#NVSummit2021

Getting started with Microsoft Defender for Office and Endpoints

- Marius A. Skovli
- Principal Consultant @ CTGlobal
- Twitter @MariusSkovli
- MVP Enterprise Mobility

NORDIC — VIRTUAL SUMMIT —

NORDIC
– VIRTUAL SUMMIT –

Getting started with Microsoft Defender for Office and Endpoints

Agenda

NORDIC
– VIRTUAL SUMMIT –

- How to onboard devices and users
- How to Integrate with Secure Score to better understand what to prioritize
- How to use the data and dashboard to take certain actions
- How to Implement your first anti-phishing, safe-attachment and safe-link policies
- How to monitor and act

NORDIC
– VIRTUAL SUMMIT –

600%

Cybercrime Up 600%
Due To COVID-19
Pandemic

NORDIC
— VIRTUAL SUMMIT —

The total malware infections have been on the rise for the last ten (+) years:

2009 - 12.4 million
2010 - 29.97 million
2011 - 48.17 million
2012 - 82.62 million
2013 - 165.81 million
2014 - 308.96 million
2015 - 452.93 million
2016 - 580.40 million
2017 - 702.06 million
2018 - 812.67 million

NORDIC
– VIRTUAL SUMMIT –

92%

of malware is
delivered by email

NORDIC
– VIRTUAL SUMMIT –

7 / 10

7 out of every 10
malware payloads
were ransomware.

NORDIC
– VIRTUAL SUMMIT –

18 mill.

Over 18 million websites are infected with malware at a given time, each week.

1.5 million new phishing sites are created every month.

In 2019 ransomware from phishing emails increased 109% over 2017.

NORDIC
– VIRTUAL SUMMIT –

Let’s be pragmatic!

