Deployment Plan



Microsoft 365 Business Security Plan

Prepared for

[Type Customer Name Here]

7/10/2018

Version Draft

NOTE: This is an early release preview. Please check <http://aka.ms/bsecure> for the updated release.

Prepared by

**[Author]**

[Type Author Position Here]

[Type Author Email Here]

Contributors

**[Type Contributors Here]**

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation. Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers. © 2018 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited. Microsoft Corp. is strictly prohibited. Microsoft, Microsoft Active Directory, Microsoft Hyper-V, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other products mentioned that are not trademarks include Microsoft Internet Information Services. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Revision and Signoff Sheet

Change Record

| Date | Author | Version | Change Reference |
| --- | --- | --- | --- |
|  |  | .1 | Initial draft for review/discussion |
|  |  |  |  |
|  |  |  |  |

Reviewers

| Name | Version Approved | Position | Date |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Overview 6](#_Toc517772464)

[2 Technical Design (AATP) 8](#_Toc517772465)

[2.1 Prerequisites 8](#_Toc517772466)

[2.2 Solution Design 8](#_Toc517772467)

[2.3 Design Decisions 10](#_Toc517772468)

[2.4 Implementation Activities and Tasks 14](#_Toc517772469)

[2.5 Verifying the Implementation 15](#_Toc517772470)

[3 Technical Design (WD ATP) 16](#_Toc517772471)

[3.1 Prerequisites 16](#_Toc517772472)

[3.2 Solution Design 16](#_Toc517772473)

[3.3 Design Decisions 17](#_Toc517772474)

[3.4 Implementation Activities and Tasks 19](#_Toc517772475)

[3.5 Verifying the Implementation 20](#_Toc517772476)

[4 Technical Design (O365 ATP) 21](#_Toc517772477)

[4.1 Prerequisites 21](#_Toc517772478)

[4.1.1 Best practice for setting up authentication 21](#_Toc517772479)

[4.1.2 Best practice for configuring MX records 22](#_Toc517772480)

[4.1.3 Domains 23](#_Toc517772481)

[4.1.4 Customizing mail flow 23](#_Toc517772482)

[4.2 Layered Approach 24](#_Toc517772483)

[4.3 Solution Design 24](#_Toc517772484)

[4.4 Design Decisions 24](#_Toc517772485)

[4.5 Implementation Activities and Tasks 26](#_Toc517772486)

[4.6 Verifying the Implementation 27](#_Toc517772487)

[5 Technical Design (ASC) 28](#_Toc517772488)

[5.1 Prerequisites 28](#_Toc517772489)

[5.2 Solution Design 28](#_Toc517772490)

[5.3 Design Decisions 29](#_Toc517772491)

[5.4 Implementation Activities and Tasks 30](#_Toc517772492)

[5.5 Verifying the Implementation 31](#_Toc517772493)

[6 Technical Design (ATA) 32](#_Toc517772494)

[6.1 Prerequisites 32](#_Toc517772495)

[6.2 Solution Design 32](#_Toc517772496)

[6.3 Design Decisions 33](#_Toc517772497)

[6.4 Implementation Activities and Tasks 38](#_Toc517772498)

[6.5 Verifying the Implementation 39](#_Toc517772499)

1. Overview

Provide an overall summary of the contents of this document. This should include the criteria by which the design was established and how it was validated. It should also clearly identify the intended audience.

Justification: Some project participants may need to know only the document’s highlights, and summarizing creates that user view. It also enables the full reader to know the essence of the document before they examine the details. Expand below on the customer architecture.

This document details the design and implementation of Microsoft 365 Business at Customer Name. The design meets the requirements and goals that were stated in the Statement of Work document.

The overall solution design describing both products is visualized in an architecture overview and explained in detail. After providing an overview of the in-scope infrastructure, general information about the prerequisites are given. The document also includes a general description of the implementation of the two products referring to the relevant documentation where necessary.

1. Technical Design

This chapter details the technical design of Microsoft 365 Business at Customer Name.

After providing information about the prerequisites which must be in place for a successful deployment of Microsoft 365 Business, the design is explained in detail. After that, all design decisions that were made during the Deployment Workshop which led to the design are documented.

* 1. Set up and pre-requisite information

Before starting the implementation of M365, several preparation steps must be in place. A current and up-to-date list of all prerequisites can be found on Microsoft Docs online:

* [Pre-requisites for protecting data on devices with Microsoft 365 Business](https://support.office.com/en-us/article/pre-requisites-for-protecting-data-on-devices-with-microsoft-365-business-7770e280-3a6c-436f-a157-b008a2744f51?ui=en-US&rs=en-US&ad=US)
  1. Solution Design

**Please adapt the design diagram to reflect the Microsoft 365 Business at your customer. Pick the drawing the best reflects their architecture (AADJ or Hybrid AADJ) and adapt it as needed.**

Figure 1 illustrates the solution design of M365. All design decisions which led to this solution design are listed in section 2.3: Design Decisions.



