Office 365 Security Guidelines

Change History			
Version	Author	Date	Summary of Changes
0.1	Tony Unger	23/01/2020	New document
0.2	Tony Unger	03/02/2020	Formatting, references, content
0.3	Tony Unger	14/02/2020	Additional content
0.4	Tony Unger	25/02/2020	Finalised document

Contents

Purpose

This documentation provides guidance regarding security requirements & pre-requisites for the Microsoft Office & 365 platforms.

Scope

The Microsoft Office & 365 platforms are suites of multiple service offerings. This documentation therefore focuses on the high-level platform configuration options for the typical core enterprise solutions.

At the time of writing this includes; Office 2016 (Word, Excel, PowerPoint, OneNote, Outlook, Publisher) and 365 (SharePoint Online, Exchange Online, OneDrive for Business, Microsoft Teams).

Separate extended security & best practice guidance documentation is available for each of these offerings individually and should be referred to where applicable.

Since the 365 platform and many of its features are in a release status of public preview with many functional improvements being added regularly by the vendor; these solutions are likely to change considerably, therefore this documentation should be regularly reviewed and updated accordingly.

Applying the recommended configuration settings described should provide a good security baseline for an Office 365 implementation however **additional security capabilities should also be considered** in order to provide full security coverage. Examples such as SIEM (Security information and event management) and CASB (Cloud access security broker) services are outside the scope of this article but are recommended.

The recommendations provided in this document are platform specific and should be supported by an **overarching organisation security management programme** whereby policies, processes and working practices are in place to cover typical business security expectations (beyond the scope of this document).

Background

A wealth of security and compliance documentation is available from the vendor Microsoft. The documentation provides best practice guidance for the platform services and additional configuration controls for customers to meet compliance requirements such as ISO27001, PCI/DSS and HIPAA.

Additionally, external (non-vendor) security guidance documentation is available from several reputable sources including the Center For Internet Security (CIS) whereby benchmark standards & hardening guidelines have been published.

An “out-of-the box” solution is not considered secure nor hardened, default settings must be adjusted, and baseline configurations must be implemented to ensure organizations meet their own security expectations. The same is true of any compliance level expectations.

The licensing model of the 365 platform plays an important part in regards to which security features & capabilities are available. Some 365 security capabilities are considered premium features which are only available at the higher end of the licensing model. E.g. Advanced Threat Protection, security, and collaboration tools are specific to the “E5” license tier, or as additional payed addons. Whilst this documentation is licence agnostic it is important to note that some of the recommendations provided are only available at higher licensing tiers and may therefore incur additional costs for compliance requirements.

It is clear from vendor and best practice documentation that a large proportion of effort and resourcing should go into strategic planning when implementing Office365.

All of the information within this documentation is taken directly from official sources listed. This documentation aims to consolidate the many different sources of currently available Office 365 security information into a single checklist document.

Guidance

The guidance documentation is broken down into several sections and are organized by priority of work.

Checklist documents have been accumulated to allow teams to review this guidance with greater ease within a single Excel format spreadsheet. Available on Github

{See attached "Unger Office 365 Security Checklist"}

Implementations teams & business decision makers should complete these checklists and provide relevant information for each item. Any deviations from best practice guidance should be fully documented with detailed reasoning. This ensures accurate documentation and allows for risk assessment processes.

In addition to the security specific requirements which have been defined, implementors should follow general best practice implementation guidance defined in available vendor documentation.

References to source documentation are available in the appendix section of this document.

Introduction (Tab1)

The first tab of the "Unger Office 365 Security Checklist" provides a brief introduction.

Microsoft 365 Security for Business Decision Makers (BDMs)

The 2nd tab is based on the Microsoft article which discusses some of the most common threat and attack scenarios currently faced by organizations for their Microsoft 365 environments, and recommended actions for mitigating these risks. While Microsoft 365 comes with a wide array of pre-configured security features, it also requires you as the customer to take responsibility to secure your own identities, data, and devices used to access cloud services. This guidance was developed by Kozeta Beam (Microsoft Cloud Security Architect) and Thiagaraj Sundararajan (Microsoft Senior Consultant).

This article is organized by priority of work, starting with protecting those accounts used to administer the most critical services and assets, such as your tenant, e-mail, and SharePoint. It provides a methodical way for approaching security and works together with the following spreadsheet so you can track your progress with stakeholders and teams across your organization: Microsoft 365 security for BDMs spreadsheet. See "Unger Office 365 Security Checklist" tab 2.