In order to take the first step, we need to know which direction

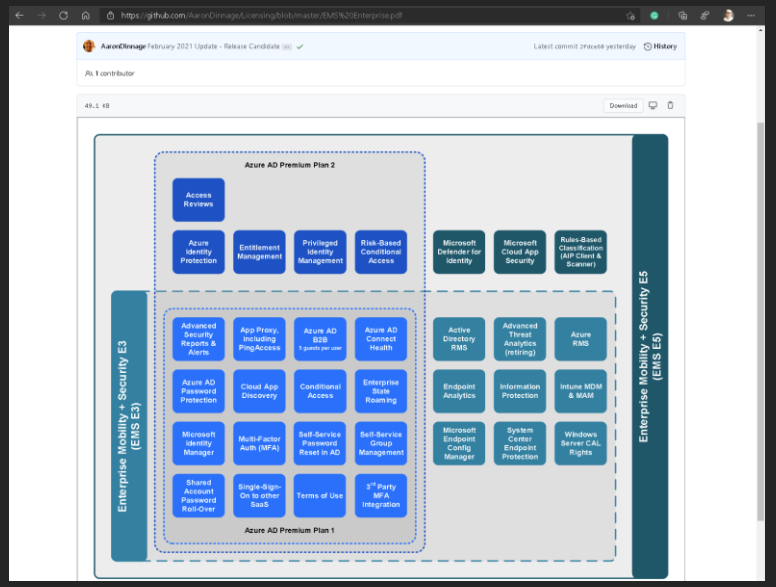
NORDIC
– VIRTUAL SUMMIT –

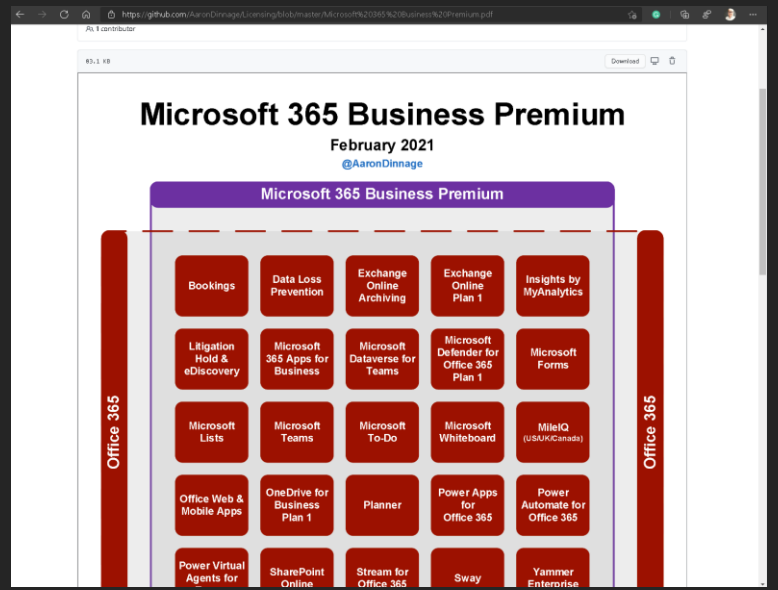
First step should then be…

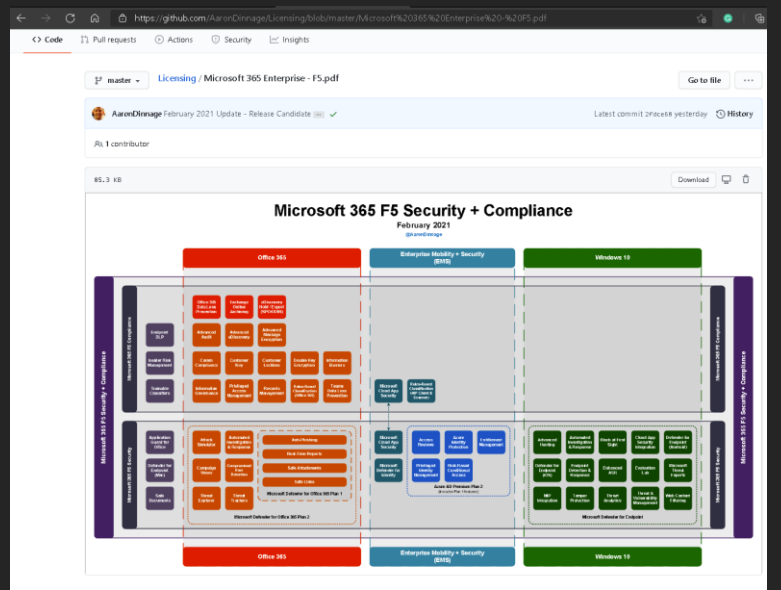
1. Verfiy your licenses
2. Onboard devices and servers and get the intel and insights on how to proceed
3. Integrate with Secure Score
    - Identity
    - Apps
    - Devices
4. Use recommended steps as an initial guide to get the momentum up
5. Enable Office ATP policies (Anything with “Anti” or “Safe” in it)
6. Secure Score will keep you accountable

Licenses

- Always the good stuff…
- Consult with your CSP or License partner
- Use docs.microsoft.com
- Check out this git site for guidens inspiration: https://github.com/AaronDinnage/Licensing







Onboard your endpoints

NORDIC
– VIRTUAL SUMMIT –

- Get the insights to take the right actions
- Supported platforms
  - Native:
    - Windows Server 2019/1803
    - Windows 10
    - Windows 10 multi-session running on Windows Virtual Desktop (WVD)
  - With MMA (Microsoft Monitoring Agent):
    - Windows Server 2016 / 2012 R2 / 2008 R2 SP1
    - Windows 7 / 8.1
  - macOS
  - Linux Server
  - Android
  - (iOS)
- Integrate with Endpoint Manager (Intune)
- Attack Surface Reducation Policies = Audit Mode

[Onboard Windows servers to the Microsoft Defender ATP service - Windows security | Microsoft Docs]

Offboard your endpoints

NORDIC
– VIRTUAL SUMMIT –

- You need this routine
  - Especially for Win10 and Server 2019/1803
- Offboard key expires (after 30 days)

> For security reasons, the offboarding package will expire within 30 days of its creation. The expiry date is embedded in the created package name: *WindowsDefenderATPOffboardingPackage_valid_until_YYYY-MM-DD.zip* (where YYYY-MM-DD is the expiry date of the package).
> Expired offboarding packages sent to a device will fail to offboard the device.

