

# Microsoft 365

for Enterprise

## Elevating Your Cloud Security with Microsoft 365

Cyber risks are major concerns to businesses today. The growing number of endpoints, tools, data storage being used across enterprises is leading to a rapid expansion in the attack surface, which many businesses are struggling to monitor & secure, and adhere to the ever-increasing data governance & compliance needs.

**Microsoft 365 for Enterprise** is a pragmatic approach combining consultation, technical implementation and fully managed services\* of Microsoft 365 Security features, in a sequence of steps that ensures protection of enterprise data across Microsoft ecosystem, adherence to regulatory requirements and simplify operational complexity.

\*optional

**Microsoft 365 for Enterprise Services** are available in 2 options, allowing enterprise businesses to choose the right level of service as per their requirements and budget



### Once-Off (fixed onetime price)

- ✓ Implementation of Microsoft 365 Security features across 3 key pillars
- ✓ Sentinel Security Monitoring & Auditing Dashboard
- ✓ Knowledge Transfer to the IT team / administrators of the organisation
- ✓ 1-month post-implementation support to the IT team / administrators of the organisation



### Managed Services (fixed per user, per month price)

- ✓ Implementation of Microsoft 365 Security features across 3 key pillars
- ✓ Sentinel Security Monitoring & Auditing Dashboard
- ✓ User Support Help Desk, Email and Chat based
- ✓ Microsoft 365 Account & Subscription Administration
- ✓ End-User Security Awareness & Adoption Training

# Microsoft 365 for Enterprise Scope

Microsoft 365 for Enterprise scope includes deployment of following Microsoft 365 Security features across 3 key pillars in a phased approach or deployment of each pillar as a standalone project, based upon the organisation's business requirements:



## Secure Identities & Access

- ✓ Enable Self-Service Password Reset (SSPR) – employees can reset their password on their own anytime, without requiring IT support
- ✓ Enable Multi-Factor Authentication (MFA) – put in place an additional login security layer which makes it exponentially more difficult for hackers to get access to employees' accounts
- ✓ Conditional Access – maintains control over how organisation data is being accessed by employees based on permitted application or their geographical location – for e.g., block specific employees who are accessing organisation data from outside home country
- ✓ Risk Based Conditional Access – prevents unauthorised access to organisation data through real-time detection of identity-based risks
- ✓ Azure Active Directory (AD) Identity Governance – controls internal & external users' access to applications, groups, Teams and SharePoint sites, with multi-stage approval, and ensure users do not retain access indefinitely through time-limited assignments and recurring access reviews
- ✓ Azure Active Directory (AD) Privileged Identity Management – provides as-needed and just-in-time access to important resources to mitigate the risks of excessive, unnecessary, or misused access permissions



## Secure Apps & Endpoints

- ✓ Mobile Device Management (MDM) for enrollment of corporate-owned devices (such as mobiles, PCs & laptops), managing the organisation's security policies and business applications
- ✓ Mobile Application Management (MAM) for restricting copying or saving of company data to unauthorised apps & locations, for e.g. employees cannot save organisation data on personal devices such as home PC or mobiles
- ✓ Safeguard the organisation's endpoints across multiple platforms against ransomware and other emerging cyberthreats with real-time antivirus and antimalware protection, including endpoint detection & response, with intelligent automated investigation and remediation capabilities
- ✓ Microsoft Defender for Office 365 – safeguards your organisation against malicious threats such as phishing attempts and ransomware, posed by email messages, links (URLs)
- ✓ Attack Simulation – run cyberattack simulations within the organisation to test the efficacy of security policies in place, identify & find vulnerable users and train them to increase their awareness & decrease their susceptibility to attacks
- ✓ Sentinel Security Monitoring & Auditing Dashboard – real-time dashboard offering proactive security monitoring & reporting of the organisation's Microsoft 365 environment to detect potential sophisticated cyber threats and comply with audit requirements



## Protect & Govern Sensitive Data Across Documents & Emails

- ✓ Classify, identify & tag email and documents with sensitivity labels (such as General, Internal Only or Sensitive, etc.) to apply data protection policies (for e.g. do-not-print, do-not-forward, for internal sharing only, etc.)
- ✓ Data Loss Prevention on emails & documents – protects organisation sensitive data from intentional or unintentional leakage, blocking undesired actions and access by untrusted and/or malicious actors
- ✓ Discover & manage shadow IT - discover all cloud apps being used within the organisation, identify risks associated with the discovered apps based on security factors, industry & legal regulations, and govern access to the apps & resources (for e.g., sanction, unsanctioned, mark for review or entirely block)
- ✓ Email & documents long-term retention – enable long-term data retention policies to ensure organisation never lose an email or document due to intentional or unintentional delete by anyone and allows for organisation-wide search of emails, documents using specific keywords, message / document properties, sensitive data types, etc.

### Contact Us

[www.tcf.cloud](http://www.tcf.cloud)

#### Mauritius Office

The Cloud Factory EMEA Ltd  
1, The Factory Building, Vivéa Business Park, Moka | Mauritius  
T: +(230) 433 7629 | E: [hello@tcf.cloud](mailto:hello@tcf.cloud)

#### UK Office

TCF EMEA LTD  
228 Portland Crescent, Stanmore, Middlesex, England HA7 1LS  
T: +(44) 20 8078 7251 | E: [hello@tcf.cloud](mailto:hello@tcf.cloud)