Microsoft provides you with the Secure Score tool within your tenant to automatically analyse your security posture based on your regular activities, assign a score, and provide security improvement recommendations. Before taking the actions recommended in this article, take note of your current score and recommendations. The actions recommended in this article will increase your score. See Microsoft Secure Score.

One more thing before we get started is be sure to turn on the Office 365 audit log. You'll need this data later, in the event you need to investigate an incident or a breach.

CIS Foundations Benchmark

The 3rd tab features the latest checklist (v1.1.0 - 12-20-2019) from The Center for Internet Security (CIS) which has published benchmarks for Microsoft products and services including the Microsoft Azure and Microsoft 365 Foundations Benchmarks, the Windows 10 Benchmark, and the Windows Server 2016 Benchmark.

CIS benchmarks are internationally recognized as security standards for defending IT systems and data against cyberattacks. Used by thousands of businesses, they offer prescriptive guidance for establishing a secure baseline configuration. System and application administrators, security specialists, and others who develop solutions using Microsoft products and services can leverage these best practices to assess and improve the security of their applications.

Like all CIS benchmarks, the Microsoft benchmarks were created using a consensus review process based on input from subject matter experts with diverse backgrounds spanning software development, audit and compliance, security research, operations, government, and law. Microsoft was an integral partner in these CIS efforts. For example, Office 365 was tested against the listed services, and the resulting Microsoft 365 Foundations Benchmark covers a broad range of recommendations for setting appropriate security policies that cover account and authentication, data management, application permissions, storage, and other security policy areas.

In addition to the benchmarks for Microsoft products and services, CIS has also published CIS Hardened Images for use on Azure virtual machines configured to meet CIS benchmarks. These include the CIS Hardened Image for Microsoft Windows Server 2016 certified to run on Azure. CIS states that, “All CIS hardened images that are available on the Azure Marketplace are certified to run on Azure. They have been pre-tested for readiness and compatibility with the Azure public cloud, the Microsoft Cloud Platform hosted by service providers through the Cloud OS Network, and on-premise private cloud Windows Server Hyper-V deployments managed by customers.”

Office 365 Compliance Baseline

The 4th tab details the latest release of the recommended vendor security compliance configuration baseline settings for Microsoft Office 365 ProPlus (Microsoft Security Compliance Toolkit 1.0).

It details how to apply the group policy settings shown on following tab 5 (computer) and tab 6 (user). These additional tabs display all available Office 365 ProPlus Group Policy settings and the corresponding Microsoft-recommended configuration of those settings for well-managed enterprise systems.

124 User baseline configuration options have defined values which should be applied via group policy (of 2129 total available).

16 Computer baseline configuration options have defined values which should be applied via group policy (of 73 total available).

Deployment Planning Checklist for Office 365

The 7th tab details the recommended deployment planning checklist for Office 365 available from Microsoft.

When you move an enterprise organization to Office 365, it's important to plan exactly what steps you want to take, when to perform them, and who will perform them. This checklist will help your organization as you plan and prepare for a migration to Office 365. The phases and steps in the checklist are aligned with the guidance provided by the Onboarding Center. Feel free to adapt this checklist to your organization's needs.

Whilst not specific to security, this checklist provides the recommended typical information required for an Office 365 deployment, allowing security teams to assess accordingly.

Security Roadmap Checklist for Office 365

The 8th tab details the high-level security roadmap checklist for Office 365 available from Microsoft.

This article includes top recommendations from Microsoft's cybersecurity team for implementing security capabilities to protect your Office 365 environment. This article is adapted from a Microsoft Ignite session — “Secure Office 365 like a cybersecurity pro: Top priorities for the first 30 days, 90 days, and beyond”. This session was developed and presented by Mark Simos and Matt Kemelhar, Enterprise Cybersecurity Architects.

The same information is shown in the “Roadmap” section of this document.

Next steps

Implementations teams & business decision makers should complete these checklists and provide relevant information for each item. Any deviations from best practice guidance should be fully documented with detailed reasoning. This ensures accurate documentation and allows for risk assessment processes.

These checklists should be reviewed regularly and kept up to date.