- Different method for different platforms

Enable notifications

- Alert notifications
- Exploit or vulnerability events

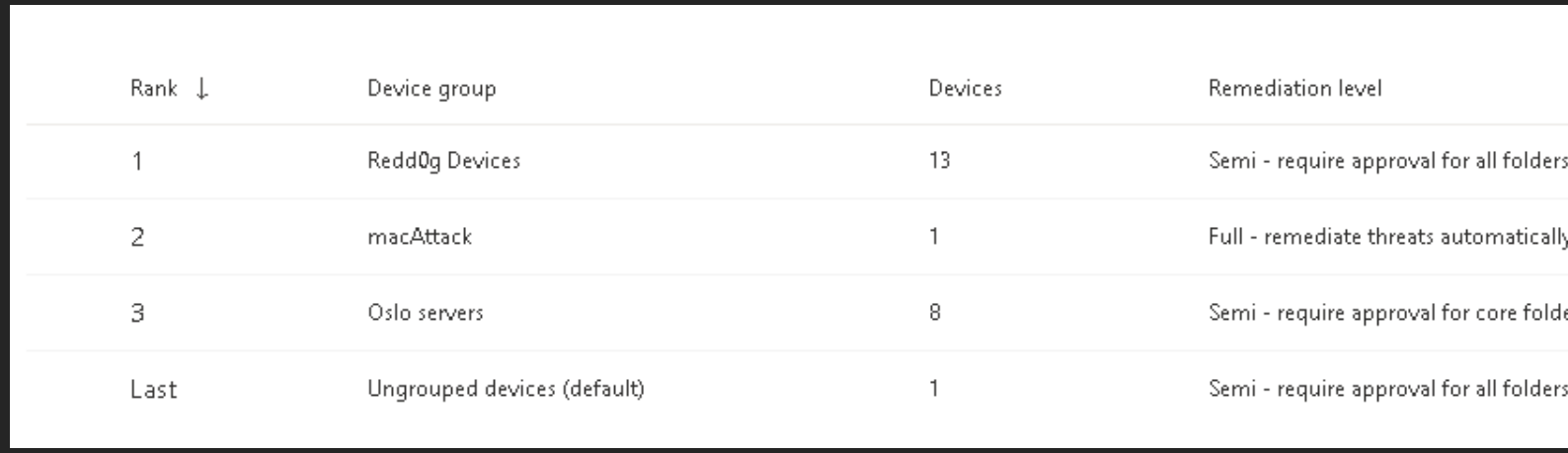
NORDIC
– VIRTUAL SUMMIT –

Create device groups

NORDIC
– VIRTUAL SUMMIT –

Create device groups for

1. Better reporting
2. Granular control over remediation
3. Use Tags
    1. Manually in the console
    2. During onboarding
    3. RegKey