Figure 1: Solution Design of Microsoft 365 Business at Customer Name with Azure Active Directory domain joined devices



Figure 1: Solution Design of Microsoft 365 Business at Customer Name with Hybrid Azure Active Directory domain joined devices

* 1. Design Decisions

In this section all design decisions that led to the solution depicted in the previous section are documented. All design options are listed for reference and the choice and rationale that was made is documented in the right most column.

**Please customize all Design Decisions according to your need. Also, please be sure to include plenty of context with each decision (for example by also including the alternatives and marking the actual choices. This makes sure the customer can deduct the reasoning of the design at a later point in time. Don’t delete any of the design decisions even if they’re not applicable as they can provide context to the customer and serve as documentation.**

|  |  |  |
| --- | --- | --- |
| **Design Decision** | **Description** | **Choice and Rationale** |
|  | **Tenant Security** |  |
|  | Enable MFA for all admins |  |
|  | Enable MFA for all users |  |
|  | Enable mailbox owner auditing |  |
|  | Who will review reports? |  |
|  | Who will review privileged access? |  |
|  | Enable client rules forwarding block? |  |
|  | Enable audit data recording? |  |
|  | Enable additional mailbox auditing? |  |
|  | Disable external sharing? |  |
|  | Disable external SIP federation? |  |
|  | Enable mobile device management services? |  |
|  | Require mobile devices to use a password? |  |
|  | **Office 365 EOP** |  |
|  | Keep Default Policy or create custom policy. |  |
|  | Malware Detection Response? YES/NO and STANDARD/CUSTOM |  |
|  | Common Attachment Types Filter? ON/OFF |  |
|  | Sender Notification? INTERNAL/EXTERNAL/OFF |  |
|  | Administrator Notification? YES/NO |  |
|  | Custom Notification? YES/NO |  |
|  | Enable Standard Settings? YES/NO (overrides Custom Settings) |  |
|  | Modify SCL level? – Value ? |  |
|  | Enable DKIM for all authoritative domains? YES/NO |  |
|  | **Office 365 ATP** |  |
|  | Use Default ATP Policy? YES/NO |  |
|  | Is there need for a specific policy for dedicated recipients? YES/NO |  |
|  | Enable ATP Safe attachments for all users? YES/NO |  |
|  | Use redirect in Policy? YES/NO |  |
|  | Scope by domain? YES/NO |  |
|  | Ramp up using Distribution Groups? YES/NO |  |
|  | Turn on ATP for SharePoint, OneDrive, and Microsoft Teams? YES/NO |  |
|  | Lowering Phishing threshold for key users? YES/NO |  |
|  | Enable check for authentication in ETRs? YES/NO |  |
|  | Make use of updated reporting add-in? YES/NO |  |
|  | Implement SPF, DKIM and DMARC? YES/NO |  |
|  | Implement DMARC with p=reject |  |
|  | Use ETRs to Skip Safe Attachments/Safe Links |  |
|  | Create ETRs to skip ATP internally? YES/NO |  |
|  | **Placeholder** |  |
|  |  |  |
|  |  |  |
|  | **Placeholder** |  |
|  |  |  |
|  |  |  |
|  | **Placeholder** |  |
|  |  |  |
|  |  |  |

* 1. Secure Activities and Tasks

The best source for up-to-date security information for Microsoft 365 Business is Microsoft’ public documentation site: [Get started with Microsoft 365 Business](https://support.office.com/en-us/article/get-started-with-microsoft-365-business-496e690b-b75d-4ff5-bf34-cc32905d0364?ui=en-US&rs=en-US&ad=US).

An Microsoft 365 BusinessSecurity deployment generally follows the flow described below:

|  |
| --- |
| **Step Description** |
| 1. [Get Microsoft Business](https://support.office.com/en-us/article/get-microsoft-365-business-5abfef7b-5957-484a-b06b-a7c55e013e44?ui=en-US&rs=en-US&ad=US) |
| 1. [Set up Microsoft 365 Business by using the setup wizard](https://support.office.com/en-us/article/set-up-microsoft-365-business-by-using-the-setup-wizard-6e7a2dfd-8ec4-4eb7-8390-3ee103e5fece?ui=en-US&rs=en-US&ad=US) |
| 1. [Mange Microsoft 365 Business](https://support.office.com/en-us/article/manage-microsoft-365-business-27ff1678-865a-4707-8145-e1155aa815d6?ui=en-US&rs=en-US&ad=US) |
| 1. Secure mobile devices |
| 1. Secure Windows 10 PCs |
| 1. Use AutoPilot to deploy Windows 10 devices (optional) |

* 1. Verifying the Implementation

After Microsoft 365 Business is secured, you can validate it is working properly by performing a few simple steps.