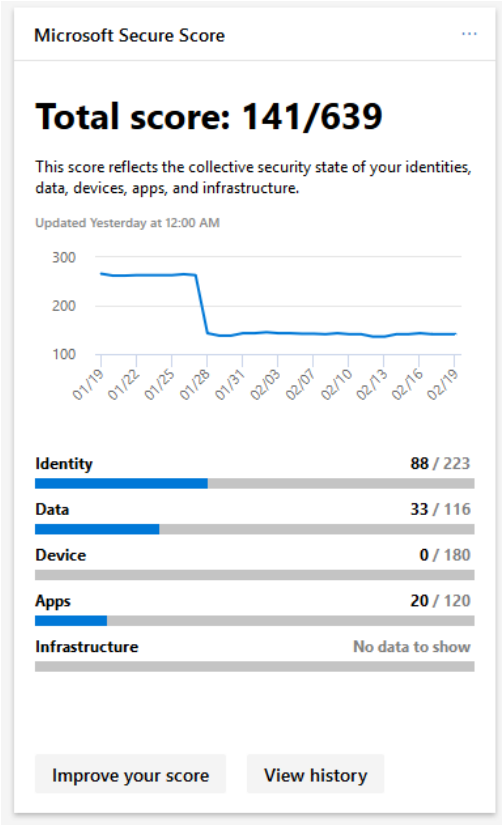
These checklists establish the basic level of security for anyone adopting in-scope Microsoft products and services. However, they should not be considered as an exhaustive list of all possible security configurations and architecture but as a starting point. Each organization must still evaluate its specific situation, workloads, and compliance requirements and tailor its environment accordingly.

The Microsoft Secure Score and the and Office 365 Security & compliance Dashboard within the 365 tenant also offer useful ways to gauge ongoing security requirements.

The current configuration checks and a high level 365 security roadmap are shown in the following sections.

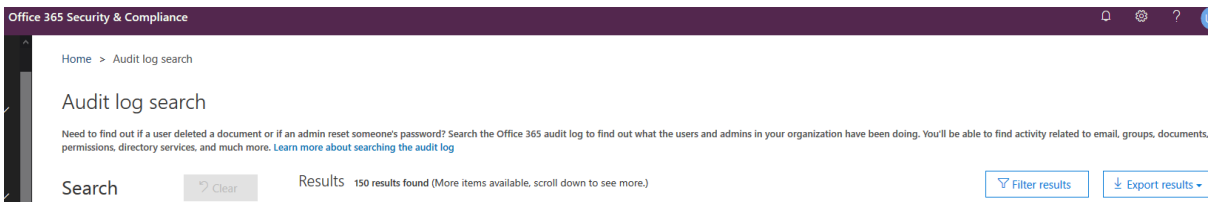
Current Configuration

Check the current secure score (e.g. 141/639):



Check if Advanced Threat Protection (ATP) is enabled or licenced:

Check if the audit log is enabled:



Roadmap

Office 365 security roadmap - Top priorities for the first 30 days, 90 days, and beyond

This article includes top recommendations from Microsoft's cybersecurity team for implementing security capabilities to protect your Office 365 environment.

In this article:

Roadmap outcomes

These roadmap recommendations are staged across three phases in a logical order with the following goals.

Timeline	Outcomes
30 days	Rapid configuration: • Basic admin protections • Logging and analytics • Basic identity protections
	Tenant configuration
	Prepare stakeholders
90 days	Advanced protections: • Admin accounts • Data & user accounts
	Visibility into compliance, threat, and user needs
	Adapt and implement default policies and protections
Beyond	Adjust and refine key policies and controls
	Extend protections to on-premises dependencies
	Integrate with business and security processes (legal, insider threat, etc.)

30 days — powerful quick wins

These tasks can be accomplished quickly and have low impact to users.

Area	Tasks
Security management	• Check Secure Score and take note of your current score (https://securescore.office.com).
	• Turn on audit logging for Office 365. See Search the audit log.
	• Configure your Office 365 tenant for increased security .
	• Regularly review dashboards and reports in the Microsoft 365 security center and Cloud App Security.
Threat protection	Connect Office 365 to Microsoft Cloud App Security to start monitoring using the default threat detection policies for anomalous behaviors. It takes seven days to build a baseline for anomaly detection.
	Implement protection for admin accounts: • Use dedicated admin accounts for admin activity. • Enforce multi-factor authentication (MFA) for admin accounts. • Use a highly secure Windows 10 device for admin activity.
Identity and access management	• Enable Azure Active Directory Identity Protection.
	• For federated identity environments, enforce account security (password length, age, complexity, etc.).
Information protection	Review example information protection recommendations. Information protection requires coordination across your organization. Get started with these resources: • Office 365 Information Protection for GDPR • Secure SharePoint Online sites and files (includes sharing, classification, data loss prevention, and Azure Information Protection)

90 days — enhanced protections

These tasks take a bit more time to plan and implement but greatly increase your security posture.