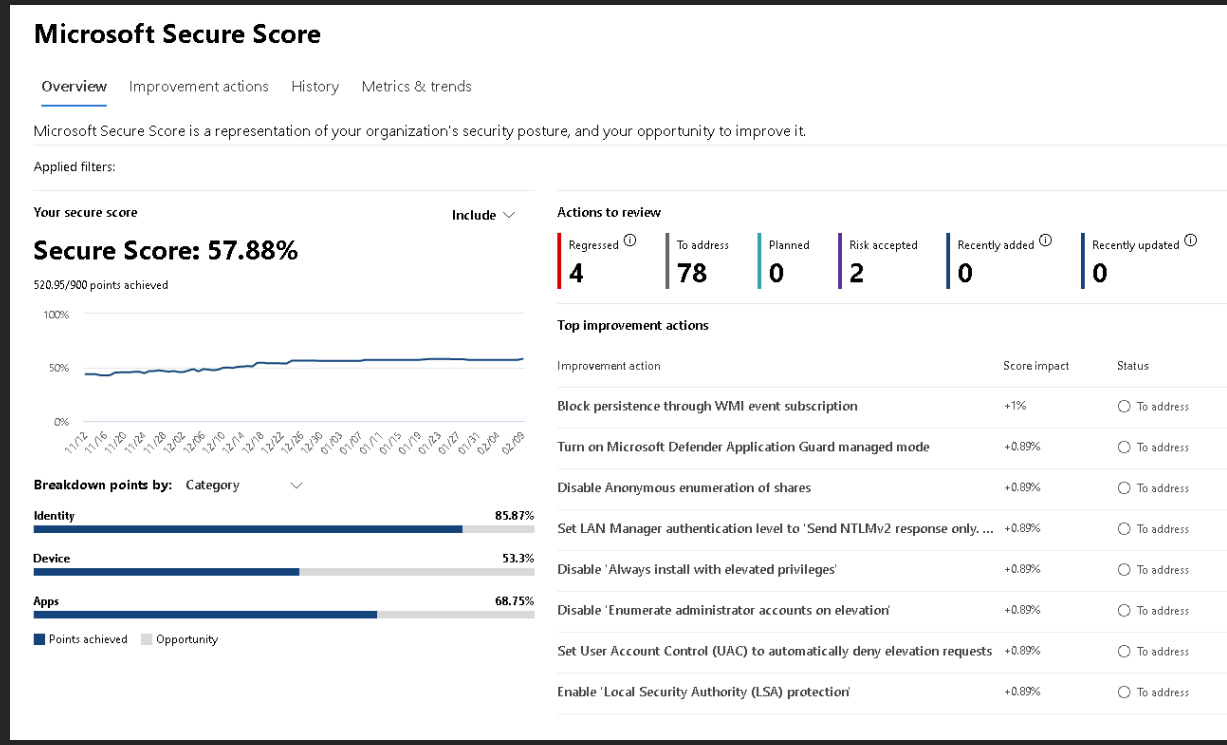


Rank ↓	Device group	Devices	Remediation level
1	Redd0g Devices	13	Semi - require approval for all folders
2	macAttack	1	Full - remediate threats automatically
3	Oslo servers	8	Semi - require approval for core folde
Last	Ungrouped devices (default)	1	Semi - require approval for all folders

Integrate with Secure Score

NORDIC
— VIRTUAL SUMMIT —

- Integrate with Secure Score
- Use the date and improvement actions as guidelines and map
- Integrate other services like Identity and Apps for a consolidated view of your security posture
- Use the portal activly
- Use Security recomendations and prioritize



https://security.microsoft.com

https://securitycenter.windows.com/

NORDIC
– VIRTUAL SUMMIT –

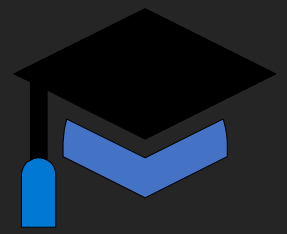
Demo ▷

1. Onboarding
2. Device Groups
3. Notifications
4. Security recommendations
5. Secure Score
6. Device Inventory / controls

