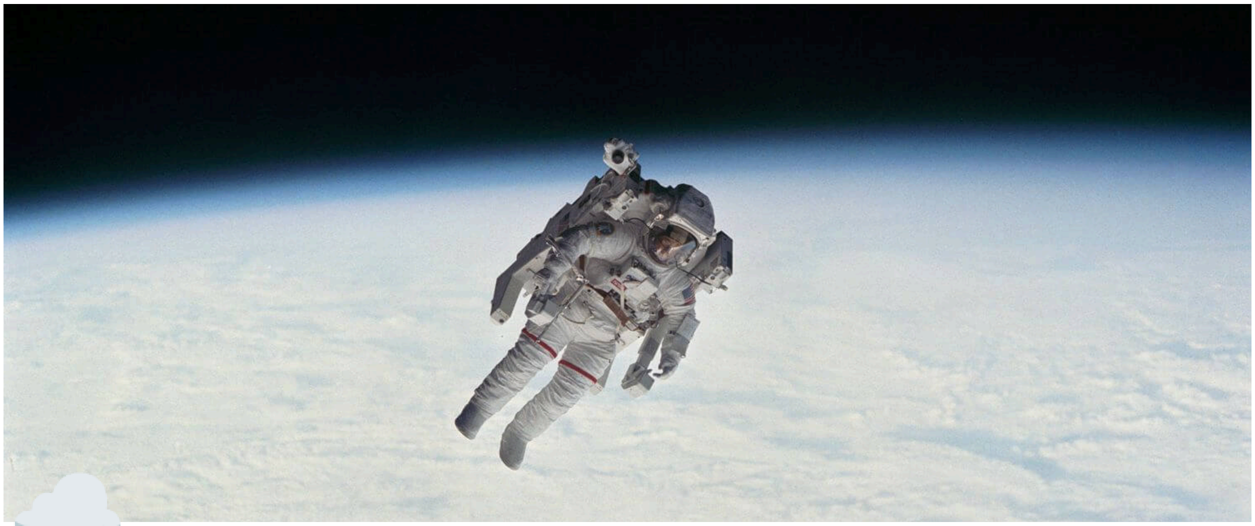

Cloud Security

Area	Application	Configuration
Essentials 1.1	Entra	Multi-factor authentication is enforced for all users
Essentials 1.2	Entra	MFA is required for all Admins
Essentials 1.3	Entra	Legacy Authentication is blocked
Essentials 1.4	Entra	Break Glass users are created for emergency access
Essentials 1.5	Entra	Ensure that between two and four global admins are designated
Essentials 1.6	Entra	Highly privileged accounts shall be cloud-only
Essentials 1.7	Entra	Non-admin users shall be prevented from providing consent to 3rd party applications
Essentials 1.8	Entra	Guest users have limited access to properties and memberships of directory objects

Area	Application	Configuration
Core 1.9	Entra	Passwords shall not expire
Core 1.1	Entra	MFA shall be required to enroll devices to Azure AD
Core 1.11	Entra	Local Administrator settings are configured for device joins
Core 1.12	Entra	Dormant Accounts are disabled with 45 days of Inactivity
Core 1.13	Entra	Browser Sessions are limited for Privileged Users
Core 1.14	Entra	Devices shall be deleted that haven't checked in for over 30 days
Core 1.15	Entra	All corporate approved applications are cataloged and periodically reviewed
Premium 1.16	Entra	Dynamic Groups are leveraged for automated group management
Premium 1.17	Entra	MFA Shall be required for Intune Enrollment
Premium 1.18	Entra	Require Managed Devices for Sign in
Advanced 1.19	Entra	Device Compliance is required for access to resources
Advanced 1.2	Entra	Require Phishing Resistant MFA for Admins
Advanced 1.21	Entra	High risk users and sign-ins are blocked
Advanced 1.22	Entra	Privileged Identity Management (PIM) is configured for JIT access
Advanced 1.23	Entra	Microsoft Sentinel in configured in ingest logs from Entra and Defender
Essentials 2.1	Exchange	SPF, DKIM, and DMARC records are set up for every domain
Essentials	Exchange	Anti-spam policies are configured

Area	Application	Configuration
2.2		
Essentials 2.3	Exchange	Anti-phishing policies are configured
Essentials 2.4	Exchange	Anti-malware policies are configured
Essentials 2.5	Exchange	Automatic forwarding to external domains SHALL be disabled
Essentials 2.6	Exchange	Mailbox Auditing SHALL Be Enabled
Essentials 2.7	Exchange	Calendar and Contact Sharing Shall Be Restricted
Core 2.8	Exchange	External Sender Warnings are Implemented
Essentials 3.1	Teams	External User Access SHALL Be Restricted
Essentials 3.2	Teams	External Participants SHOULD NOT Be Enabled to Request Control of Shared Desktops or Windows in Meetings
Essentials 3.3	Teams	Anonymous Users SHALL NOT Be Enabled to Start Meetings
Essentials 3.4	Teams	Automatic Admittance to Meetings SHOULD Be Restricted
Essentials 3.5	Teams	Unmanaged users SHALL NOT be enabled to initiate contact with internal users.
Essentials 3.6	Teams	Contact with Skype Users SHALL Be Blocked.
Essentials 3.7	Teams	File Sharing and File Storage Options shall be blocked
Core 4.1	Intune	Automated patching is performed on all devices
Core 4.2	Intune	Managed devices are enrolled in MDM

Area	Application	Configuration
Essentials 4.3	Intune	Personal Devices should be restricted from enrolling into the MDM solution
Essentials 4.4	Intune	Security Baselines should be configured for Windows Devices
Essentials 4.5	Intune	Devices compliance policies shall be configured for every supported device platform
Essentials 4.6	Intune	All devices have drive encryption applied
Core 4.7	Intune	Lockout screen and password settings shall be configured for each device
Core 4.8	Intune	App Protection policies should be created for mobile devices
Premium 4.9	Intune/SharePoint & OneDrive	Approved 3rd party applications are deployed and patched
Advanced 4.1	Intune	Local Administrators passwords are managed with LAPS
Essentials 5.1	SharePoint & OneDrive	Default sharing settings are set for New and Existing Guest
Essentials 5.2	SharePoint & OneDrive	Expiration Dates are set for Anyone links
Essentials 6.1	Defender	Security Awareness training is conducted at least once per year
Essentials 6.2	Defender	Anti-virus protections are applied to all devices
Essentials 6.3	Defender	Endpoint detection and response software is running on all devices
Essentials 6.4	Defender	Firewall protections configured on devices
Essentials 6.5	Defender	Safe Links policies are configured
Essentials 6.6	Defender	Safe Attachment policies are configured

Area	Application	Configuration
Core 6.7	Defender	Tamper Protection is configured
Core 6.8	Defender	Attack Surface reduction rules are configured
Advanced 6.9	Defender	Defender for Cloud Apps is configured to monitor applications on the network
Essentials 7.1	Purview	Periodic backups are performed for email, files, and Servers
Essentials 7.2	Purview	Audit Logging SHALL Be Enabled
Core 7.3	Purview	Retention Polices are configured
Premium 7.4	Purview	Sensitivity Labels are configured
Advanced 7.5	Purview	Data Loss Prevention Policies are configured
Entra Essentials Scripts (1.1 -1.8)	Script	
Entra Core Scripts (1.9 - 1.15)	Script	
1.16 - 3.3 Script	Script	
3.3 - 4.9 Script	Script	
5.1 - 7.5 Script	Script	
More		
More		