Area	Task
Security management	• Check Secure Score for recommended actions for your environment (https://securescore.office.com).
	• Continue to regularly review dashboards and reports in the Microsoft 365 security center, Cloud App Security, and SIEM tools.
	• Look for and implement software updates.
	• Conduct attack simulations for spear-phishing, password-spray, and brute-force password attacks using Attack Simulator (included with Office 365 Threat Intelligence).
	• Look for sharing risk by reviewing the built-in reports in Cloud App Security (on the Investigate tab).
	• Check Compliance Score to review status for regulations that apply to your organization (such as GDPR, NIST 800-171).
Threat protection	Implement enhanced protections for admin accounts: • Configure Privileged Access Workstations (PAWs) for admin activity. • Configure Azure AD Privileged Identity Management. • Configure a security information and event management (SIEM) tool to collect logging data from Office 365, Cloud App Security, and other services, including AD FS. The Office 365 Audit Log stores data for only 90 days. Capturing this data in SIEM tool allows you to store data for a longer period.
Identity and access management	• Enable and enforce MFA for all users.
	• Implement a set of conditional access and related policies.
Information protection	Adapt and implement information protection policies. These resources include examples: • Office 365 Information Protection for GDPR • Secure SharePoint Online sites and files
	Use data loss prevention policies and monitoring tools in Office 365 for data stored in Office 365 (instead of Cloud App Security).
	Use Cloud App Security with Office 365 for advanced alerting features (other than data loss prevention).

Beyond 90 days

These are important security measures that build on previous work.

Area	Task
Security management	• Continue planning next actions by using Secure Score (https://securescore.office.com).
	• Continue to regularly review dashboards and reports in the Microsoft 365 security center, Cloud App Security, and SIEM tools.
	• Continue to look for and implement software updates.
	• Integrate eDiscovery into your legal and threat response processes.
Threat protection	• Implement Secure Privileged Access (SPA) for identity components on premises (AD, AD FS).
	• Use Cloud App Security to monitor for insider threats.
	• Discover shadow IT SaaS usage by using Cloud App Security.
Identity and access management	• Refine policies and operational processes.
	• Use Azure AD Identity Protection to identify insider threats.
Information protection	Refine information protection policies: • Microsoft 365 and Office 365 sensitivity labels and data loss prevention (DLP), or Azure Information Protection. • Cloud App Security policies and alerts.

Security Concerns

The following are potential high level security concerns with the implementation of Office 365 which should be considered;

- Project Management (or lack thereof)
- Time constraints & business deadlines
- Resourcing availability
- Technical knowledge & capabilities
- Licence & cost barriers for security features
- Dependency items, pre-requisites and related configuration planning (Hybrid, DLP, ATP, PAM, etc.)
- Potential for decrease in security capabilities for any replaced existing security solutions (email protection, file storage, etc.)
- Unexpected platform changes by vendor
- Business impact (Service outages during migration work, user education & awareness)

References

https://docs.microsoft.com/en-gb/microsoft-365/security/

https://docs.microsoft.com/en-gb/microsoft-365/security/microsoft-365-security-for-bdm

https://github.com/MicrosoftDocs/microsoft-365-docs/raw/public/microsoft-365/downloads/Microsoft-365-BDM-security-recommendations-spreadsheet.xlsx

https://practical365.com/office-365-security-resources/

https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-overview

https://docs.microsoft.com/en-us/microsoft-365/enterprise/deploy-microsoft-365-enterprise

https://docs.microsoft.com/en-gb/microsoft-365/security/office-365-security/security-roadmap

https://docs.microsoft.com/en-gb/microsoft-365/security/office-365-security/

https://www.cisecurity.org/benchmark/microsoft_office/

https://cloudsecurityalliance.org/star/registry/microsoft/

https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home?view=o365-worldwide

https://www.microsoft.com/en-gb/trust-center/product-overview

https://docs.microsoft.com/en-us/deployoffice/readiness-tools

https://docs.microsoft.com/en-GB/microsoftteams/security-compliance-overview

https://www.ncsc.gov.uk/blog-post/securing-office-365-with-better-configuration

https://www.ncsc.gov.uk/news/rise-microsoft-office-365-compromise

https://www.ncsc.gov.uk/collection/saas-security?curPage=/collection/saas-security/product-evaluations/office-365

https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

https://techcommunity.microsoft.com/t5/office-365-blog/released-office-365-audited-controls-for-nist-800-53/ba-p/61479

https://www.microsoft.com/en-gb/microsoft-365/compare-all-microsoft-365-plans

https://docs.microsoft.com/en-us/microsoft-365/enterprise/contoso-overview

https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-secure-score

https://docs.microsoft.com/en-gb/microsoft-365/security/office-365-security/turn-on-atp-for-spo-odb-and-teams