Defender for Office

Protection from phishing and malware

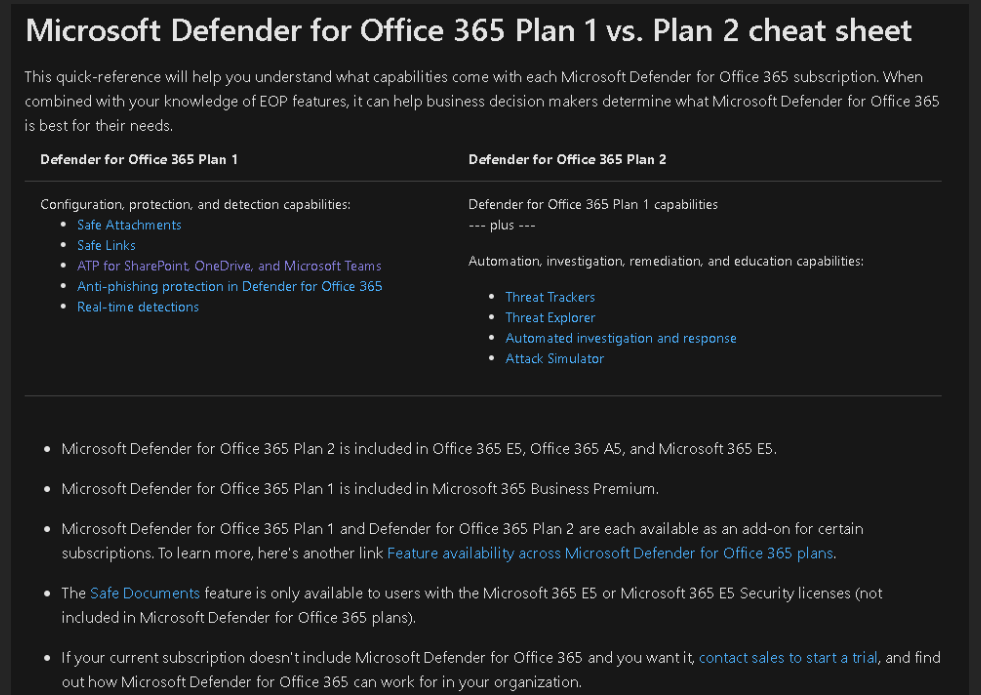
Post-breach automated incident response



Attack simulation and user awareness

Enable the Safe and Anti

- Anti-Phishing
- Anti-spam
- Anti-malware
- Safe Attachments
- Safe Links



Microsoft Defender for Office 365 Plan 1 vs. Plan 2 cheat sheet

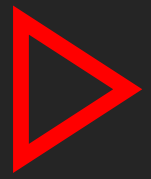
This quick-reference will help you understand what capabilities come with each Microsoft Defender for Office 365 subscription. When combined with your knowledge of EOP features, it can help business decision makers determine what Microsoft Defender for Office 365 is best for their needs.

Defender for Office 365 Plan 1	Defender for Office 365 Plan 2
Configuration, protection, and detection capabilities: • Safe Attachments • Safe Links • ATP for SharePoint, OneDrive, and Microsoft Teams • Anti-phishing protection in Defender for Office 365 • Real-time detections	Defender for Office 365 Plan 1 capabilities --- plus --- Automation, investigation, remediation, and education capabilities: • Threat Trackers • Threat Explorer • Automated investigation and response • Attack Simulator

- Microsoft Defender for Office 365 Plan 2 is included in Office 365 E5, Office 365 A5, and Microsoft 365 E5.
- Microsoft Defender for Office 365 Plan 1 is included in Microsoft 365 Business Premium.
- Microsoft Defender for Office 365 Plan 1 and Defender for Office 365 Plan 2 are each available as an add-on for certain subscriptions. To learn more, here's another link Feature availability across Microsoft Defender for Office 365 plans.
- The Safe Documents feature is only available to users with the Microsoft 365 E5 or Microsoft 365 E5 Security licenses (not included in Microsoft Defender for Office 365 plans).
- If your current subscription doesn't include Microsoft Defender for Office 365 and you want it, contact sales to start a trial, and find out how Microsoft Defender for Office 365 can work for in your organization.

NORDIC
– VIRTUAL SUMMIT –

Demo



1. Create ATP Safe-Attachment policy
2. Create ATP Safe-Links policy
3. Create ATP Anti-Phishing policy
4. End-user experience
5. Monitoring

Summery

NORDIC
– VIRTUAL SUMMIT –

Licenses

- Consult
- Figure out what features you need
- Answers may come after you get the data

Onboard & Evaluate

- Get the insights you need and prioritize
- Enable Attack Surface Reduction Policies in Audit Mode
- Enable the "Safe" and "Anti policies" in Defender for Office
  - Start small an Scale Up

Create Operations routines

- Get a habit of using secure score and security recommendations to continuously fix and mitigate issues
- Create incident and response routines to alerts and other notifications (i.n. Action Center – quarantined files)

Thank you!

NORDIC
– VIRTUAL SUMMIT –

MSEndPointMgr.com
#MSEndPointMgr

System Center User Group Finland
#SCUGFI

System Center User Group Denmark

#SCUGDK

System Center User Group Sweden
#SCUGSE

Modern Management User Group Norway
#MMUGNO