SERVICE DESCRIPTION: SECURE WORKPLACE - ENDPOINTS

DESCRIPTION

The **Secure Workplace - Endpoints** Service is designed to rapidly uplift the security capability across Endpoints within small and medium-sized businesses. It leverages the capability of Microsoft Endpoint Manager (also known as Intune) from within Microsoft 365, Azure Active Directory and Microsoft Defender for Business to provide cloud management and protection capability for Endpoints.

This service has a cadence of policy updates to ensure that devices that are in scope are kept up to date and secure in line with industry best practice.

Service Capability	Notify
Multi-Factor Authentication	✓
Endpoint Security Policies	✓
Endpoint Data Loss Prevention	✓
Endpoint Secure Access Policies	✓
Endpoint Incident Management and Handling	Can be added at an additional cost per user, please talk to your Account Manager

SERVICE SCOPE - NOTIFY

The section describes the in-scope items for the Notify tier of the service.

1. AZURE ACTIVE DIRECTORY

1. 1 This service includes the following in-scope items across Azure Active Directory:

(a) Creation of an Azure Active Directory Security Group to control the deployment and assignment of the service configuration and policies.

(b) Creation of an Azure Active Directory guest account from One New Zealand to receive notifications for quality assurance.

(c) Deployment of the Secure Workplace Azure Active Directory Enterprise Application for the service to deploy and manage the service configurations.

(d) Configuration of a Multi-Factor Authentication (MFA) Registration Campaign to support the registration of the Microsoft Authenticator app.

(e) Deployment of the following Conditional Access Policies:

(i) Require that an App on Android/iOS devices accessing business applications be protected by an App Protection Policy.

(ii) Require Multifactor Authentication every one (1) hour for devices protected by the service that are marked non-compliant by Microsoft Endpoint Manager (Compliance Policy is detailed below).

2. MICROSOFT ENDPOINT MANAGER

This service includes the following in-scope items across Azure Active Directory:

2. 1 **Device Configuration Profiles**:

The following Device Configuration Profiles will be deployed;

(a) Device Restriction Profile to ensure the following controls are set;

(i) A complex alphanumeric password of at least 8 characters or,

(ii) A complex PIN number with at least 6 digits.

(iii) Prevention of password sharing on iOS devices.

(b) A Windows Update policy to configure device updates on Windows devices ensuring the following controls are set;

(i) Quality Updates are deferred for 14 days from each release.

(ii) Feature Updates are deferred for 60 days from each release.

2. 2 **Device Compliance Policies**:

The following Device Compliance Policies will be deployed across each operating system;

(a) A Static Device Compliance policy ensuring the following controls are set;

(i) A Device PIN or Password is set.

(ii) Device Encryption is configured.

(iii) Anti-virus software is running.

(iv) The device operating system is within 6 months of the latest supported release.

(v) Defender for Business anti-malware definitions are configured.

(b) A Reactive Device Compliance Policies will be deployed to supported operating systems to ensure following controls are set;

(i) The machine risk of the in-scope endpoints is clear.

2. 3 **Endpoint Security Profiles**:

The following Endpoint Security Profiles will be deployed across each operating system;

(a) An Antivirus policy across MacOS and Windows endpoints to ensure the following controls are set;

(i) Cloud Protection is enabled and set to High.

(ii) Real-time Protection, Intrusion Protection, Behaviour Monitoring (abnormal activity detection), file-scanning and Network Protection are enabled.

(iii) Daily quick anti-virus scanning with signature updates before scan and twice each day if available.

(b) Windows and MacOS Firewall configuration.

(c) Attack Surface Reduction rules for Windows endpoints to ensure the following controls are set;

(i) Block credential stealing from the Windows local security authority subsystem (lsass.exe) to reduce the likelihood of cached credentials being stolen if the device is compromised.

(ii) Use advanced protection against ransomware to determine whether a file resembles ransomware.

(iii) Block executable content download from email and webmail clients.

(iv) Block untrusted and unsigned processes that run from USB.

(v) Block JavaScript or VBScript from launching downloaded executable content.

(d) Endpoint Detection and Response policy to onboard Defender for Business for in-scope endpoints.

(e) Disk Encryption to configure Bitlocker on Windows and FileVault on MacOS Endpoints.

