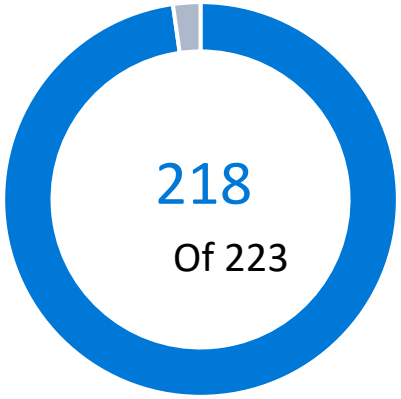
Identity

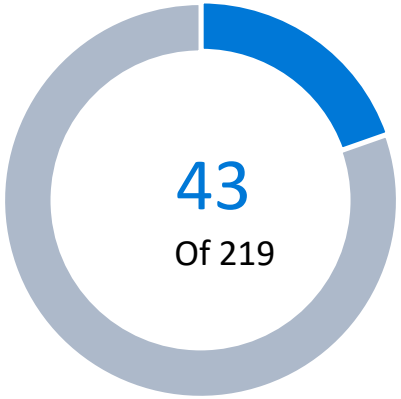
Data

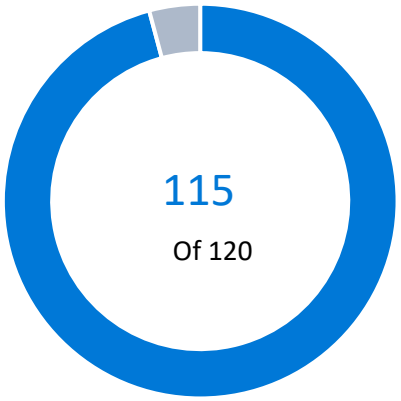


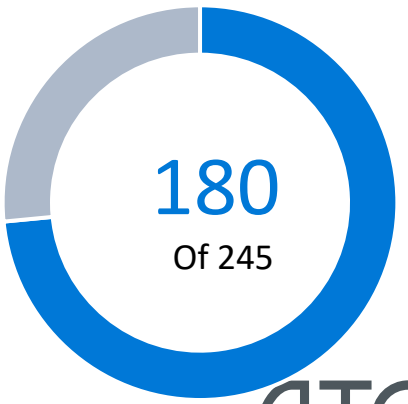
Apps

Device









ATEA