2. 4 **App Protection Policies**:

The following Endpoint Security Profiles will be deployed across each operating system;

(a) The following App Protection Policies will be deployed across Android and iOS mobile endpoints to ensure the following controls are set;

(i) Company Data will not be saved within iCloud/iTunes and Google Backups.

(ii) Data will not be copied from managed Company Apps to unmanaged and/or personal apps.

(iii) Web content will be opened only within Microsoft Edge.

(iv) Notifications from managed Company Apps will not be visible on the device lock screen.

(v) A PIN or biometric will be required to access managed Company Apps after 30 minutes of device inactivity.

(vi) Jailbroken or rooted devices will be prevented from accessing managed Company Apps.

(vii) Users with disabled accounts in Azure Active Directory will have their company data wiped from managed Company Apps.

2. 5 **App Deployment Policies**:

The following Applications will be deployed across mobile operating systems;

(a) App Deployment (via public app store) and Configuration of;

(i) Defender for Endpoint (Android/MacOS/iOS)

(ii) Microsoft line-of-business apps for mobile endpoints (such as Outlook Mobile and Microsoft Authenticator).

3. MICROSOFT DEFENDER FOR BUSINESS

3. 1 This service includes the following in-scope items across Microsoft Defender for Business:

(a) Defender for Business integration with Intune. This will allow Defender for Business to be onboarded via Intune for Windows Endpoints.

(b) Defender for Business Tamper Protection. This ensures that Defender for Business cannot be interfered with and disabled.

(c) Automated Investigation and Remediation will be enabled to allow Defender for Business to detect and remediate threats automatically.

(d) Configuration of alerts and vulnerability notifications within Defender for Business. This will notify if the service detects malware or new vulnerabilities within the Endpoints onboarded for the service.

4. SERVICE EXCLUSIONS

4. 1 The service does not include configuration or deployment of the following;

(a) Device Configuration profiles not explicitly identified within Service Scope such as Certificates, OneDrive, WiFi and Personalisations.

(b) App Deployment and Configuration beyond Defender for Endpoint (Android/MacOS/iOS) and Microsoft line-of-business apps for mobile endpoints (such as Outlook Mobile and Microsoft Authenticator)

(c) Endpoint Analytics Configuration and Reporting.

(d) Zero-Touch provisioning across Autopilot, MacOS/iOS and Android.

(e) PowerShell Scripts.

(f) Enrolment restrictions and limitations.

(g) Creation of Azure Active Directory users and Security Groups beyond those required for the service.

(h) Configuration and maintenance of connectors, including Google Play, Apple Business Manager and Microsoft Store for Business.

(i) Company Branding and Customisation.

5. SERVICE OFFBOARDING

5. 1 The offboarding of the service will involve the following;

(a) Removal of Intune policies included in the service from the Customer tenant. This will not remove existing configuration of devices that were previously onboarded to the service, but these devices will cease to receive future service updates and new devices will not have service policies applied.

(b) Removal of the Secure Workplace Azure Active Directory Application.

(c) Removal of the Service Azure Active Directory Security Group and Guest account.

(d) Removal of service email aliases from the Defender for Endpoint/Business portal.

6. LIMITATIONS

6. 1 You need to be aware that this service is evergreen with continual updates to operating systems, therefore any devices with specific operating system versioning may need to be excluded from management via the service.

7. SERVICE CONDITIONS

7. 1 The service is based on a minimum 12-month term

(a) We make no guarantees or warranties that the service will correctly detect and identify all:

(i) Security Events or Incidents

(ii) Instances of unauthorised access to your network

(iii) Malware

(iv) Exploits or

(v) Other types of attacks or issues.

(b) All necessary access controls will be provided

(c) You will provide the access required to establish and maintain the service

(d) You will provide remote access to information and communication capabilities

(e) You will make available any required system or information

(f) You will inform (or authorise us to inform) all relevant parties of the activities being carried out by DEFEND under your authorisation, including any key third parties

(g) You will provide the necessary business context and confirmation of activities outside the scope of our level of visibility and privileges

(h) You will provide access to the relevant resources and materials to enable completion of the deliverables of the service

(i) You will take responsibility for raising support requests with Microsoft for any issues with deployed resources within the subscription being used

(j) Travel and disbursements will be agreed prior and charged at cost if required

(k) For a full list of terms and conditions please see here https://www.one.nz/legal/terms-conditions/microsoft-365-business-premium/.

